



(12) BREVET D'INVENTION

(11) N° de publication :
MA 39243 A1

(51) Cl. internationale :
H04L 12/56

(43) Date de publication :
30.03.2018

(21) N° Dépôt :
39243

(22) Date de Dépôt :
01.08.2016

(71) Demandeur(s) :
Université Mohammed V Rabat, Avenue des Nations Unies, Agdal, bp 8007 NU Rabat, 10000 (MA)

(72) Inventeur(s) :
ECH-CHERIF EL Kettani Mohamed Dafir ; el haddouti samia

(74) Mandataire :
FATIMA ZAOUI

(54) Titre : **Un modèle flexible et interopérable d'agrégation d'attributs pour la fédération d'identité**

(57) Abrégé : La présente invention concerne un nouveau modèle flexible qui vise à fournir les mécanismes nécessaires pour assurer l'agrégation d'attributs afin de relever les défis de l'interopérabilité pour les systèmes de la gestion d'identité actuels. Le modèle proposé est une solution modulaire basée sur les technologies de la fédération d'identité et introduit un nouveau composant appelé Fournisseur de Liaison de Comptes (en abrégé, ALP, pour Account Linking Provider). Ce dernier joue le rôle d'une passerelle entre les Fournisseurs de Service et les Fournisseurs d'identité permettant à un utilisateur final, disposant de plusieurs comptes auprès de plusieurs Fournisseurs d'identité, de fédérer ses identités et d'agréger ses attributs tout en améliorant les relations de confiance entre les différentes parties prenantes et en respectant les concepts de la sécurité et de la vie privée.

Abrégé :

La présente invention concerne un nouveau modèle flexible qui vise à fournir les mécanismes nécessaires pour assurer l'agrégation d'attributs afin de relever les défis de l'interopérabilité pour les systèmes de la gestion d'identité actuels. Le modèle proposé est une solution modulaire basée sur les technologies de la fédération d'identité et introduit un nouveau composant appelé Fournisseur de Liaison de Comptes (en abrégé, ALP, pour Account Linking Provider). Ce dernier joue le rôle d'une passerelle entre les Fournisseurs de Service et les Fournisseurs d'Identité permettant à un utilisateur final, disposant de plusieurs comptes auprès de plusieurs Fournisseurs d'Identité, de fédérer ses identités et d'agréger ses attributs tout en améliorant les relations de confiance entre les différentes parties prenantes et en respectant les concepts de la sécurité et de la vie privée.

Titre : Un modèle flexible et interopérable d'agrégation d'attributs pour la fédération d'identité

Description

La présente invention se rapporte à un système de la gestion d'identité numérique flexible pour supporter de nouveaux scénarios qui nécessitent des attributs des utilisateurs gérés par différentes autorités d'attributs après une seule et unique authentification auprès d'un tiers de confiance

L'état de l'art :

Lors du fonctionnement typique d'un système de la gestion d'identité, l'utilisateur final, via son navigateur web, tente d'accéder à une ressource web gérée par un Fournisseur de Service (en abrégé, SP ou RP, pour Service Provider or Relying Party) et ce dernier redirige l'utilisateur vers son Un Fournisseur d'Identité (en abrégé, IdP, pour Identity Provider) pour l'authentification. Si l'utilisateur a été authentifié avec succès, l'IdP envoie une assertion d'authentification au SP. Avant d'accorder l'accès à la ressource, le SP envoie une requête de demande des attributs auprès de l'IdP. En se basant sur les informations reçues, le SP peut alors effectuer le contrôle d'accès puis retourner une réponse au navigateur. De cette manière les technologies et les bonnes pratiques des systèmes de la gestion d'identité facilitent l'accès aux services applicatifs et fidélisent l'utilisateur en lui évitant des contraintes d'inscriptions ou d'authentifications répétitives tout en sécurisant les échanges entre toutes les parties prenantes (E. Bertino et al, 2011).

En contrepartie des avantages des systèmes de la gestion d'identité cités ci-dessus, les modèles actuels disposent des limitations en supposant que l'utilisateur ne peut sélectionner qu'un seul IdP dans une session donnée avec un SP pour fournir tous les attributs requis afin d'accéder à la ressource demandée. Cependant, la plupart des utilisateurs disposent de plusieurs comptes et des attributs sur différents IdPs (Facebook, Gmail, Twitter, IdP de son établissement de rattachement...). Plusieurs scénarios peuvent être envisagés pour justifier la nécessité de récupérer des informations et des attributs gérés par différentes autorités d'attributs en s'authentifiant une seule fois. Par exemple, pour payer la réservation d'une chambre d'hôtel en ligne, l'utilisateur a besoin de présenter sa carte bancaire et sa carte de fidélité tout en obtenant un surclassement de chambre et en gagnant des points avec son compagnie aérienne. Avec les

systèmes de la gestion d'identité actuels, un SP ne peut recevoir que les attributs fournis par un seul IdP (l'utilisateur ne peut sélectionner qu'un seul IdP), alors que cette transaction nécessite des attributs fournis par trois IdPs (IdP de l'hôtel, IdP de la banque et l'IdP de la compagnie aérienne) en une seule session d'accès. Par conséquent, ces systèmes ne sont pas adéquats pour résoudre le problème que pose l'agrégation d'attributs dans ce contexte.

Pour résoudre ce problème, plusieurs approches ont été proposées pour agréger les attributs des utilisateurs en provenance de multiples IdPs (Bob Hulsebosch et al, 2011, David W. Chadwick, 2009, AlejandroPérez et al, 2011). Le modèle « Linking Service » propose une approche d'agrégation d'attributs en introduisant une entité (un SP) qui permet d'agréger les identités de l'utilisateur au niveau des différents IdPs. Cependant, ce modèle ne suit pas la conception et le fonctionnement typiques des systèmes de la fédération d'identité dans lesquelles le premier point de contact pour l'authentification de l'utilisateur final est un IdP et non pas un SP. Par conséquent, des modifications techniques importantes devraient être apportées au niveau des SPs ce qui peut rendre ce dernier démotivé à se joindre aux systèmes basés sur ce modèle. D'autre part, le « Linking Service » envoie la liste totale des IdPs disposant des comptes pour l'utilisateur final même ceux qui gèrent des attributs non demandés par le SP ce qui ne respecte pas la deuxième loi d'identité (Data Minimization). Le projet SWIFT utilise le concept d'identité virtuelle (VID) en se basant sur un IdP (IdAggr : Identity Aggregator). Cependant, la deuxième loi d'identité n'est pas respectée et les assertions des attributs sont signées par l'IdAggr ce qui cache la source originale des données au SPs. Un autre inconvénient de ce modèle est que l'authentification ne se fait pas au niveau de l'IdAggr.

La présente invention concerne un modèle et un système visant à pallier la problématique de l'interopérabilité des systèmes de management d'identité en se basant sur le principe d'agrégation d'attributs, les mécanismes de la fédération d'identité et le modèle du relais d'identité (Identity Relay) tout en réduisant au maximum ses inconvénients.

L'invention trouve avantageusement de nombreuses applications où le citoyen est invité à fournir des informations (des attributs) provenant de multiples autorités d'attribut sans nécessité de s'authentifier séparément auprès de chaque IdP, notamment dans le domaine académique, de

l'administration en ligne (E-Government), de la cybersanté (eHealth), du commerce électronique (E-Business) et de la banque électronique (E-Banking).

Notre invention propose une architecture particulièrement avantageuse dans le domaine d'agrégation d'attributs par l'introduction d'un nouveau module appelé Fournisseur de Liaison de Comptes (en abrégé, ALP, pour Account Linking Provider). L'ALP est un IdP qui joue le rôle d'une passerelle entre le SP et les IdPs permettant à un utilisateur final, disposant de plusieurs comptes auprès de plusieurs IdPs, de fédérer ses identités et d'agréger ses attributs tout en respectant les concepts de la sécurité et de la vie privée. Le processus d'agrégation d'attributs se base sur la création d'une table de liaison de comptes (Account Linking Table) en vue de faire la correspondance entre les IdPs et les attributs de l'utilisateur.

Des aspects préférés mais non limitatifs de ce modèle selon l'invention sont les suivants :

-L'accès aux ressources nécessite une seule et unique authentification auprès de l'ALP. Par conséquent, l'utilisateur n'a pas besoin d'être authentifié auprès de chaque IdP au cours d'une seule session d'accès. En outre, le système prévoit un mécanisme d'authentification unique (Single Sign-On : SSO) pour éviter la réauthentification de l'utilisateur final à chaque fois qu'il accède à un service protégé au cours d'une période de validité spécifique;

-L'utilisateur final dispose d'un contrôle complet et d'une visibilité sur la diffusion et l'utilisation de ses identités et ses attributs. D'autre part, aucun IdP ne devrait être au courant des identités de l'utilisateur final au niveau des autres IdPs, ce qui permet de renforcer la protection de la vie privée.

-Les IdPs communiquent aux ALP les identifiants des attributs (attributeID) et non pas les valeurs de ces attributs.

-La gestion des relations de confiance entre les parties prenantes est optimisée. Chaque IdP devrait avoir des relations de confiance avec le SP et avec l'ALP afin qu'ils puissent communiquer entre eux avec succès. Toutefois, les IdPs n'ont pas besoin d'avoir des relations de confiance entre eux;

-Le SP devrait savoir l'IdP qui a initialement affirmé les attributs de l'utilisateur final et toutes les assertions devraient être signées par des sources fiables. En outre, l'ALP ne communique au

SP que la liste des IdPs gérant les attributs qui sont raisonnablement nécessaires pour autoriser l'accès à la ressource demandée.

-Le modèle proposé est cohérent et en ligne avec les approches de la fédération d'identité réussies. Il utilise des protocoles standards existants en les étendant le cas échéant tout en évitant d'apporter de grandes modifications techniques au niveau des SPs qui peuvent les rendre démotivés à se joindre au système proposé.

Notre invention suit le processus de fonctionnement suivant

1- Phase d'agrégation d'attributs et de remplissage de la table de liaisons (Linking Table)

L'utilisateur final accède au portail du fournisseur ALP via son navigateur Web et une page d'accueil apparaît en lui invitant à s'authentifier. Une fois authentifié, l'ALP lance une recherche dans sa table de liaisons et deux scénarios sont envisageables :

-Si la table de liaisons ne contient pas de données relatives à l'utilisateur final, ce dernier sera invité à ajouter les comptes et les attributs qu'il souhaite agréger. Pour ce faire, l'ALP redirige l'utilisateur final vers un service de découverte qui affiche une liste prédéfinie de tous les IdPs ayant des relations de confiance avec cet ALP. Après avoir choisi un IdP, l'utilisateur est alors redirigé vers ce dernier auprès duquel en lui demandant de s'authentifier. En cas d'authentification réussie, une liste des noms de tous les attributs, gérés par cet IdP, s'affiche et l'utilisateur peut sélectionner d'une manière transparente les noms des attributs qui seront fournis par cet IdP suite aux requêtes des SPs. La liste des noms des attributs sélectionnés et l'assertion d'authentification de l'utilisateur seront envoyées vers l'ALP qui créera une entrée pour cet utilisateur dans la Table de Liaison.

L'utilisateur peut être invité à choisir un autre IdP et le processus décrit ci-dessus sera répété à nouveau.

- Dans le cas de la présence préalable de l'entrée relative à l'utilisateur final dans la Table de Liaisons, l'utilisateur peut consulter les informations relatives à ses comptes et ses attributs agrégés et il a aussi la possibilité de supprimer et d'ajouter de nouveaux comptes et attributs.

2-Phase d'accès à un Fournisseur de Service (SP)

Lorsque l'utilisateur final tente d'accéder à une ressource dont l'accès est contrôlé par un SP, un dialogue d'authentification apparaît avec une liste d'attributs nécessaires pour autoriser l'accès à

la ressource en demandant à l'utilisateur final s'il souhaite utiliser l'agrégation d'attributs avec ce service. Si l'utilisateur final choisit d'effectuer l'agrégation d'attributs, il sera redirigé vers le service de découverte des ALPs en listant tous les AIPs disposant des relations de confiance avec le SP. L'utilisateur final choisit son ALP. Ce faisant, il sera redirigé vers l'ALP choisi en lui invitant à s'authentifier. Une fois authentifié auprès du fournisseur ALP, ce dernier renvoie au SP une assertion d'authentification portant l'identifiant (uid) de l'utilisateur authentifié. Avant d'accorder l'accès à la ressource, le SP envoie une requête de demande d'attributs au fournisseur ALP qui initie un processus de recherche dans sa table de liaisons à base de l'uid de l'utilisateur final. Une fois qu'il a situé l'entrée appropriée pour cet utilisateur, l'ALP envoie une liste sélective de toutes les IdPs gérants les attributs requis. Le SP envoie des requêtes de demande d'attributs à chaque IdP avec l'uid de l'utilisateur et l'assertion d'authentification (L'utilisateur n'a pas besoin d'être authentifié à ces IdPs). Chaque IdP renvoie une réponse avec les attributs demandés et par conséquent le SP peut prendre sa décision de refuser ou d'accorder l'accès à l'utilisateur final en se basant sur les attributs reçus par tous les IdP.

Liste des Figures

La figure 1 illustre schématiquement la phase d'enregistrement pour la construction de la table de liaison de comptes de l'utilisateur en vue d'agréger ses attributs gérés par différents IdPs.

La figure 2 montre un exemple d'une table de liaison de comptes

La figure 3 décrit le processus d'accès à une ressource web contrôlée et dont l'accès nécessite un ensemble d'attributs gérés par plusieurs IdPs.

Revendications :

- 1- Un modèle d'agrégation d'attributs des utilisateurs disposant de plusieurs comptes auprès de différents Fournisseurs d'Identité (IdPs) en utilisant une seule et unique authentification dans une seule session d'accès. Ledit modèle se base sur les mécanismes de la fédération d'identité et le model du relais d'identité (Identity Relay) en introduisant un nouveau module, (un IdP) appelé Fournisseur de Liaison de Comptes (en abrégé, ALP, pour Accounts Linking Provider) avec une Table de Liaison des Comptes (Linking Table) qui illustre l'ensemble des IdPs et les attributs correspondants.
- 2- Un modèle d'agrégation d'attributs selon la revendication1, comprenant une phase d'agrégation d'attributs et de remplissage de la Table de Liaisons de Comptes caractérisé en ce que ladite phase d'agrégation d'attributs comprend les étapes suivantes :
 - L'utilisateur (end-user) s'authentifie auprès du Fournisseur de Liaison des Comptes (ALP : Accounts Linking Provider). Deux scénarios sont envisageables : - Si l'utilisateur dispose de données dans la Table de Liaison de Comptes, il peut consulter les informations relatives à ses comptes et ses attributs agrégés avec la possibilité de modifier, de supprimer et d'ajouter de nouveaux comptes et attributs. - Si la Table de Liaison de Comptes ne contient pas de données relatives à l'utilisateur authentifié, ce dernier sera invité à ajouter les comptes et les attributs qu'il souhaite agréger en suivant les étapes suivantes :
 - L'ALP redirige l'utilisateur vers un Service de Découverte des IdPs ayant des relations de confiance avec L'ALP.
 - L'utilisateur sélectionne un IdP puis il s'authentifie auprès de ce dernier.
 - Après la réussite de l'authentification, l'IdP lance un processus de recherche dans son annuaire/ base de données puis il affiche une liste des noms des attributs de l'utilisateur authentifié.
 - L'utilisateur sélectionne les attributs qui seront fournis par cet IdP suite aux requêtes de demande d'attributs envoyées par des SPs.
 - L'IdP envoie la liste des noms des attributs sélectionnés et l'assertion d'authentification de l'utilisateur vers l'ALP qui créera une entrée pour cet utilisateur dans la Table de Liaison de Comptes en faisant la correspondance entre l'IdP et les noms des attributs.

L'utilisateur peut être invité à choisir un autre IdP et le processus décrit ci-dessus sera répété à nouveau.

- 3- Un modèle d'agrégation d'attributs selon la revendication 1, comprenant une phase d'accès à un SP caractérisé en ce que ladite phase d'accès comprend les étapes suivantes :
 - L'utilisateur tente d'accéder à une ressource dont l'accès est contrôlé par un SP.
 - Le SP affiche la liste des attributs nécessaires pour autoriser l'accès à la ressource en demandant à l'utilisateur s'il souhaite utiliser l'agrégation d'attributs avec ce service.
 - Si l'utilisateur choisit d'effectuer l'agrégation d'attributs, il sera redirigé vers le Service de Découverte des ALPs ayant des relations de confiance avec ce SP.
 - L'utilisateur sélectionne un ALP en lui invitant à s'authentifier auprès de ce dernier.
 - Après la réussite de l'authentification, l'ALP renvoie au SP une assertion d'authentification portant l'identifiant (uid) de l'utilisateur authentifié.
 - Avant d'accorder l'accès à la ressource, le SP envoie une requête de demande d'attributs au fournisseur ALP.
 - L'ALP initie un processus de recherche dans sa Table de Liaisons de Comptes à base de l'uid de l'utilisateur. Une fois qu'il a situé l'entrée appropriée pour cet utilisateur, l'ALP envoie la liste des IdPs gérant les attributs requis.
 - Le SP envoie des requêtes de demande d'attributs à chaque IdP avec l'uid de l'utilisateur et l'assertion d'authentification.
 - Chaque IdP renvoie une réponse avec les attributs demandés.
 - Le SP prend sa décision de refuser ou d'accorder l'accès à l'utilisateur en se basant sur les attributs reçus par tous les IdPs.
- 4- Un modèle d'agrégation d'attributs selon les revendications 1 et 2 caractérisé en ce que l'ALP est sous le contrôle total de l'utilisateur. Ce dernier détient d'une visibilité complète sur la diffusion et l'utilisation de ses identités et ses attributs.
- 5- Un modèle d'agrégation d'attributs selon les revendications 1 et 2 caractérisé en ce que les IdPs n'envoient que les attributeIDs (les noms des attributs) à l'ALP ; les valeurs des attributs restent stockées au niveau des annuaires des IdPs.
- 6- Un modèle d'agrégation d'attributs selon les revendications 1 et 3 caractérisé en ce que l'accès à un SP nécessite une unique authentification sans avoir à s'authentifier séparément auprès de chaque IdP.

- 7- Un modèle d'agrégation d'attributs selon les revendications 1 et 3 caractérisé en ce que l'ALP n'envoie que la liste sélective des IdPs gérant les attributs demandés par le SP.
- 8- Un modèle d'agrégation d'attributs selon la revendication 1 caractérisé en ce que le SP devrait disposer des relations de confiance avec tous les IdPs, tandis que ces derniers n'ont pas besoin d'avoir des relations de confiance entre eux. D'autre part, aucun IdP ne devrait être au courant de l'existence des comptes de l'utilisateur final au niveau des autres IdPs.

Annexe

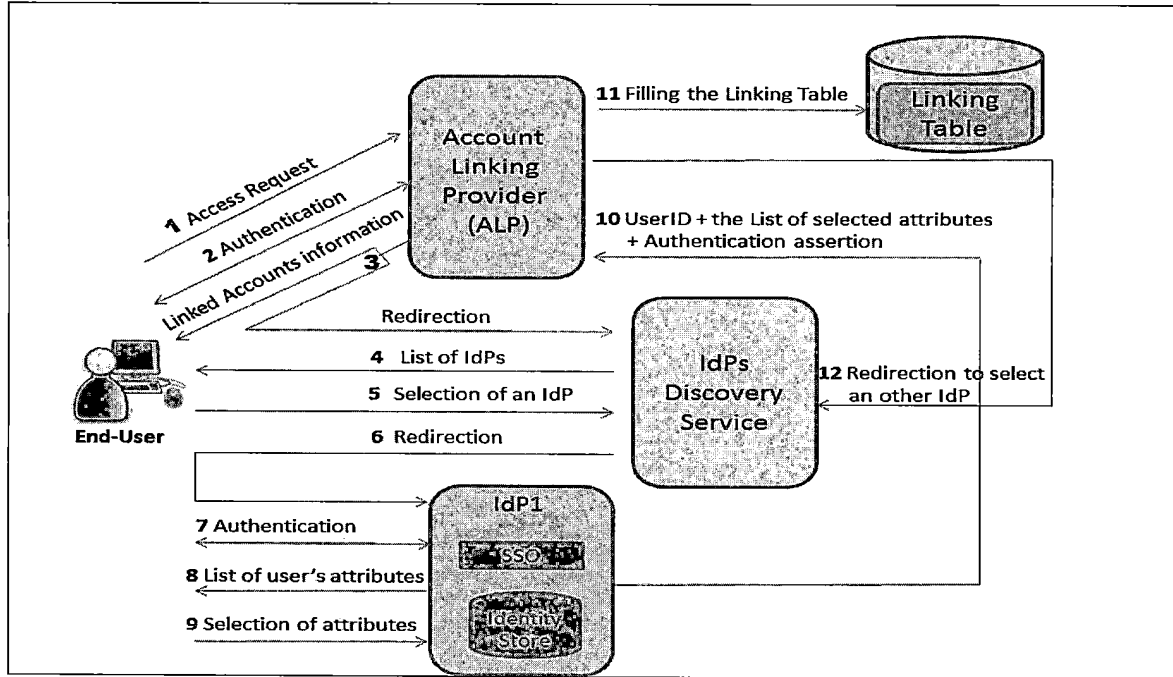


Figure1: Accounts Aggregation and Linking Table Filling

	IdPs	Attributes	Authentication Assertion
UserID1	IdP1	Email CIN	OK
	IdP2	givenName displayName	OK
	IdPn	telephoneNumber	OK

Figure 2: Linking Table

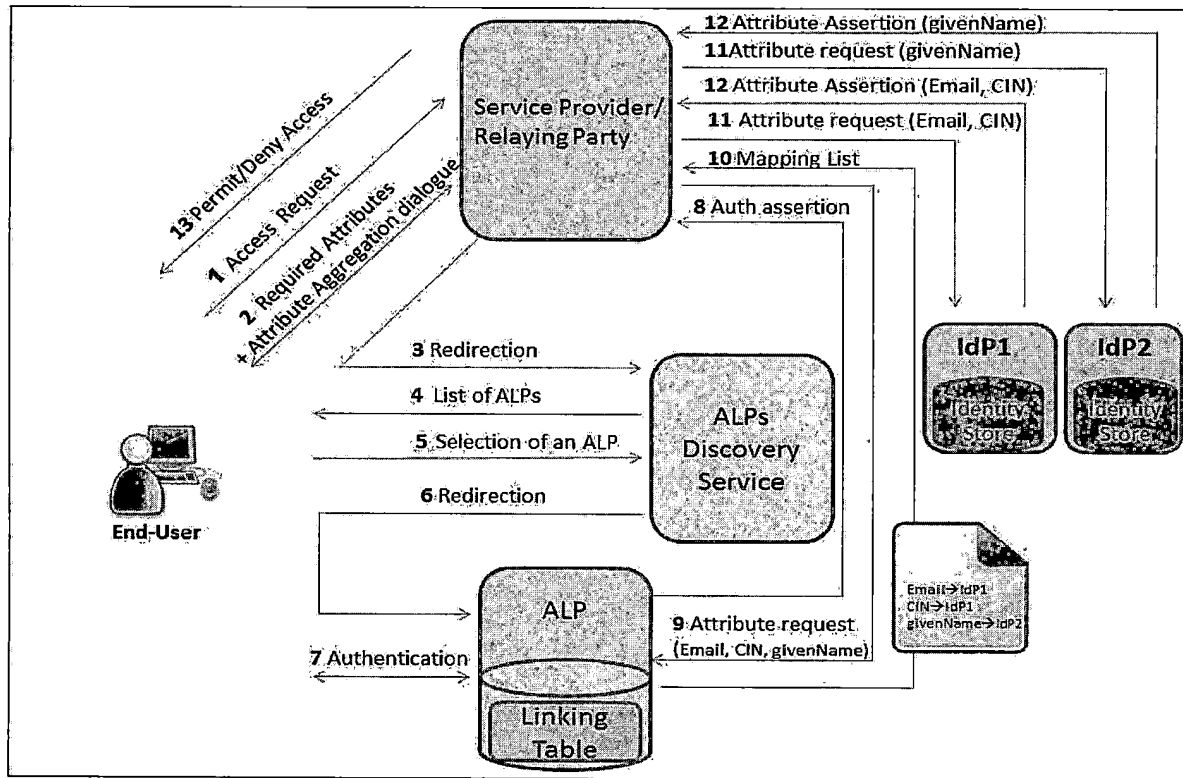


Figure 3: Access Process



**RAPPORT DE RECHERCHE
AVEC OPINION SUR LA BREVETABILITE**
(Conformément aux articles 43 et 43.2 de la loi 17-97 relative à la
protection de la propriété industrielle telle que modifiée et
complétée par la loi 23-13)

Renseignements relatifs à la demande	
N° de la demande : 39243	Date de dépôt : 01/08/2016 ;
Déposant : Université Mohammed V Rabat	
Intitulé de l'invention : Un modèle flexible et interopérable d'agrégation d'attributs pour la fédération d'identité	
Le présent document est le rapport de recherche avec opinion sur la brevetabilité établi par l'OMPIC conformément aux articles 43 et 43.2, et notifié au déposant conformément à l'article 43.1 de la loi 17-97 relative à la protection de la propriété industrielle telle que modifiée et complétée par la loi 23-13.	
Les documents cités par l'examineur dans la partie rapport de recherche sont joints au présent document	
Le présent rapport contient des indications relatives aux éléments suivants :	
Partie 1 : Considérations générales	
<input checked="" type="checkbox"/> Cadre 1 : Base du présent rapport <input type="checkbox"/> Cadre 2 : Priorité <input type="checkbox"/> Cadre 3 : Titre et/ou Abrégé tel qu'ils sont définitivement arrêtés	
Partie 2 : Rapport de recherche	
Partie 3 : Opinion sur la brevetabilité	
<input checked="" type="checkbox"/> Cadre 4 : Remarques de clarté <input checked="" type="checkbox"/> Cadre 5 : Déclaration motivée quant à la Nouveauté, l'Activité Inventive et l'Application Industrielle <input type="checkbox"/> Cadre 6 : Observations à propos de certaines revendications dont aucune recherche significative n'a pu être effectuée <input type="checkbox"/> Cadre 7 : Défaut d'unité d'invention	
Examineur: F.Belafkih	Date d'établissement du rapport : 11/10/2016
Téléphone: 212 5 22 58 64 14/00	

Partie 1 : Considérations générales		
<i>Cadre 1 : base du présent rapport</i>		
Les pièces suivantes de la demande servent de base à l'établissement du présent rapport :		
<ul style="list-style-type: none"> • <u>Description</u> 5 Pages • <u>Revendications</u> 8 • <u>Planches de dessin</u> 2 Pages 		
Partie 2 : Rapport de recherche		
Classement de l'objet de la demande :		
CIB : H04L12/56 CPC : H04L67/327, H04L63/0815, H04L67/02, H04L47/70		
Bases de données électroniques consultées au cours de la recherche :		
EPOQUE, Orbit		
Catégorie*	Documents cités avec, le cas échéant, l'indication des passages pertinents	N° des revendications visées
X	A Conceptual Model for Attribute Aggregation; David W. Chadwick , George Inman , Nate Klingenstein ;2010 http://sec.cs.kent.ac.uk/shintau/FGCS%20ModelAttribute%20Aggregation.pdf Tout le document	1-8
A	Obtaining Strong Identifiers Through Attribute Aggregation ; Walter Priesnitz Filho, Carlos Ribeiro ; 2014 https://www.thinkmind.org/download.php?articleid=securware_2014_4_40_30155 Tout le document	1-8
A	US 20140189123 A1 ; International Business Machines Corporation ; 03 Juillet 2014 Tout le document	1-8
*Catégories spéciales de documents cités :		
-« X » document particulièrement pertinent ; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément -« Y » document particulièrement pertinent ; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier -« A » document définissant l'état général de la technique, non considéré comme particulièrement pertinent -« P » documents intercalaires ; Les documents dont la date de publication est située entre la date de dépôt de la demande examinée et la date de priorité revendiquée ou la priorité la plus ancienne s'il y en a plusieurs -« E » Éventuelles demandes de brevet interférentes. Tout document de brevet ayant une date de dépôt ou de priorité antérieure à la date de dépôt de la demande faisant l'objet de la recherche (et non à la date de priorité), mais publié postérieurement à cette date et dont le contenu constituerait un état de la technique pertinent pour la nouveauté		

Partie 3 : Opinion sur la brevetabilité*Cadre 4 : clarté*

L'objet des revendications 1-8 n'est pas clairement défini. En effet l'objet revendiqué « **Modèle d'agrégation d'attributs** » n'est pas admissible comme catégorie, conformément à l'article 10 du décret d'application de la loi 17-97 modifiée et complétée par la loi 23-13 qui stipule que l'objet des revendication doit être un produit, procédé, dispositif ou utilisation.

Les termes **fournisseur de liaison de compte** et **table de liaison des comptes** employés dans la revendication 1 ont un sens relatif qui n'est pas bien établi, et ils laissent subsister un doute quant à la signification des caractéristiques techniques auxquelles ils se rapportent, au point que l'objet de ladite revendication n'est pas clairement défini.

Cadre 5 : Déclaration motivée quant à la Nouveauté, l'Activité Inventive et l'Application Industrielle

Nouveauté (N)	Revendications aucune	Oui
	Revendications 1-8	Non
Activité inventive (AI)	Revendications aucune	Oui
	Revendications 1-8	Non
Possibilité d'application Industrielle (PAI)	Revendications 1-8	Oui
	Revendications aucune	Non

Il est fait référence aux documents suivants. Les numéros d'ordre qui leur sont attribués ci-après seront utilisés dans toute la suite de la procédure

D1 : A Conceptual Model for Attribute Aggregation**1. Nouveauté (N) et Activité inventive (AI) :**

Nonobstant le manque de clarté mentionné ci-dessus, l'objet de la revendication 1 n'est pas nouveau et n'implique pas une activité inventive au sens des articles 26 et 28 de la loi 17-97 modifiée et complétée par la loi 23-13.

En effet, le document D1 divulgue un modèle d'agrégation d'attributs des utilisateurs disposant de plusieurs comptes auprès de différents fournisseurs d'identité en utilisant une seule et unique authentification dans une seule session d'accès (**D1 : Abrégé**) . Ledit modèle se base sur les mécanismes de la fédération d'identité et le relais d'identité en introduisant un module qui permet la liaison des comptes (**D1 : Abrégé, service de liaison**) avec une table de liaison des comptes qui illustre l'ensemble des IdPs et les attributs correspondants (**D1 : Figures 2, 3 pages 7 et 9**).

Les revendications dépendantes 2-8 ne contiennent aucune caractéristique qui, en combinaison avec les revendications auxquelles elles se réfèrent, définissent un objet satisfaisant aux exigences de la nouveauté et de l'activité inventive.

2. Possibilité d'application industrielle (PAI) :

L'objet de la présente invention est susceptible d'application industrielle au sens de l'article 29 de la loi 17-97 telle que modifiée et complétée par la loi 23-13, parce qu'il présente une utilité déterminée, probante et crédible.