Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1258

(09/2016)

SÉRIE X: RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

Sécurité du cyberespace – Gestion des identités

Authentification d'entité améliorée basée sur des attributs agrégés

Recommandation UIT-T X.1258

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

RÉSEAUX PUBLICS DE DONNÉES	X.1–X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	X.200–X.299
INTERFONCTIONNEMENT DES RÉSEAUX	X.300–X.399
SYSTÈMES DE MESSAGERIE	X.400–X.499
ANNUAIRE	X.500–X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	X.600–X.699
GESTION OSI	X.700–X.799
SÉCURITÉ	X.800–X.849
APPLICATIONS OSI	X.850–X.899
TRAITEMENT RÉPARTI OUVERT	X.900–X.999
SÉCURITÉ DE L'INFORMATION ET DES RÉSEAUX	
Aspects généraux de la sécurité	X.1000–X.1029
Sécurité des réseaux	X.1030–X.1049
Gestion de la sécurité	X.1050–X.1069
Télébiométrie	X.1080–X.1099
APPLICATIONS ET SERVICES SÉCURISÉS	
Sécurité en multidiffusion	X.1100–X.1109
Sécurité des réseaux domestiques	X.1110–X.1119
Sécurité des télécommunications mobiles	X.1120–X.1139
Sécurité de la toile	X.1140–X.1149
Protocoles de sécurité	X.1150–X.1159
Sécurité d'homologue à homologue	X.1160–X.1169
Sécurité des identificateurs en réseau	X.1170–X.1179
Sécurité de la télévision par réseau IP	X.1180–X.1199
SÉCURITÉ DU CYBERESPACE	
Cybersécurité	X.1200–X.1229
Lutte contre le pollupostage	X.1230–X.1249
Gestion des identités	**X.1250–X.1279**
APPLICATIONS ET SERVICES SÉCURISÉS	
Communications d'urgence	X.1300–X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310–X.1339
Recommandations relatives aux infrastructures de clé publique	X.1340–X.1349
ECHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	
Aperçu général de la cybersécurité	X.1500–X.1519
Echange concernant les vulnérabilités/les états	X.1520–X.1539
Echange concernant les événements/les incidents/l'heuristique	X.1540–X.1549
Echange de politiques	X.1550–X.1559
Heuristique et demande d'informations	X.1560–X.1569
Identification et découverte	X.1570–X.1579
Echange garanti	X.1580–X.1589
SÉCURITÉ DE L'INFORMATIQUE EN NUAGE	
Aperçu de la sécurité de l'informatique en nuage	X.1600–X.1601
Conception de la sécurité de l'informatique en nuage	X.1602–X.1639
Bonnes pratiques et lignes directrices concernant la sécurité de l'informatique en nuage	X.1640–X.1659
Mise en oeuvre de la sécurité de l'informatique en nuage	X.1660–X.1679
Sécurité de l'informatique en nuage (autres)	X.1680–X.1699

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T X.1258

Authentification d'entité améliorée basée sur des attributs agrégés

Résumé

L'agrégation d'attributs provenant de multiples autorités d'attribut peut être nécessaire afin de permettre à une partie utilisatrice d'accroître sa confiance dans l'identité d'une partie. On peut considérer que l'agrégation consiste à traiter un ensemble d'identificateurs uniques au niveau mondial, qui est commun à toutes les autorités d'attribut. Dans la pratique, les entités n'ont pas d'identificateur mondial, mais elles ont différents identificateurs et attributs d'entité assignés par leurs différents fournisseurs de service d'identité (IdSP).

Pour résoudre le problème que pose l'agrégation d'attributs dans ce contexte, on utilise le concept de fédération d'identités. Par exemple, si une librairie électronique prévoit une opération commerciale à l'intention des personnes âgées, l'ensemble agrégé d'attributs (carte de crédit et tranche d'âge) provenant de deux fournisseurs IdSP doit lui être communiqué, mais sans que les fournisseurs IdSP sachent quel est le rôle de l'autre. Dans la gestion des identités fédérées type, une entité peut fournir uniquement des attributs pour une seule identité, alors que cette transaction nécessite des attributs pour deux. Il existe plusieurs méthodes de fédération des identités: le langage de balisage d'assertion de sécurité (SAML), la méthode de Shibboleth, l'identité ouverte (OpenID), l'authentification ouverte (OAuth), etc.

La Recommandation UIT-T X.1258 présente le concept d'agrégation d'attributs en vue de permettre à une entité d'agréger des attributs provenant de multiples fournisseurs IdSP. L'agrégation d'attributs est le mécanisme consistant à recueillir les attributs d'une entité obtenus auprès de multiples fournisseurs IdSP. Elle est nécessaire pour agréger les attributs de manière dynamique à la demande. Le fournisseur IdSP peut effectuer la demande d'agrégation lorsqu'une entité veut obtenir un service. En outre, un mécanisme d'agrégation des attributs centré sur l'entité pourrait être également appliqué à l'authentification afin de limiter les fuites de données confidentielles.

Historique

Edition	Recommandation	Approbation	Commission d'études	ID unique*
1.0	ITU-T X.1258	2016-09-07	17	11.1002/1000/12850

Mots clés

Agrégation d'attributs, gestion d'identité fédérée.

* Pour accéder à la Recommandation, reporter cet URL http://handle.itu.int/ dans votre navigateur Web, suivi de l'identifiant unique, par exemple http://handle.itu.int/11.1002/1000/11830-en.

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT avait été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux développeurs de consulter la base de données des brevets du TSB sous http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

Recommandation UIT-T X.1258

Authentification d'entité améliorée basée sur des attributs agrégés

1 Domaine d'application

La présente Recommandation décrit une authentification améliorée basée sur l'agrégation d'attributs d'entité dans différents domaines. Elle porte sur les aspects suivants:

– méthodes d'agrégation d'attributs provenant de multiples fournisseurs de service d'identité (IdSP); et

– authentification améliorée basée sur des attributs agrégés.

2 Références

Néant.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 attribut [b-UIT-T X.1252]: information liée à une entité qui en spécifie une caractéristique.

3.1.2 authentification (d'entité) [b-UIT-T X.1252]: processus utilisé pour obtenir une confiance suffisante dans le lien entre l'entité et l'identité présentée.

NOTE – Dans un contexte de gestion d'identité (IdM), le terme authentification désigne l'authentification d'entité.

3.1.3 cercle de confiance [b-UIT-T X.1251]: ensemble de critères établis pour regrouper des organisations au sein d'une fédération, afin de fournir un accès sécurisé aux ressources de chacune d'elles. Il est à noter qu'un cercle de confiance est également le résultat final du regroupement d'organisations au sein d'une fédération.

3.1.4 fédération [b-UIT-T X.1252]: association d'utilisateurs, de fournisseurs de service et de fournisseurs de service d'identité.

3.1.5 identité [b-UIT-T X.1252]: représentation d'une entité sous la forme d'un ou de plusieurs attributs qui sont suffisants pour pouvoir distinguer les entités dans un contexte. Aux fins de la gestion des identités (IdM), le terme identité désigne l'identité contextuelle (sous-ensemble d'attributs), c'est-à-dire que la diversité des attributs est limitée par un cadre avec des frontières définies (le contexte) dans lequel l'entité existe et interagit.

NOTE − Chaque entité est représentée par une identité holistique, qui comprend tous les éléments d'information possibles caractérisant cette entité (les attributs). Toutefois, l'identité holistique est théorique et échappe à toute description et utilisation pratique, car le nombre de tous les attributs possibles est indéfini.

3.1.6 fournisseur de service d'identité (IdSP) [b-UIT-T X.1252]: entité qui vérifie, tient à jour, gère et peut créer et attribuer des informations d'identité concernant d'autres entités.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

3.2.1 agrégation d'attributs: mécanisme consistant à recueillir les attributs d'une entité obtenus auprès de multiples fournisseurs de service d'identité (IdSP).

NOTE – Une fois rassemblés, les attributs doivent être agrégés et validés en vue de l'authentification et de l'autorisation.

3.2.2 domaine: périmètre de gestion couvert par un seul fournisseur de service d'identité (IdSP).

3.2.3 fournisseur de services (SP): entité qui fournit des services aux clients ou aux autres fournisseurs de services.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

CoT cercle de confiance (*circle of trust)*

DB base de données (*database*)

ID identité (*identity*)

IdM gestion d'identité (*identity management*)

IdSP fournisseur de service d'identité (*identity service provider*)

LS service d'association (*linking service*)

OAuth authentification ouverte (*open authentication*)

OpenID identité ouverte (*open identity*)

PKI infrastructure de clé publique (*public key infrastructure*)

SAML langage de balisage d'assertion de sécurité (*security assertion markup language*)

SP fournisseur de services (*service provider*)

SSO authentification unique (*single sign-on*)

VC collaboration virtuelle (*virtual collaboration*)

5 Conventions

Aucune.

6 Généralités

En général, la gestion d'identité (IdM) électronique couvre la gestion de toutes les formes d'identité numérique. L'élaboration d'annuaires, comme ceux pris en charge par [b-UIT-T X.500], pourrait être considérée comme étant à l'origine de la gestion IdM. [b-UIT-T X.509] définit des certificats contenant des attributs d'identité. Les certificats définis dans [b-UIT-T X.509] et les systèmes d'infrastructure de clé publique (PKI) permettent de prouver "l'identité" en ligne d'un sujet. Par conséquent, on pourrait considérer la gestion IdM comme étant la gestion d'informations.

L'identité d'une entité peut être composée d'attributs qui caractérisent cette entité dans différents contextes. Différentes identités peuvent être nécessaires en fonction du contexte et de la situation. Un système de gestion IdM fournit des outils permettant de gérer ces identités dans un environnement numérique. La gestion IdM est un ensemble de fonctions et de capacités, comme la création/suppression d'identité, la découverte et l'échange d'informations. Dans le monde réel, une personne choisit les informations qui peuvent être révélées à d'autres personnes, compte tenu du contexte et de la sensibilité des informations. Dans le monde numérique, cette tâche est menée à bien par le système de gestion IdM.

Selon les technologies et les normes concernant la gestion IdM, les méthodes appliquées par les systèmes de gestion IdM peuvent être conventionnelles, centralisées ou fédérées. Dans le cadre de la méthode conventionnelle, un fournisseur de services (SP) gère les identités et est situé au même endroit que le fournisseur de service d'identité (IdSP). Une entité crée son identité numérique (ID) pour chaque fournisseur SP dont elle veut obtenir des services. En général, les identités d'une entité ne sont pas partagées avec les différents fournisseurs SP et cette approche est souvent plus coûteuse à la fois pour l'entité et pour les fournisseurs SP. Chaque fournisseur SP risque de devoir obtenir à plusieurs reprises son propre ensemble d'attributs pour composer l'identité numérique de l'entité.

La méthode centralisée, qui a été élaborée pour remédier à l'absence de souplesse de la méthode conventionnelle, permet de partager les identités avec les fournisseurs SP; elle repose sur le concept d'authentification unique (SSO). On tente ainsi d'éviter les incohérences et les redondances de la méthode conventionnelle en donnant aux entités la capacité d'interagir avec différents fournisseurs SP sans que ceux-ci aient besoin d'effectuer une authentification redondante.

Chaque fournisseur SP qui a une relation de confiance avec un fournisseur IdSP s'appuie entièrement sur les authentifications d'entité fournies par ce fournisseur. Le fournisseur IdSP est chargé d'authentifier une entité et de communiquer aux fournisseurs SP les informations d'attribut de cette entité dans un domaine, qui peut correspondre à une entreprise, une université, etc. et qui est composé d'entités, de multiples fournisseurs SP et d'un seul fournisseur IdSP. L'authentification SSO est très pratique pour les entités, qui ne doivent mener à bien le processus d'authentification qu'une seule fois et peuvent ensuite utiliser les justificatifs obtenus pour tous les fournisseurs SP auxquels elles souhaitent accéder. Toutefois, le point faible de la méthode centralisée est que le fournisseur IdSP contrôle entièrement les informations des entités qui font appel à lui et peut utiliser ces informations comme il le veut. Il s'agit de la principale raison expliquant pourquoi la méthode centralisée n'a pas été largement adoptée.

Pour résoudre les problèmes liés à la méthode centralisée, on a mis en place la méthode des identités fédérées, qui repose sur la répartition de l'opération d'authentification entre de multiples fournisseurs IdSP, qui appartiennent à différents domaines. Le concept d'identité fédérée repose sur les relations de confiance qui sont établies entre de multiples fournisseurs IdSP et les domaines correspondants. Pour relier des informations d'identité réparties entre un fournisseur IdSP et un fournisseur SP, une relation de confiance est nécessaire entre ces deux parties. Cette relation est appelée cercle de confiance (CoT) et ce cercle de confiance peut comprendre un ou plusieurs fournisseurs IdSP et fournisseurs SP. Dans un cercle CoT, si un utilisateur s'authentifie auprès d'un fournisseur IdSP, il peut alors accéder aux fournisseurs SP appartenant à ce cercle CoT sans s'authentifier de nouveau. Ainsi, un utilisateur ne doit s'authentifier qu'une seule fois dans un cercle de confiance [b-UIT-T X.1251].

La gestion IdM fédérée est une solution pour résoudre le problème que pose la présence d'un seul fournisseur IdSP et réduire l'échange d'informations avec le fournisseur IdSP pendant l'authentification. Ces accords entre fournisseurs IdSP garantissent que les identités émises dans un domaine sont reconnues par les fournisseurs SP dans d'autres domaines et que l'authentification SSO est possible même lorsque des domaines différents sont concernés.

L'avantage des identités fédérées pour les fournisseurs SP est qu'ils peuvent traiter un plus petit nombre d'informations concernant les entités. Les méthodes de la Kantara Initiative [b-Kantara], de Shibboleth [b-Shibboleth] et de Higgins [b-Higgins] appliquent la gestion IdM fédérée. Dans le cadre des méthodes utilisant des identités fédérées, les identités sont réparties entre différents fournisseurs IdSP et tous les autres tiers (fournisseurs IdSP) appartenant à la fédération peuvent avoir accès aux informations sur les entités.

7 Architectures et flux pour les méthodes d'agrégation d'attributs

Les premiers travaux menés sur le regroupement d'attributs provenant de multiples autorités reposaient sur l'hypothèse que l'entité avait un identificateur unique au niveau mondial qui était commun pour toutes les autorités d'attributs. Dans la pratique, les entités n'ont pas d'identificateur mondial, mais elles ont différents identificateurs et attributs d'entité assignés par leurs différents fournisseurs IdSP.

La Liberty Alliance [b-Liberty], qui est ensuite devenue la Kantara Initiative [b-Kantara], a été le premier groupe à traiter la question de l'agrégation d'attributs, avec son concept de fédération d'identités [b-Chadwick]. Toutefois, elle n'a pas résolu le problème de l'absence de méthode normalisée d'agrégation d'attributs d'entité, validés par de multiples autorités, que les fournisseurs SP utiliseraient pour prendre des décisions en matière de contrôle d'accès.

Plusieurs cas d'utilisation peuvent être utiles pour comprendre pourquoi l'agrégation d'attributs est nécessaire:

– Si une librairie électronique prévoit une opération commerciale à l'intention des seniors, l'ensemble agrégé d'attributs (données de carte de crédit et preuve du statut de senior) provenant de multiples fournisseurs IdSP doit lui être communiqué. En l'espèce, une entité doit fournir les attributs pour deux identités.

– Prenons le cas d'un chercheur qui souhaite acheter un ordinateur en utilisant un compte bancaire fédéré, sur un site en ligne qui accorde des réductions aux personnes du secteur de l'éducation. Le chercheur doit apporter la preuve qu'il est membre d'une structure d'enseignement et qu'il est titulaire d'un compte dans sa banque. Les attributs stockés dans de multiples entités distinctes doivent être réunis et le résultat de cette réunion devrait être transmis à un fournisseur SP; ce processus est appelé agrégation d'attributs [b-Klingenstein].

Le partage et l'utilisation coordonnée de ressources au sein de communautés dynamiques composées de multiples institutions sont essentiels pour des applications informatiques de plus en plus diverses, dans des domaines allant de la collaboration scientifique aux soins de santé. Ce partage doit nécessairement faire l'objet d'un contrôle strict. Il est nécessaire que les fournisseurs de ressources et les consommateurs définissent de manière claire et rigoureuse les informations qui sont partagées, les entités autorisées à les partager et les conditions selon lesquelles elles sont partagées. L'ensemble des personnes ou institutions défini dans le cadre de ces règles de partage constitue ce que l'on appelle une collaboration virtuelle (VC). La mise en place d'une autogestion afin que les collaborations virtuelles soient en mesure de créer et de gérer facilement les membres et les rôles dans leurs propres groupes; ainsi que les contrôles d'accès pour leurs propres ressources est une tâche délicate, en particulier lorsque ces ressources partagées sont hébergées par de multiples institutions. Dans un scénario de collaboration virtuelle, le fournisseur IdSP fédéré ne peut généralement pas fournir tous les attributs dont ont besoin les fournisseurs SP participants. Ces attributs relatifs à la collaboration virtuelle, le nom de la collaboration, le statut des membres, la liste de diffusion, etc., doivent être agrégés à partir d'autres sources. Plusieurs autorités d'attribut distinctes doivent participer à la gestion des attributs d'utilisateur [b-Hulsebosch].

Il existe plusieurs méthodes de fédération des identités: le langage de balisage d'assertion de sécurité (SAML), les méthodes de Shibboleth [b-Shibboleth], de la Web Services-Federation [b-WS-Federation], de la Kantara Initiative [b-Kantara], l'identité ouverte [b-OpenID], l'authentification ouverte [b-OAuth], les méthodes CardSpace [b-CardSpace], Higgins Project [b-Higgins], etc. Les méthodes d'agrégation d'attributs pourraient être réparties en trois catégories, selon que le processus dans son ensemble est géré par le fournisseur IdSP, par le fournisseur SP ou par l'entité.

7.1 Gestion par le fournisseur de service d'identité

7.1.1 Association d'identités

Une méthode élaborée par la Liberty Alliance est l'une des premières à traiter le problème de l'agrégation d'attributs grâce à son concept de fédération d'identité, voir la Figure 1 [b-Liberty]. Dans la Figure 1, le fournisseur IdSP autorise l'entité à créer un lien d'homologues (CoT3) entre deux fournisseurs IdSP. Lorsqu'une entité passe d'un service à un autre, le premier fournisseur IdSP (IdSP1 dans la Figure 1) demande à cette entité si elle souhaite fédérer ce fournisseur IdSP (IdSP1) avec un autre fournisseur IdSP (IdSP2). A ce stade, les deux fournisseurs IdSP interagissent mutuellement pour créer un indicateur d'association. Lors de l'accès aux services d'un fournisseur SP, un fournisseur IdSP fournit cet indicateur d'association au fournisseur SP, avec l'assertion contenant les attributs. Le fournisseur SP peut utiliser cet indicateur pour extraire une autre assertion contenant les attributs de l'autre fournisseur IdSP. En combinant les attributs des deux fournisseurs IdSP, le fournisseur SP peut établir si l'entité peut accéder à un service.

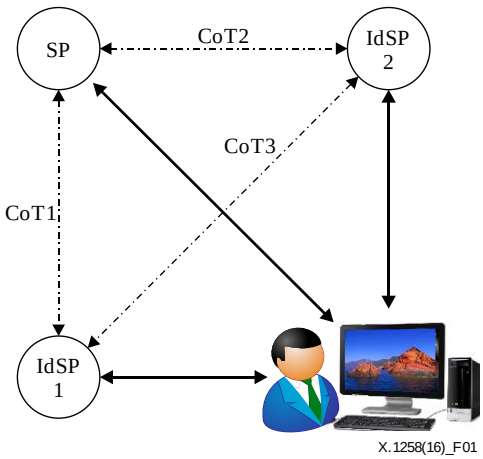

Figure 1 – Architecture de la méthode par association d'identités

La Figure 2 montre un flux théorique de contrôle de l'agrégation d'attributs selon la méthode par association d'identités:

1) Une entité envoie une demande de service à un fournisseur SP.
2) Lorsque le fournisseur SP a besoin d'une permission pour fournir le service à l'entité, il envoie une demande d'authentification et une demande d'assertion d'authentification.
3) L'entité est redirigée vers le fournisseur IdSP 1 en vue de l'authentification.
4) Le fournisseur IdSP 1 authentifie l'entité et demande des attributs supplémentaires.
5) Le fournisseur IdSP 1 renvoie l'assertion d'authentification.
6) L'entité soumet une assertion d'authentification au fournisseur SP.
7) Le fournisseur SP demande des attributs supplémentaires concernant l'entité au fournisseur IdSP 2.
8) Le fournisseur IdSP 2 fournit l'attribut supplémentaire.
9) Le fournisseur SP vérifie les assertions et autorise l'entité à accéder aux services.

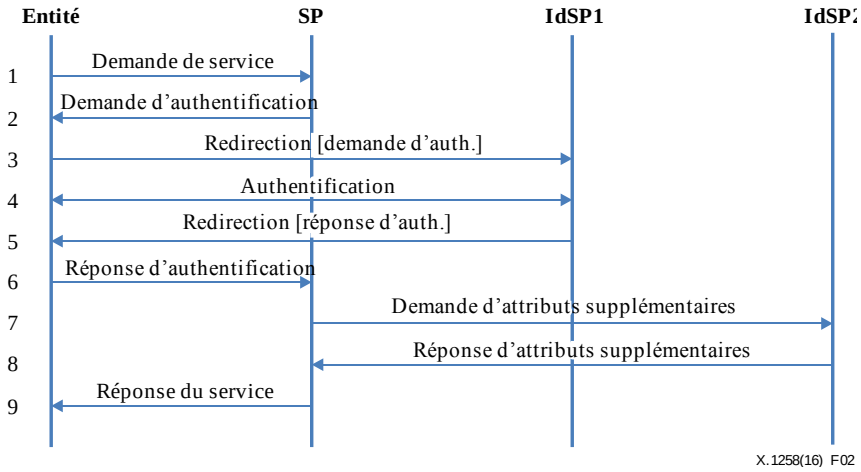

Figure 2 – Flux d'agrégation d'attributs selon la méthode par association d'identités

7.1.2 Mandataire d'identité

Il existe un fournisseur IdSP mandataire avec lequel un fournisseur SP dispose d'une connexion dans laquelle il a entièrement confiance; d'autres fournisseurs IdSP, qui sont inconnus du fournisseur SP, ont une relation de confiance uniquement avec le fournisseur IdSP mandataire (IdSP 1), voir la Figure 3 [b-Klingenstein]. Si l'entité souhaite agréger des attributs provenant de plusieurs fournisseurs IdSP, elle est redirigée tout d'abord vers le fournisseur IdSP mandataire (IdSP 1 dans la Figure 3), puis le fournisseur IdSP mandataire redirige l'entité vers plusieurs autres fournisseurs IdSP. Après que l'entité s'est authentifiée séparément auprès de chaque fournisseur IdSP, elle renvoie une assertion au fournisseur IdSP mandataire. Le fournisseur IdSP mandataire vérifie ensuite chaque assertion, extrait les attributs auprès des fournisseurs IdSP et agrège tous ces attributs. Le fournisseur IdSP mandataire peut ensuite remplir l'ensemble agrégé des attributs d'entité qu'il émet lui-même et valider à nouveau les assertions. Après cela, le fournisseur IdSP mandataire envoie toutes les assertions d'attribut revalidées au fournisseur SP. Le fournisseur SP établit ensuite si l'entité peut accéder au service sur la base des attributs agrégés. Etant donné que le fournisseur SP ne sait pas qu'il y a d'autres fournisseurs IdSP et a uniquement une relation avec le fournisseur IdSP mandataire, il part du principe que tous les attributs ont été émis par le fournisseur IdSP mandataire.

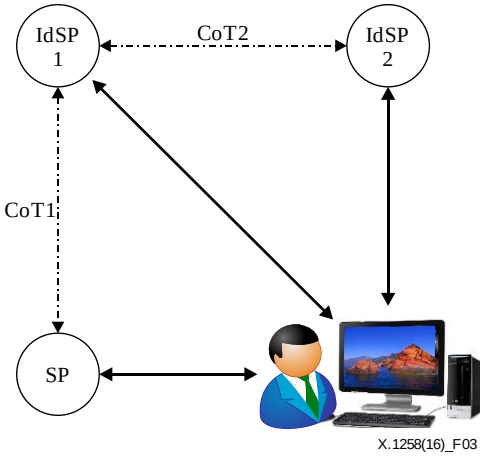

Figure 3 – Architecture de la méthode avec mandataire d'identité

La Figure 4 montre un flux théorique de contrôle de l'agrégation d'attributs selon la méthode avec mandataire d'identité:

1) L'entité envoie une demande de service au fournisseur SP.

2) Lorsque le fournisseur SP a besoin d'une permission pour fournir le service à l'entité, il envoie une demande d'authentification et une demande d'assertion d'authentification.

3) L'entité est redirigée vers le fournisseur IdSP 1 (mandataire) en vue de l'authentification.

4) Le fournisseur IdSP 1 redirige l'entité vers le fournisseur IdSP 2.

5) Le fournisseur IdSP 2 reçoit une demande d'authentification et une demande d'attribut.

6) Le fournisseur IdSP 2 authentifie l'entité.

7) Le fournisseur IdSP 2 renvoie le résultat de l'authentification et les assertions d'attribut.

8) L'entité fait suivre le résultat de l'authentification et les assertions d'attribut au fournisseur IdSP 1.

9) Le fournisseur IdSP 1 ajoute des attributs supplémentaires, signe les assertions et les renvoie à l'entité.

10) L'entité soumet les assertions au fournisseur SP.

11) Le fournisseur SP vérifie les assertions et autorise l'entité à accéder au service.

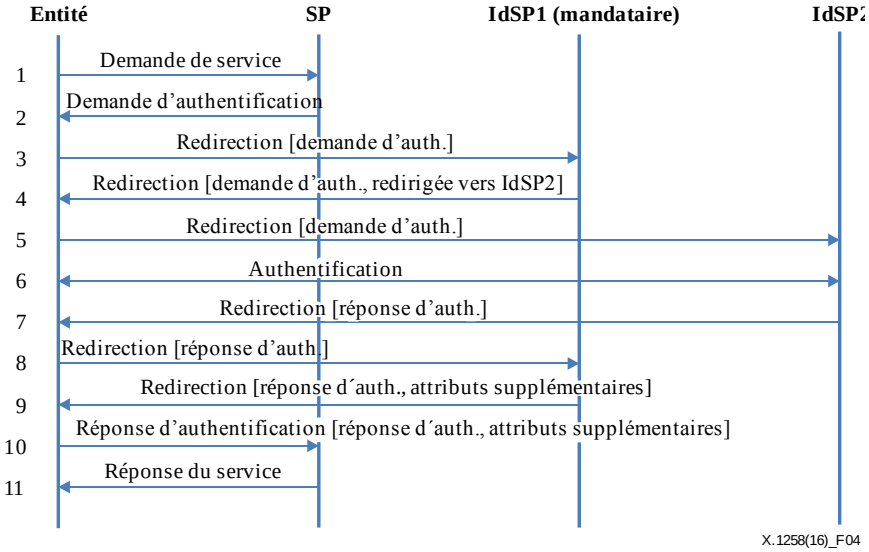

Figure 4 – Flux d'agrégation d'attributs selon la méthode avec mandataire d'identité

7.1.3 Relais d'identité

La méthode avec relais d'identité est analogue à la méthode avec mandataire, mais ne nécessite pas une confiance forte entre un fournisseur SP et un fournisseur IdSP mandataire. La méthode avec mandataire exige que le fournisseur SP ait une confiance totale dans le fournisseur IdSP de confiance, mais, dans la pratique, il risque d'être impossible de garantir une confiance absolue entre le fournisseur IdSP mandataire et le fournisseur SP. Dans le cadre de la méthode avec relais d'identité, un fournisseur IdSP intermédiaire (ou fournisseur IdSP relais) (IdSP1 dans la Figure 5) peut agir comme un fournisseur IdSP mandataire. Le flux est ensuite analogue à celui pour la méthode avec mandataire, l'entité est tout d'abord redirigée vers le fournisseur IdSP relais, puis le fournisseur IdSP relais redirige l'entité vers plusieurs autres fournisseurs IdSP. Après que l'entité s'est authentifiée séparément auprès de chaque fournisseur IdSP, elle renvoie une assertion au fournisseur IdSP relais. Après cela, le fournisseur IdSP relais regroupe toutes les assertions en une assertion unique qu'elle transmet au fournisseur SP. La différence entre le modèle avec mandataire et le modèle avec relais concerne la signature des assertions d'attribut. Le fournisseur IdSP relais ne signe pas les assertions d'attribut, mais ne fait que relayer les assertions signées par le fournisseur IdSP d'origine. Le fournisseur SP reçoit ensuite les assertions d'attribut chiffrées provenant des fournisseurs IdSP et du fournisseur IdSP relais et établit si l'entité peut accéder au service sur la base des attributs agrégés. Cette méthode nécessite une relation de confiance entre les fournisseurs IdSP et le fournisseur SP.

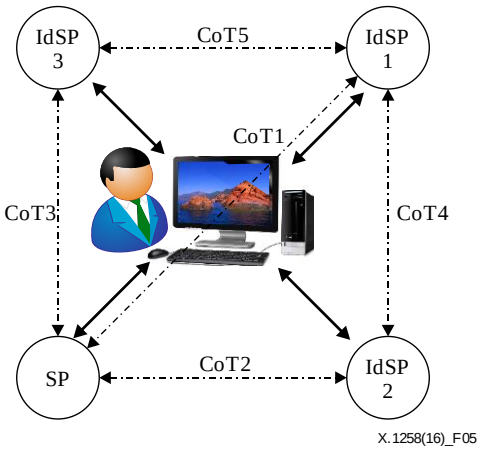

Figure 5 – Architecture de la méthode avec relais d'identité

La Figure 6 montre un flux théorique de contrôle de l'agrégation d'attributs selon la méthode avec relais identité:

1) L'entité envoie une demande de service au fournisseur SP.
2) Lorsque le fournisseur SP a besoin d'une permission pour fournir le service à l'entité, il envoie une demande d'authentification et une demande d'assertion d'authentification.
3) L'entité est redirigée vers le fournisseur IdSP 1 (relais) en vue de l'authentification.
4) Le fournisseur IdSP 1 redirige l'entité vers le fournisseur IdSP 2.
5) Le fournisseur IdSP 2 reçoit une demande d'authentification et une demande d'attribut.
6) Le fournisseur IdSP 2 authentifie l'entité.
7) Le fournisseur IdSP 2 renvoie le résultat de l'authentification et les assertions d'attribut.
8) L'entité fait suivre le résultat de l'authentification et les assertions d'attribut au fournisseur IdSP 1.
9) Le fournisseur IdSP 1 ajoute des attributs supplémentaires, signe les assertions et les renvoie à l'entité.
10) L'entité soumet les assertions au fournisseur SP.
11) Le fournisseur SP vérifie les assertions et autorise l'entité à accéder au service.

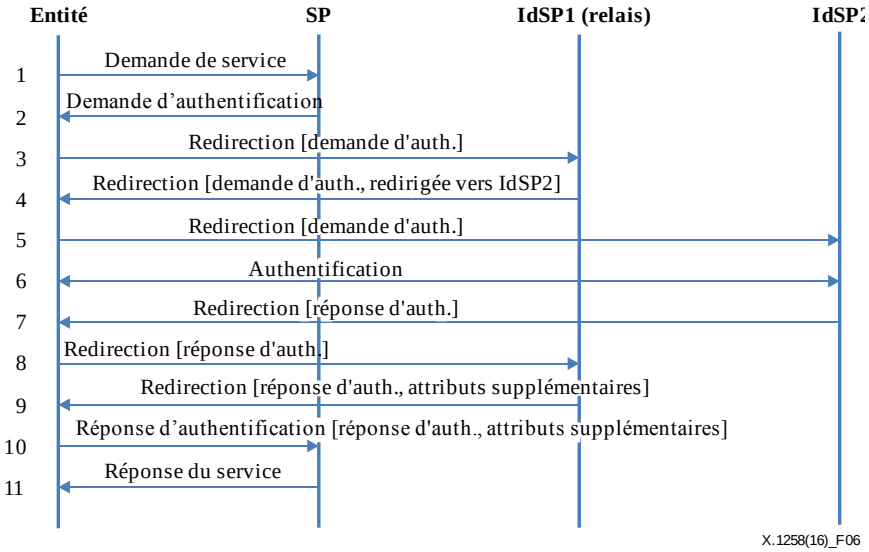

Figure 6 – Flux d'agrégation d'attributs selon la méthode avec relais l'identité

7.2 Gestion par le fournisseur de services

7.2.1 Base de données d'applications

La méthode avec base de données (DB) d'applications est la méthode d'agrégation d'attributs la plus simple, voir la Figure 7 [b-Hulsebosch]. Le fournisseur SP conserve des attributs d'entité supplémentaires, un surnom, les préférences de l'entité pour le service concerné, les membres du groupe, etc., en plus des attributs fournis par le fournisseur IdSP. Le fournisseur SP gère les attributs ajoutés pour les applications. En outre, ces attributs contenus dans sa base de données peuvent être extraits ultérieurement pour permettre au fournisseur SP d'établir si l'entité peut accéder à un service donné.

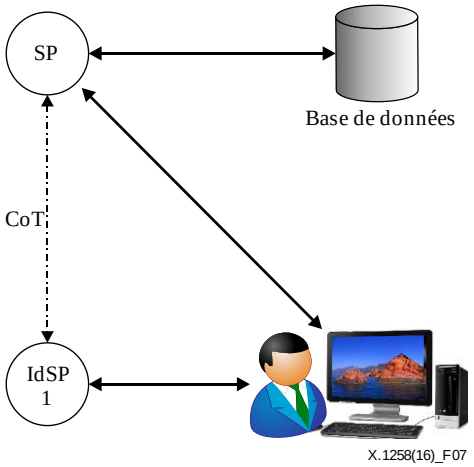

Figure 7 – Architecture de la méthode avec base de données d'applications

La Figure 8 montre un flux théorique de contrôle de l'agrégation d'attributs selon la méthode avec base de données d'applications:

1) L'entité envoie une demande de services au fournisseur SP.
2) Lorsque le fournisseur SP a besoin d'une permission pour fournir le service à l'entité, il envoie une demande d'authentification et une demande d'assertion d'authentification.
3) L'entité est redirigée vers le fournisseur IdSP 1 en vue de l'authentification.
4) Le fournisseur IdSP 1 authentifie l'entité.
5) Une fois l'authentification menée à bien, le fournisseur IdSP 1 renvoie le résultat de l'authentification et l'assertion d'authentification.
6) L'entité soumet l'assertion d'authentification au fournisseur SP.
7) Le fournisseur SP extrait des attributs d'entité supplémentaires de sa base de données, au besoin.
8) Le fournisseur SP vérifie la ou les assertions et autorise l'entité à accéder au service.

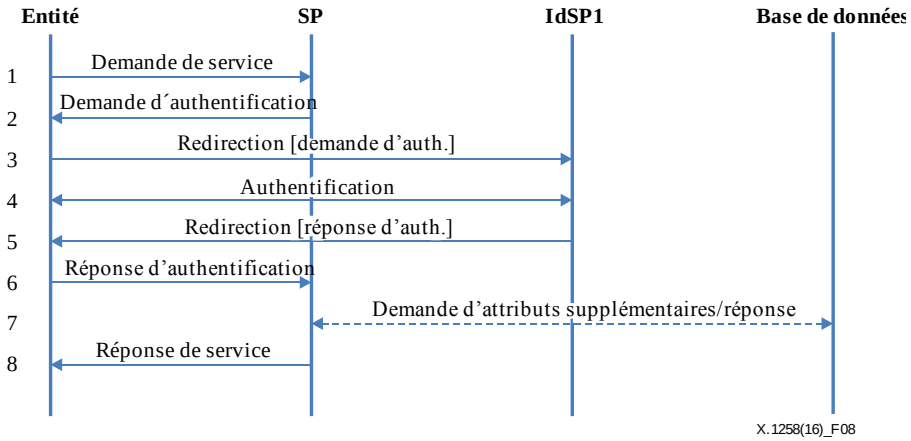

Figure 8 – Flux d'agrégation des attributs selon la méthode avec base de données d'applications

7.2.2 Fournisseur de services

La méthode reposant sur le fournisseur SP permet à l'entité d'agréger des attributs provenant de multiples fournisseurs IdSP dans une session unique, voir la Figure 9 [b- Hulsebosch]. L'entité est redirigée vers différents fournisseurs IdSP successifs, qui authentifient l'entité séparément et renvoient une assertion d'attribut au fournisseur SP. Le fournisseur SP agrège les assertions d'attribut transmises par les fournisseurs IdSP et établit si l'entité peut accéder à un service donné.

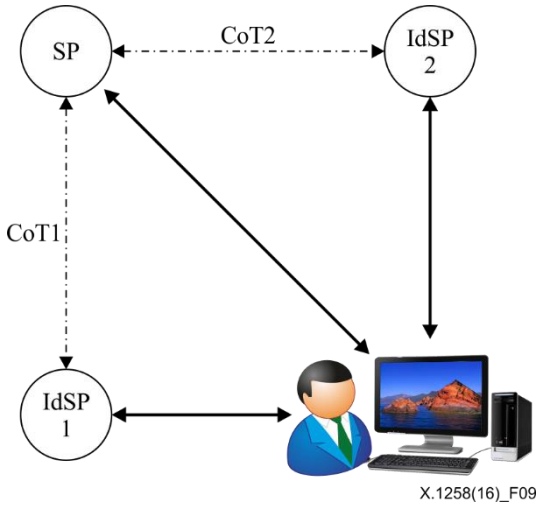

Figure 9 – Architecture de la méthode reposant sur le fournisseur de services

La Figure 10 montre un flux théorique de contrôle de l'agrégation d'attributs selon la méthode SP:

1) L'entité envoie une demande de service au fournisseur SP.
2) Lorsque le fournisseur SP a besoin d'une permission pour fournir le service à l'entité, il envoie une demande d'authentification et une demande d'assertion d'authentification.
3) L'entité est redirigée vers le fournisseur IdSP 1 en vue de l'authentification.
4) Le fournisseur IdSP 1 authentifie l'entité.
5) Le fournisseur IdSP 1 renvoie le résultat de l'authentification et l'assertion d'authentification.
6) L'entité soumet l'assertion d'authentification au fournisseur SP.
7) Le fournisseur SP demande à l'entité des attributs supplémentaires la concernant.
8) L'entité envoie des demandes d'attribut supplémentaire au fournisseur IdSP 2.
9) Le fournisseur IdSP 2 authentifie l'entité.

10) Le fournisseur IdSP 2 fournit les attributs supplémentaires.

11) L'entité soumit les assertions d'authentification au fournisseur SP.

12) Le fournisseur SP vérifie la ou les assertions et autorise l'entité à accéder au service.

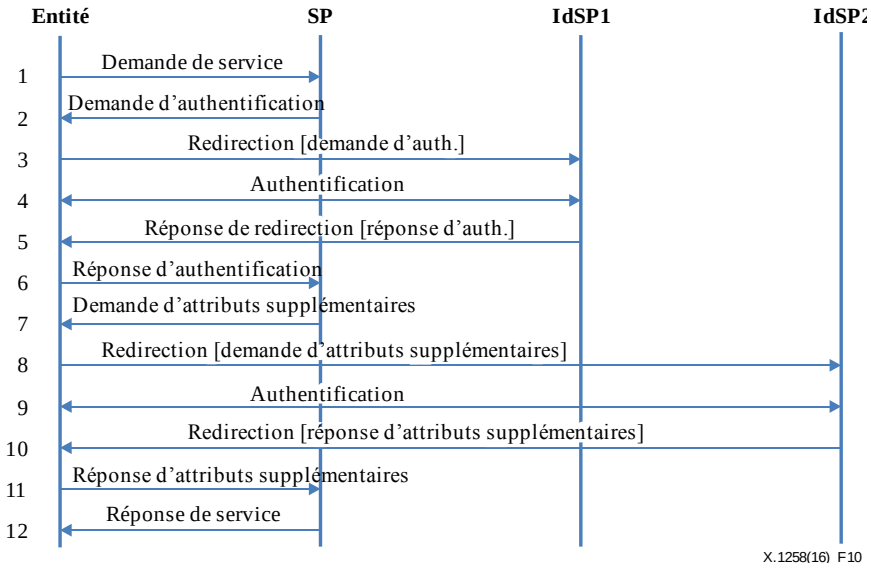

Figure 10 – Flux d'agrégation d'attributs selon la méthode reposant sur le fournisseur de services

7.2.3 Service d'association

La méthode avec service d'association (LS) est une combinaison de la méthode avec association d'identités et de la méthode avec relais d'identité. Le service LS correspond à un type particulier de fournisseur SP (voir la Figure 11), auquel a recours l'entité grâce à un identificateur fourni par le service LS [b-Chadwick], [b-Hulsebosch]. Cet identificateur sert à associer différents fournisseurs IdSP utilisant des identificateurs persistants propres au service LS fournis par des fournisseurs IdSP dans un tableau appelé tableau d'association. Si une entité veut accéder à un service, elle s'adresse au fournisseur SP qui la redirige vers le premier fournisseur IdSP (IdSP 1 dans la Figure 11). L'entité est authentifiée auprès du fournisseur IdSP 1, puis une assertion contenant des attributs d'entité, ainsi que l'identificateur pour le service LS sont renvoyés au fournisseur SP par l'intermédiaire de l'entité. Le fournisseur SP fait suivre l'identificateur au service LS afin d'obtenir des attributs supplémentaires. A ce stade, deux options sont possibles: le service LS peut extraire la liste des fournisseurs IdSP associés pour cet identificateur persistant en utilisant le tableau d'association et extraire les attributs auprès de chacun d'entre eux, attributs qui sont ensuite regroupés au niveau du service LS et renvoyés au fournisseur SP, ou le service LS peut renvoyer la liste des fournisseurs IdSP associés au fournisseur SP. Le fournisseur SP extrait ensuite les attributs fournis par chaque fournisseur IdSP. Enfin, le fournisseur SP établit si l'entité peut accéder au service sur la base des attributs agrégés

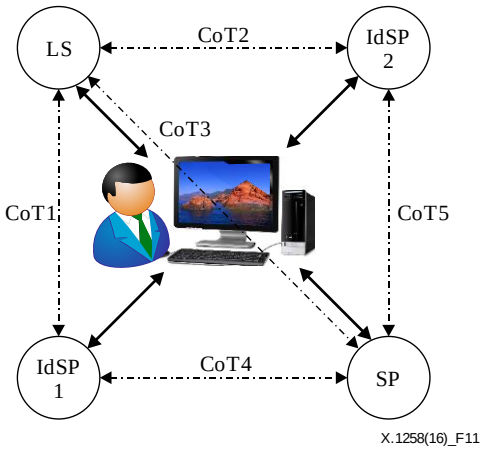

Figure 11 – Architecture de la méthode avec service d'association

La Figure 12 montre un flux théorique de contrôle de l'agrégation d'attributs selon la méthode LS:

1) L'entité envoie une demande de service au fournisseur SP.
2) Lorsque le fournisseur SP a besoin d'une permission pour fournir le service à l'entité, il envoie une demande d'authentification et une demande d'assertion d'authentification.
3) L'entité est redirigée vers le fournisseur IdSP 1.
4) Le fournisseur IdSP 1 authentifie l'entité.
5) Le fournisseur IdSP 1 renvoie une assertion d'authentification et l'identificateur pour le service LS.
6) L'entité soumet l'assertion et l'identificateur pour le service LS au fournisseur SP.
7) Le fournisseur SP envoie des demandes d'attribut supplémentaire à l'entité.
8) L'entité est redirigée vers le service LS.
9) Le service LS demande des attributs au fournisseur IdSP 2.
10) Le fournisseur IdSP 2 fournit les attributs.
11) Les attributs sont renvoyés à l'entité.
12) L'entité soumet la ou les assertions d'authentification au fournisseur SP.
13) Le fournisseur SP vérifie la ou les assertions et autorise l'entité à accéder au service.

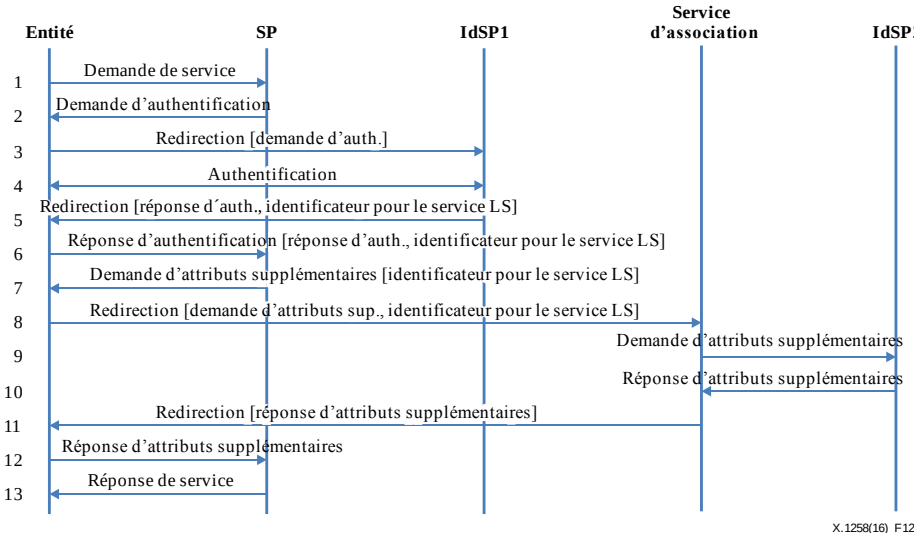

Figure 12 – Flux d'agrégation d'attributs selon la méthode avec service d'association

7.3 Gestion par l'entité

La méthode gérée par l'entité fait appel à un client (l'entité-agent ou application) qui a la capacité d'agréger des attributs provenant de différents fournisseurs IdSP, voir la Figure 13 [b-Klingenstein] et [b-Hulsebosch]. Le fournisseur SP communique au client la liste des fournisseurs IdSP de confiance. Le client redirige l'entité vers chacun de ces fournisseurs IdSP. A l'issue de l'authentification auprès de chaque fournisseur IdSP, le client reçoit des assertions envoyées par tous les fournisseurs IdSP et présente au fournisseur SP l'ensemble des assertions regroupées. Le fournisseur SP vérifie chaque assertion, extrait tous les attributs et établit ensuite si l'entité peut accéder au service.

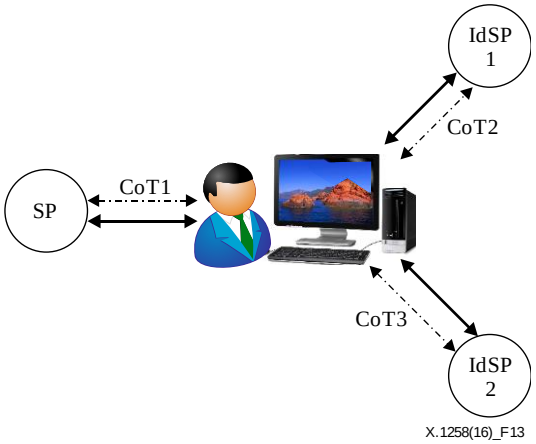

Figure 13 – Architecture de la méthode avec client

La Figure 14 montre un flux théorique de contrôle de l'agrégation d'attributs selon la méthode avec client:

1) L'entité envoie une demande de service au fournisseur SP.
2) Lorsque le fournisseur SP a besoin d'une permission pour fournir le service à l'entité, il envoie une demande d'authentification et une demande d'assertion d'authentification.
3) Le fournisseur IdSP 1 authentifie l'entité.
4) Le fournisseur IdSP 1 renvoie l'assertion d'authentification.
5) L'entité est redirigée vers le fournisseur IdSP 2 pour des assertions d'attribut supplémentaire.
6) Le fournisseur IdSP 2 authentifie l'entité.
7) Le fournisseur IdSP 2 renvoie la ou les assertions d'attribut.
8) L'entité soumet la ou les assertions d'authentification au fournisseur SP.
9) Le fournisseur SP vérifie la ou les assertions et autorise l'entité à accéder au service.

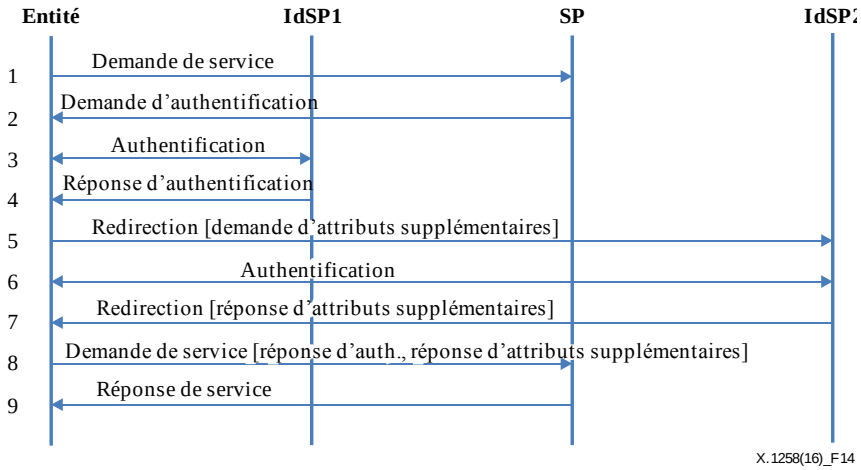

Figure 14 – Flux d'agrégation d'attributs selon la méthode avec client

8 Comparaison des méthodes d'authentification avec agrégation

Les sept méthodes présentées dans le paragraphe 7 sont de nouvelles solutions mises au point à partir du système classique de gestion IdM fédérée. Chacune de ces méthodes comprend des entités ou des interactions supplémentaires. Sur la base de ces modifications, les sept méthodes peuvent être analysées et comparées selon différents facteurs afin de sélectionner la méthode d'agrégation qui convient. Les concepteurs et développeurs devraient tenir compte de plusieurs aspects comme: qui gère/agrège/vérifie les attributs, la difficulté de mise en oeuvre ou l'ajout de nouveaux éléments.

Le paragraphe 7 présente plusieurs méthodes d'agrégation d'attributs fondées sur le langage SAML. Ces méthodes pourraient être interopérables selon la façon dont elles sont exprimées en SAML.

Les méthodes d'agrégation sont analysées du point de vue de la gestion de l'agrégation, de la mise en oeuvre de l'agrégation et d'autres éléments. Une comparaison des méthodes d'agrégation est présentée dans le Tableau 1.

Dans le Tableau 1, lorsqu'une cellule est cochée "✓", cela signifie que la méthode d'agrégation indiquée sur la ligne a la capacité indiquée dans la colonne. Plus précisément, la capacité en question devrait être prise en charge par la mise en oeuvre de la méthode indiquée.

Tableau 1 – Comparaison des méthodes d'agrégation

Méthode d'agrégation	**Capacité**						
	Gestion par le fournisseur IdSP	**Gestion par le fournisseur SP**	**Gestion par le client**	**Agrégation par le fournisseur IdSP**	**Agrégation par le fournisseur SP**	**Agrégation par le client**	**Elément supplémentaire**
Association d'identités	✓				✓		
Mandataire d'identité	✓			✓			
Relais d'identité	✓			✓			
Base de données d'applications		✓			✓		DB
Fournisseur de services		✓			✓		
Service d'association		✓			✓		LS
Client			✓			✓	client

En ce qui concerne la méthode par association d'identités, l'agrégation est gérée par le fournisseur IdSP et mise en oeuvre au niveau du fournisseur SP. Cela signifie que le protocole d'agrégation des attributs devrait être mis en oeuvre au niveau du fournisseur IdSP et du fournisseur SP. En revanche, pour les autres méthodes, la gestion et la mise en oeuvre de l'agrégation peuvent être assurées au niveau du même fournisseur. Il pourrait être plus facile pour le fournisseur d'effectuer l'agrégation d'attributs plutôt que d'appliquer la méthode par association d'identités. S'agissant des éléments supplémentaires pour l'agrégation d'attributs, la méthode avec base de données d'applications nécessite une base de données dédiée; la méthode avec service d'association nécessite un service d'association (LS) en tant que type particulier de fournisseur SP; la méthode gérée par l'entité nécessite un client en tant qu'agent. Sur la base de ces critères, il est recommandé d'utiliser la méthode avec mandataire d'identité et la méthode avec relais d'identité dans le cas d'une gestion par le fournisseur IdSP, tandis que dans le cas d'une gestion par le fournisseur SP, il est recommandé d'utiliser la méthode SP.

Bibliographie

[b-UIT-T X.500] Recommandation UIT-T X.500 (2016) | ISO/CEI 9594-1:2017, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: aperçu général des concepts, modèles et services*.

[b-UIT-T X.509] Recommandation UIT-T X.509 (2016) | ISO/CEI 9594-8:2017, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: Cadre général des certificats de clé publique et d'attribut*.

[b-UIT-T X.1251] Recommandation UIT-T X.1251 (2009), *Cadre régissant le contrôle par l'utilisateur des identités numériques*.

[b-UIT-T X.1252] Recommandation UIT-T X.1252 (2010), *Termes et définitions de base relatifs à la gestion d'identité*.

[b-CardSpace] *Introducing windows cardspace*. MSDN technical articles, Microsoft Corporation.
Disponible (vu le 19-12-2016) à l'adresse: http://msdn.microsoft.com/en-us/library/aa480189.aspx.

[b-Chadwick] Chadwick, D.W., Inman, G. (2009). Attribute aggregation in federated identity management. *IEEE Computer*, **42**(5), pp. 33–40.
<http://doi.ieeecomputersociety.org/10.1109/MC.2009.143>

[b-Higgins] Higgins, *Project.*
Disponible (vu le 05-12-2016) à l'adresse: <http://www.eclipse.org/higgins/>

[b-Hulsebosch] Hulsebosch, B., Wegdam, M., Zoetekouw, B., van Dijk, N,, Poortinga-van Wijnen, R. (2012), Virtual collaboration attribute management. 41 pp. Disponible (vu le 05-12-2016) à l'adresse:
<https://www.surf.nl/binaries/content/assets/surf/en/knowledgebase/2012/EDS+11-06+Attribute+Management+v1.0.pdf >

[b-Kantara] Kantara, *Initiative*
Disponible (vu le 19-12-2016) à l'adresse: https://kantarainitiative.org/reports-recommendations/

[b-Klingenstein] Klingenstein, N. (2007). Attribute aggregation and federated identity. In: *Proceedings of the 2007 International Symposium on Applications and the Internet Workshops (SAINTW'07)*, p. 26–29.

[b-Liberty] Liberty Alliance, *ID-FF 1.2 Specifications*, Disponible (vu le 05-12-2016) à l'adresse:
<http://www.projectliberty.org/liberty/resource_center/specifications/liberty_alliance_id_ff_1_2_specifications

[b-OAuth] OAuth.
Disponible (vu le 19-12-2016) à l'adresse: http://oauth.net/documentation/getting-started/

[b-OpenID] OpenID authentication 2.0.
Disponible (vu le 19-12-2016) à l'adresse: http://openid.net/specs/openid-authentication-2_0.html

[b-Shibboleth] Shibboleth Consortium, *Open Source Project*.
Disponible (vu le 05-12-2016) à l'adresse: <https://shibboleth.net/>

[b-WS-Federation] Web Services Federation Language (WS-Federation) Version 1.2.
Disponible (vu le 19-12-2016) à l'adresse: http://docs.oasis-open.org/wsfed/federation/v1.2/os/ws-federation-1.2-spec-os.html

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	**Organisation du travail de l'UIT-T**
Série D	Principes de tarification et de comptabilité et questions de politique générale et d'économie relatives aux télécommunications internationales/TIC
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Environnement et TIC, changements climatiques, déchets d'équipements électriques et électroniques, efficacité énergétique, construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Terminaux et méthodes d'évaluation subjectives et objectives
Série Q	Commutation et signalisation et mesures et tests associés
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	Réseaux de données, communication entre systèmes ouverts et sécurité
Série Y	Infrastructure mondiale de l'information, protocole Internet, réseaux de prochaine génération, Internet des objets et villes intelligentes
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2017