

PROGRAMME D'ACTION "IDENTITES ACTIVES"

Fing avec Cecurity.com et EIfEL

www.identitesactives.net

Enjeux et opportunités de la fédération d'identités

Atelier de travail

18 décembre 2007, Issy-les-Moulineaux, Orange Labs

SOMMAIRE

LES 6 POINTS CLEFS DE L'ATELIER	2
1- PRESENTATION DU PROGRAMME D'ACTION "IDENTITES ACTIVES" ET DE L'ATELIER.....	4
Introduction de Charles Népote, Fing	5
2- ETAT DE L'ART SOLUTIONS DE FEDERATION D'IDENTITE : TENDANCES ET ALTERNATIVES	7
2-1 Intervention de Fulup Ar Foll, représentant Liberty Alliance/Sun : Liberty Alliance	8
2-2 Intervention de Bernard Ourghanlian, Microsoft France : CardSpace	11
2-3 Intervention de Snorri Giorgetti, Fondation OpenID	12
2-4 Intervention de Christophe Boutet, Entr'ouvert : Concordia	13
3- CAS D'USAGE ET RETOURS D'EXPERIENCE	14
3-1 Intervention de Ludovic Francesconi, GIE Cartes Bancaires : le projet FC ² ...	15
3-2 Intervention d'Eric L'excellent, Orange : stratégies d'implantation de fédération d'identité	17
3-3 Intervention de Marc Van Coillie, EIfEL : le projet "CV Universel"	18
4- DEBAT, PARTAGE D'IDEES ET DE PROJETS : QUELLES SUITES DONNER A L'ATELIER ?	20
ANNEXE : PARTICIPANTS DE L'ATELIER	22

LES 6 POINTS CLEFS DE L'ATELIER

Ce premier atelier consacré à la fédération d'identités se donnait comme premiers objectifs de valider ensemble quelques définitions et vocabulaire communs, identifier des clés de cartographie des infrastructures et valider ensemble les prochaines étapes du programme. Deux autres évènements sur ce thème seront programmés en 2008 pour compléter cet état des lieux.

Les points clefs des interventions :

⇒ **Point clef 1**

Les trois principales solutions de fédération d'identité (Liberty Alliance, OpenID et CardSpace) sont moins concurrentes que complémentaires. Elles relèvent surtout de philosophies différentes, notamment dans le parti pris de confier à l'utilisateur le soin de gérer l'usage de ses données ou de déléguer cette "gestion" à un tiers de confiance.

⇒ **Point clef 2**

Si les technologies sont anciennes, le sujet n'a pas pour autant atteint sa maturité : face au foisonnement de solutions qui émergent chaque mois, l'utilisateur oscille entre paranoïa et manque d'information. L'absence de maturité du public sur ces questions explique donc en partie que la fédération d'identité peine à "décoller" véritablement.

⇒ **Point clef 3**

Industriels et usagers sont "victimes" de flous sémantiques (fédération d'identité, fédération de services, partage d'attributs, etc.) car les termes sont souvent élaborés et utilisés sous des significations différentes par les marques commerciales. Le besoin d'un lexique "neutre" ressort tant de tous les acteurs de la chaîne de valeur : usagers, fournisseurs de services, fournisseurs d'identité et fournisseurs d'infrastructures d'identité.

⇒ **Point clef 4**

Parmi les opportunités pragmatiques identifiées, le pré-remplissage des formulaires semble une piste fertile et plutôt légère à mettre en place

⇒ **Point clef 5**

La question de l'ouverture des standards ainsi que des modèles économiques associés demeure un enjeu clef de l'évolution de la fédération d'identité.

⇒ **Point clef 6**

Une suite possible de l'atelier pourrait consister à élaborer un panel de scénarios d'usage. Dans un deuxième temps, un travail de "mapping" des différentes solutions de fédération d'identité pourrait compléter ce travail.

⇒ **Pour aller plus loin :**

- > www.fing.org/identites
- > www.identitesactives.net (ouverture du site en janvier 2008)
- > www.projectliberty.org
- > www.identityblog.com (blog de Kim Cameron)
- > <http://openid.net>
- > <http://projectconcordia.org>
- > www.ethique-et-recrutement.org

1- PRESENTATION DU PROGRAMME D'ACTION "IDENTITES ACTIVES" ET DE L'ATELIER

⇒ **Point clef 1**

La première phase du programme consiste principalement à constituer un premier référentiel de connaissances autour de ces thèmes, de constituer une communauté d'acteurs hétérogènes actifs sur les problématiques de l'identité numérique et de dresser une cartographie des questions inhérentes à l'identité numérique.

⇒ **Point clef 2**

La Fédération d'identité est en effet au cœur des problématiques du programme, ne serait-ce que par une tendance nette à la "fragmentation des identités" de chacun sous l'effet de la diversification d'usages de services numériques de plus en plus étendus.

⇒ **Point clef 3**

Pour explorer ce thème de la "fédération d'identité", l'équipe du programme propose d'organiser les travaux autour d'un "track" (cycles de conférences, repérage de projets innovants et accompagnement de projets collectifs sur des chaînons manquants, etc.) qui s'étendra tout au long de l'année 2008.

⇒ **Point clef 4**

Ce track se propose ainsi de :

- valider quelques définitions et vocabulaire communs
- proposer des règles et déontologies communes (sur le principe)
- identifier des leviers et priorités d'action
- identifier des opportunités ?

Introduction de Charles Népote, Fing

- > www.fing.org/identites
- > www.identitesactives.net (ouverture du site en janvier 2008)

Charles Népote, directeur du programme d'action "Identités actives", introduit l'atelier en 3 temps :

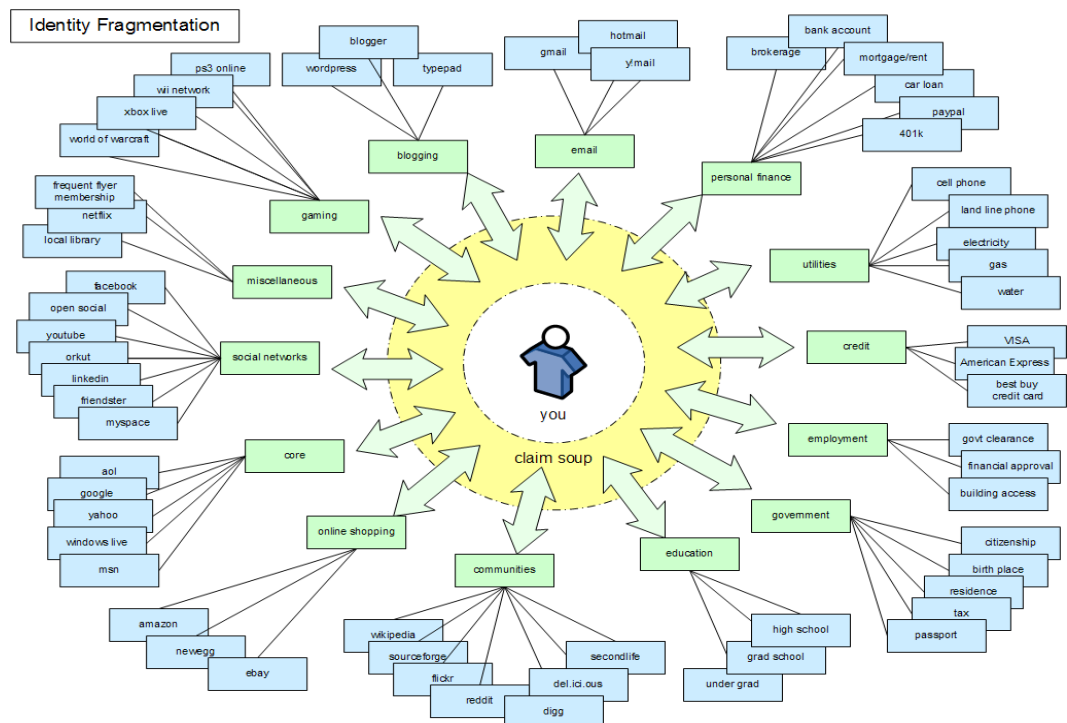
- une présentation succincte du programme d'action "Identités actives" ;
- un exposé des principales questions que pose, dans le cadre du programme, la "fédération d'identité" ;
- enfin, une présentation de l'ordre du jour ainsi que des principaux objectifs que se donne l'atelier

Le programme d'action "Identités actives", démarré en septembre 2008, se donne pour objectif de stimuler le développement d'infrastructures, d'outils et de services qui favorisent et exploitent une gestion active de leurs identités numériques par les individus et les entreprises.

Il durera 18 mois environ et recouvre de nombreux thèmes liés à l'identité numérique : exploitation, négociation, maîtrise de ses données, expressions de soi sur les réseaux, questions liées à la mémoire et aux temporalités des individus, interopérabilité et fédération des données et de services, problématiques autour de l'anonymat, etc.

La première phase du programme consiste principalement à constituer un premier référentiel de connaissances autour de ces thèmes, de constituer une communauté d'acteurs hétérogènes actifs sur les problématiques de l'identité numérique et de dresser une cartographie des questions inhérentes à l'identité numérique.

Ce 1^{er} atelier sur le thème "Fédération d'identité" s'inscrit donc dans cette phase et revêt un caractère exploratoire. La Fédération d'identité est en effet au cœur des problématiques du programme, ne serait-ce que par une tendance nette à la "fragmentation des identités" de chacun sous l'effet de la diversification d'usages de services numériques de plus en plus étendus.



Les questions que pose la fédération d'identité sont nombreuses :

- Qu'entend-on par "fédération de services" et "fédération d'identités" ? Que peuvent-elles apporter aux usagers ?
- Ces questions se posent-elles différemment selon que l'on soit usager, fournisseur d'infrastructure, prestataire de service ou prescripteur ?
- Quelles prises de l'usager en termes d'information voire d'éducation sur ce sujet (déontologie, cadre d'usage, principes de fonctionnement, etc.) ?
- Quel degré de maîtrise et de négociation de ce dernier sur ses données ? (pouvoir accéder, modifier, rectifier, mettre des règles sur des parties de mon identité, créer des filtres)
- Que se passe t-il si la fédération d'identité n'émerge pas ?
- Comment interpréter le foisonnement actuel de solutions de fédération ?

Pour y répondre, l'équipe du programme propose de procéder en plusieurs étapes, autour d'un **"track"** dédié à la fédération d'identité. Il s'agit de coupler cycles de conférences, repérage de projets innovants et accompagnement de projets collectifs sur des chaînons manquants.

Ce track se propose ainsi de :

- valider quelques définitions et vocabulaire communs
- proposer des règles et déontologies communes (sur le principe)
- identifier des leviers et priorités d'action
- identifier des opportunités ?

Pour amorcer la réflexion, ce premier atelier se donnait comme premiers objectifs de valider ensemble quelques définitions et vocabulaire communs, identifier des clés de cartographie des infrastructures et valider ensemble les prochaines étapes du programme.

2- ETAT DE L'ART SOLUTIONS DE FEDERATION D'IDENTITE : TENDANCES ET ALTERNATIVES

⇒ Point clef 1

En matière de fédération d'identité, 3 grandes "solutions" se démarquent : Liberty Alliance, OpenID et CardSpace. Ces trois solutions reflètent des philosophies d'architecture d'identité différentes : utilisateur au centre du système et localisation des données sur la machine de l'utilisateur (CardSpace), gestion de l'identité confiée à un tiers de confiance (OpenID), décentralisation totale de type P2P sans "serveur" central (Liberty Alliance). Ces solutions sont moins concurrentes que complémentaires.

⇒ Point clef 2

L'identité sert avant tout à discuter et échanger avec d'autres (un passeport sert avant tout à circuler). Par conséquent, plus on va vers un mécanisme d'identité, plus on veut qu'il soit universel, et plus le besoin d'interopérabilité est grand : c'est l'idée qui préside aux projets de fédération d'identité.

⇒ Point clef 3

CardSpace, un "métasystème" d'identité qui négocie entre le fournisseur d'identité et le poste de travail utilisateur. Après l'échec social de Passport, CardSpace illustre le changement de paradigme dans lequel s'est placé Microsoft dans son positionnement sur le marché de la fédération d'identité : il ne s'agit plus pour l'entreprise de centraliser l'ensemble des systèmes d'identité (philosophie qui présidait à Passport), mais au contraire, de laisser à l'individu le contrôle total de l'usage qui est fait de ses données.

⇒ Point clef 4

OpenID est un système d'authentification décentralisé qui permet l'authentification unique (qui prend la forme d'un URL), ainsi que le partage d'attributs. La facilité d'implémentation d'OpenID en fait un service très bien adapté aux processus "d'identification faible".

⇒ Point clef 5

Le projet Concordia, lancé par les créateurs de Liberty Alliance, vise à faire converger les standards.

2-1 Intervention de Fulup Ar Foll, représentant Liberty Alliance/Sun : Liberty Alliance

> www.projectliberty.org

Avant d'aborder les problématiques de "fédération", Fulup Ar Foll, représentant du consortium d'acteurs autour du projet "Liberty Alliance", précise quelques notions clefs de l'identité (numérique ou non).

En effet, les questions relatives à l'identité ne datent pas d'hier, encore moins du numérique. L'identité ramène souvent à la collecte d'informations qui la caractérise, souvent d'ailleurs pour des raisons qui nous échappent (le numéro de téléphone pour réserver une chambre d'hôtel, les empreintes digitales à l'aéroport, etc.). En fait, et de tout temps, il est collecté beaucoup trop d'informations !

Egalement, depuis toujours, les informaticiens se focalisent sur l'authentification ; or le but des systèmes d'identité, c'est simplement de prouver quelque chose, à l'image du permis de conduire qui sert à prouver que je suis apte à conduire un véhicule. Donc, alors qu'il semble falloir ne collecter qu'un nombre minimum d'arguments relatifs à mon identité, c'est l'inverse que l'on réalise.

Enfin, force est de constater que lorsque l'on fournit une identité à quelqu'un, on ne sait jamais ce qu'il va en faire...

L'identité comporte 3 parties:

- L'authentification qui tend à prouver (par des caractéristiques qui me sont propres, des connaissances que je suis seul à détenir, un objet que je suis seul à posséder) que je suis celui que je prétends être
- Des attributs, qui sont le cœur de l'identité, puisqu'ils définissent ce que je suis : les autorisations ou interdictions qui me sont relatives, mes caractéristiques, les groupes auxquels j'appartiens, etc.
- Enfin, la vérification qui prouve que les garanties que j'ai apportées sont valides (certificats, signature, date de validité).

Le digital change t-il réellement la donne ?

La numérisation des données ne suffit pas à bouleverser quelques fondamentaux : les données sont rarement (véritablement) tenues au secret, elles sont collectées mais rarement totalement effacées et enfin ... elles sont rarement utilisées aux fins prévues initialement.

En cela, le numérique ne diffère guère du "papier".

Pourtant, par bien des aspects, la numérisation des données change considérablement l'utilisation qui peut être faite de ces dernières. Aujourd'hui, il est facile et bon marché de faire des corrélations : il suffit pour cela d'avoir accès à l'information, sans que cela ne nécessite de disposer de ses propres infrastructures (celles-ci existent déjà).

Parallèlement, l'évolution des technologies est si rapide qu'elles en deviennent incompréhensibles par l'humain, ce qui contribue à brouiller l'usage des données.

De facto, on est plus limité non pas par ce que l'on peut faire mais plutôt parce que ce que l'on veut faire. Il revient donc aux acteurs eux-mêmes de fixer des limites, ce qui pose

problème dans la mesure où celles-ci s'établissent sur des critères subjectifs et dont l'interprétation peut ne pas être la même d'un acteur à l'autre.

L'identité sert avant tout à discuter et échanger avec d'autres

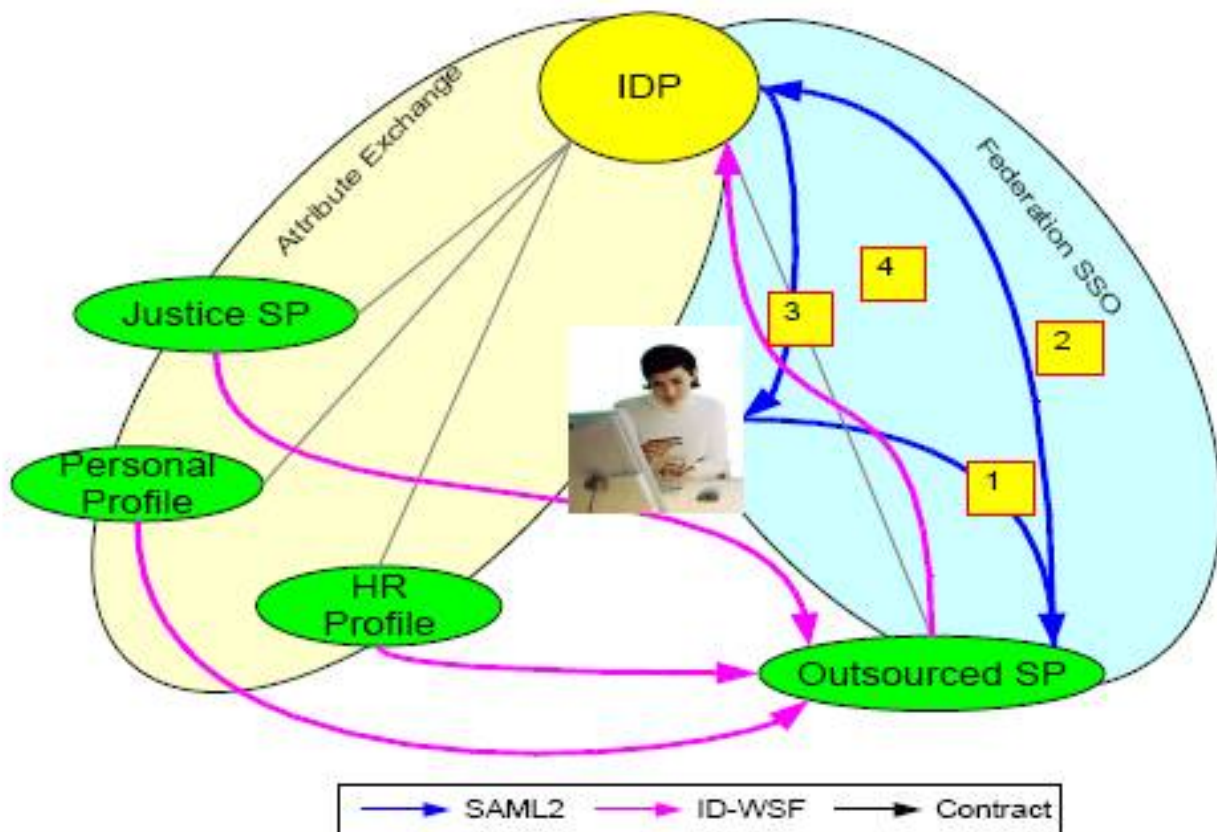
Un passeport me permet avant tout de circuler... Par conséquent, plus on va vers un mécanisme d'identité, plus on veut qu'il soit universel, et plus le besoin d'interopérabilité est grand.

C'est l'idée qui préside aux projets de fédération d'identité. Celui de Liberty Alliance a délibérément été orienté pour conserver de la souplesse.

Quelle vision de l'architecture Liberty Alliance ?

La Liberty Alliance a pour mission d'élaborer des spécifications techniques communes pour les applications de services web, en particulier pour les services d'authentification en ligne. Elle vise à promouvoir les standards techniques liée à une "identification forte".

Au niveau des infrastructures, Liberty Alliance est un environnement multicouche, où l'application web que je sollicite fait une requête vers un service, qui elle même fait un requête à une autre couche ; cela nécessite de créer de l'opacité lors du transfert d'identité entre services.





Dans Liberty Alliance, le choix est fait que les applications échangent entre elles des attributs sans passer par une autorité "suprême", "au-dessus" des autres, comme c'est le cas de beaucoup de services où la totalité des flux d'identité transite par une seule autorité car à terme cette autorité finit par collecter toutes vos données...

Liberty Alliance est une spécification accessible en ligne, à la fois un assemblage et un profilage, dont le but est de faire en sorte que l'individu ne s'occupe de rien.



2-2 Intervention de Bernard Ourghanlian, Microsoft France : CardSpace

> Blog de Kim Cameron : www.identityblog.com

De Passport à CardSpace, un changement de paradigme

Pour introduire la technologie CardSpace, Bernard Ourghanlian, directeur technique et sécurité de Microsoft France, revient sur une précédente expérience de fédération d'identité tentée par Microsoft, Passport.

Dans le projet Passport, l'idée était de créer un système d'identité global pour la totalité de l'internet. Si sur le plan technique, CardSpace s'est avéré une réussite (280 millions de comptes), au niveau social, le projet s'est soldé par un échec. Microsoft devenait en effet un intermédiaire obligatoire à tous les services.

CardSpace illustre le changement de paradigme dans lequel s'est placé Microsoft dans son positionnement sur le marché de la fédération d'identité : il ne s'agit plus pour l'entreprise de centraliser les systèmes d'identité, mais au contraire, de laisser l'individu le contrôle total de l'usage qui est fait de son identité.

L'élaboration du "système" CardSpace est issu d'une grande discussion en ligne initiée en 2004 par Kim Cameron, architecte de l'identité chez Microsoft. Cette discussion a généré 7 principes d'identité¹, que le service incarne.

CardSpace, un "métasystème" d'identité qui négocie entre le fournisseur d'identité et le poste de travail utilisateur

CardSpace est en fait un métasystème d'identité, interopérant plusieurs fournisseurs de services d'identité : il n'y a ni fournisseur, ni technologie ou protocole unique, la fédération est centrée sur l'utilisateur. Les fournisseurs d'identité sont représentés par des "cartes".

Ce type de service s'adresse notamment aux sites de e-commerce. Pour ces derniers, CardSpace a pour objectif de faciliter la transformation de la recherche du client en achat, augmenter la confiance et fidéliser les usagers

L'interface Homme/Machine est basée sur des briques que l'utilisateur construit lui-même, ce qui limite le vol d'identité. L'utilisateur établit différentes cartes regroupant des données qu'il a choisi (textes, mais aussi visuelles, ce qui permet plus facilement à l'utilisateur de constater une hypothétique usurpation).

Principes de fonctionnement

Le processus se déroule comme suit :

- Le client demande à accéder à une ressource

¹ Consentement et contrôle de la part des utilisateurs, divulgation minimale d'informations pour des usages précis et limités, "Parties légitimes", "Identité directionnelle", pluralisme d'opérateurs et de technologies, intégration humaine et expérience homogène dans des contextes différents.

- La ressource indique sa "politique", c'est-à-dire les éléments d'identité qu'elle requiert, et les retourne au client
- Le système Cardspace regarde les cartes dont il dispose et identifie les fournisseurs d'identité capables de fournir les informations requises. Autrement dit l'information n'est pas du tout nécessairement stockée sur le PC
- Le fournisseur d'identité reçoit de l'utilisateur la demande d'émettre un "jeton", ce qu'il fait, ou non s'il y a un doute sur la ressource
- Le jeton revient vers l'utilisateur, puis vers la ressource
- L'accès à la ressource est alors ouvert

2 types de cartes peuvent être générés :

- auto-émises : possibilité de se créer sa propre carte, on en crée autant qu'on veut. Ces infos ne sont pas accessibles aux services.
- gérées, managées : par exemple fournies par le site marchand ; elles font alors office de carte de fidélisation ou de carte de crédit.

Les "CardSpace" sont situées "en local" : l'utilisateur sait donc en permanence où elles se situent. Par contre, il faut effectuer un transfert en cas de changement de machine. Dans un tel système les acteurs ont un droit mutuel de veto vis-à-vis de leurs affirmations.

Daniel Kaplan remarque que le système CardSpace ne s'apparente pas nécessairement à de la fédération d'identité au sens "fédération de services" où celle-ci est définie par les 7 principes de Kim Cameron, c'est à dire des services qui communiquent entre eux pour se communiquer des données. Il s'agit plutôt d'un cas de figure au sens où l'utilisateur ne délègue pas la confiance à qui que ce soit.

2-3 Intervention de Snorri Giorgetti, Fondation OpenID

> <http://openid.net/>

OpenID est un système d'authentification décentralisé qui permet l'authentification unique, ainsi que le partage d'attributs. Il permet à un utilisateur de s'authentifier auprès de plusieurs sites (devant prendre en charge cette technologie) sans avoir à retenir un identifiant pour chacun d'eux mais en utilisant à chaque fois un unique identifiant OpenID. Cet identifiant prend la forme d'un URL.

N'importe qui peut se muer en fournisseur d'identité : depuis un individu qui tient son blog ou jusqu'à un fournisseur de service, beaucoup d'acteurs peuvent m'attribuer une identité.

OpenID propose aussi de fournir de l' "identité dirigée" qui associe plusieurs tiers de confiance et permet ainsi à l'utilisateur de ne pas être rattaché à un seul fournisseur d'identité.

Le modèle OpenID se base sur des liens de confiance préalablement établis entre les fournisseurs de services (sites web utilisant OpenID par exemple) et les fournisseurs d'identité (*OpenID providers*).

La philosophie d'OpenID repose donc sur un tiers de confiance (en l'occurrence un serveur) qui détient des informations dont on ne sait pas de quelle manière il va les utiliser.



Cela pose la question de la confiance : entre moi et un tiers, en qui ai-je le plus confiance pour confier et conserver mes données ? Suis-je plus compétent qu'un autre pour cela ? En passant par un tiers, on a besoin de garanties que celui-ci ne stockera pas mes données sur un disque dur ; mais comment en être sûr ?

La facilité d'implémentation d'OpenID en fait un service très bien adapté aux processus "d'identification faible" (cas de services de réservation d'espaces proposés par une mairie par exemple). En effet, et comme le rappelle Fulup Ar Foll, en cas de dysfonctionnement, il est facile pour les usagers de se créer une nouvelle identité ; après tout, il ne s'agit que de la réservation d'un court de tennis ou d'une salle ...

Cette potentielle volte face est moins évidente s'agissant d'une correspondance d'identité réelle en son équivalent numérique ; dans ce cas, le degré de complexification augmente car il m'est impossible de changer d'identité.

2-4 Intervention de Christophe Boutet, Entr'ouvert : Concordia

> <http://projectconcordia.org>

Si Liberty Alliance, CardSpace et OpenID sont les 3 principales solutions de fédération d'identité, elles ne sont pas les seules. En effet, de nouveaux standards et protocoles fleurissent chaque mois (SAML, WS-*, Shibboleth, ESSO, Oauth, Inames, papi, APML, Diso, etc.) pointant un autre enjeu de la fédération d'identité : sa capacité à harmoniser ces protocoles dans un contexte de course effrénée aux standards.

Le projet Concordia a ainsi été lancé dans une démarche visant à améliorer l'interopérabilité entre les technologies d'identité numérique de Liberty Alliance, Microsoft et OpenID.

Il ne s'agit pas d'une solution de fédération de fédération, mais plutôt d'un projet purement technique fondé sur une approche pragmatique qui permet à des entreprises utilisant plusieurs solutions de "s'y retrouver", c'est-à-dire répondre à la problématique des identités éparses.

Parmi les participants au projet :

- Contributeurs privés : Boeing, Chevron, General Motors...
- Contributeurs publics : Colombie Britannique, Nouvelle Zélande, US
- Fournisseurs de solutions et protocoles : Microsoft, Sun, Osis, SAML, Cardspace, Liberty, OpenID, WS-*, Oauth...

Concordia se pose en lieu d'échange (forums publics pour ceux qui déploient et leurs fournisseurs, travail de glossaire, collecte de cas d'usages réels sur l'interopérabilité tels que SAML 2.0 – WS-federation ou SAML-CardSpace) ainsi qu'en levier de facilitation (Bonnes pratiques, supports pédagogiques, tests d'interopérabilité).

OAuth permet à un utilisateur d'allouer l'accès d'un site à tout ou partie des ressources privées d'un autre site sans pour autant fournir les clés d'accès. Ce n'est donc pas une solution d'authentification partagée permettant de valider l'identité de l'utilisateur mais une façon ouverte de permettre aux applications web qui gère différentes données personnelles l'agrégation de ces données tout en respectant la non divulgation des clés permettant d'y accéder et de les gérer.

3- CAS D'USAGE ET RETOURS D'EXPERIENCE

⇒ **Point clef 1**

Le projet FC² ("Fédérations de cercles de confiance") a pour objet de développer et valider une plate-forme complète permettant le développement sécurisé de nouveaux services électroniques basée sur la gestion transparente et fédérée d'identités.

⇒ **Point clef 2**

La complexité de telles plateformes, supports de "gros" projets, pose deux questions : celle de la complexité d'usage (un tel dispositif n'est-il pas trop lourd pour des scénarios d'usage moins quotidiens?) et celle de la "réutilisabilité" (comment faire en sorte que les projets s'appuyant sur de telles plateformes ne soient-ils pas exclusivement ad-hoc ?).

⇒ **Point clef 3**

Jusqu'en 2007, Orange se "contentait" de fournir à ses clients un dispositif de SSO (Single Sign On) leur permettant de naviguer entre les différents services des portails du groupe. Pour aller un cran plus loin, le groupe adopte une stratégie visant à "ouvrir" l'identité qu'elle fournit à des services tiers ("Identité OpenID" en 2007 et Liberty Alliance courant 2008), pour à terme donner accès aux usagers non-clients d'Orange disposant d'un URL OpenID aux services Orange.

⇒ **Point clef 4**

Le projet de "CV Universel" consiste à créer un standard, basé sur les standards du CV européen, qui s'apparenterait à une forme de portfolio simplifiée. Le CVU s'avère un cas d'utilisation idéal pour comprendre les enjeux de la fédération d'identité : il met en jeu beaucoup de données, implique de nombreux acteurs, dispose d'une antériorité et est porté par des "gens du métier".

⇒ **Point clef 5**

Face au foisonnement de solutions qui émergent chaque mois, l'utilisateur oscille entre paranoïa et manque d'information. L'absence de maturité du public sur ces questions explique donc en partie que la fédération d'identité peine à "décoller" véritablement.

3-1 Intervention de Ludovic Francesconi, GIE Cartes Bancaires : le projet FC²

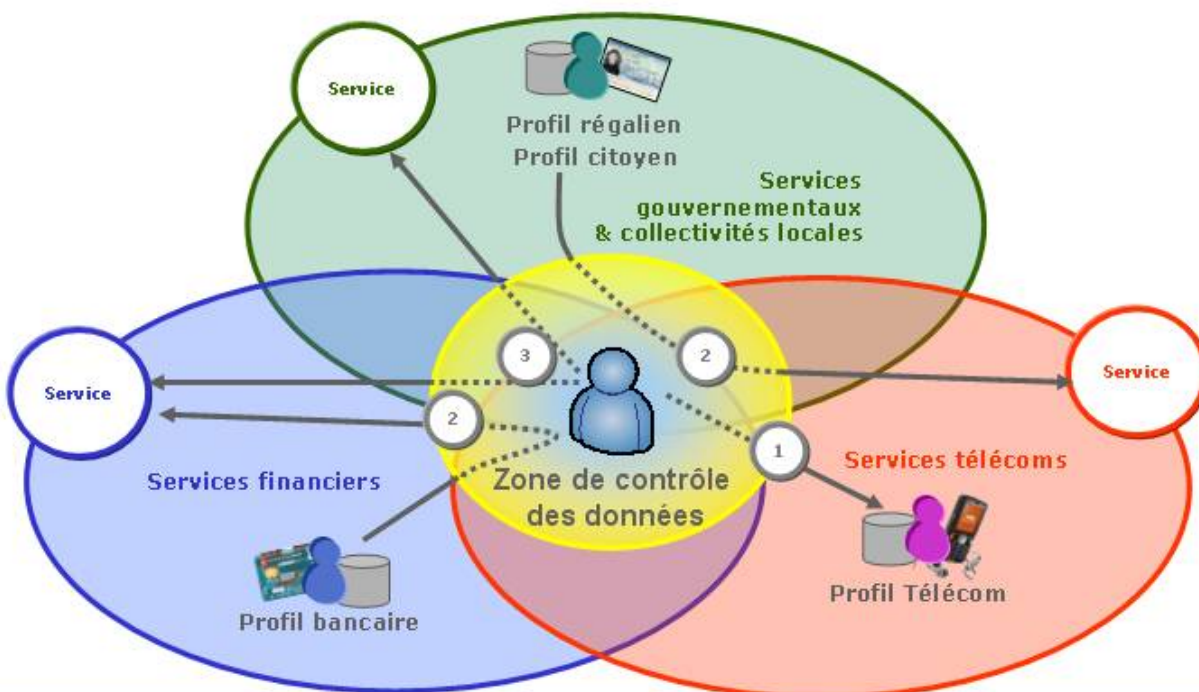
Le projet FC² ("Fédérations de cercles de confiance") a pour objet de développer et valider une plate-forme complète permettant le développement sécurisé de nouveaux services électroniques basée sur la gestion transparente et fédérée d'identités.

Il s'agit à la fois de mettre en œuvre de modèles d'architectures de fédération d'identité interopérables (Liberty Alliance, Microsoft/Cardspace, ...), de fournir des services d'authentification forte et de gestion de la vie privée, de mettre en place une infrastructure dédiée pour les fournisseurs de service et enfin, de développer des modèles économiques tout au long de la chaîne de valeur. Déployé courant 2008, le projet est labellisé par 2 pôles de compétitivité : TES et Systematic.

Au niveau opérationnel, FC² met en scène 3 cercles de confiance, l'utilisateur se situant au centre :

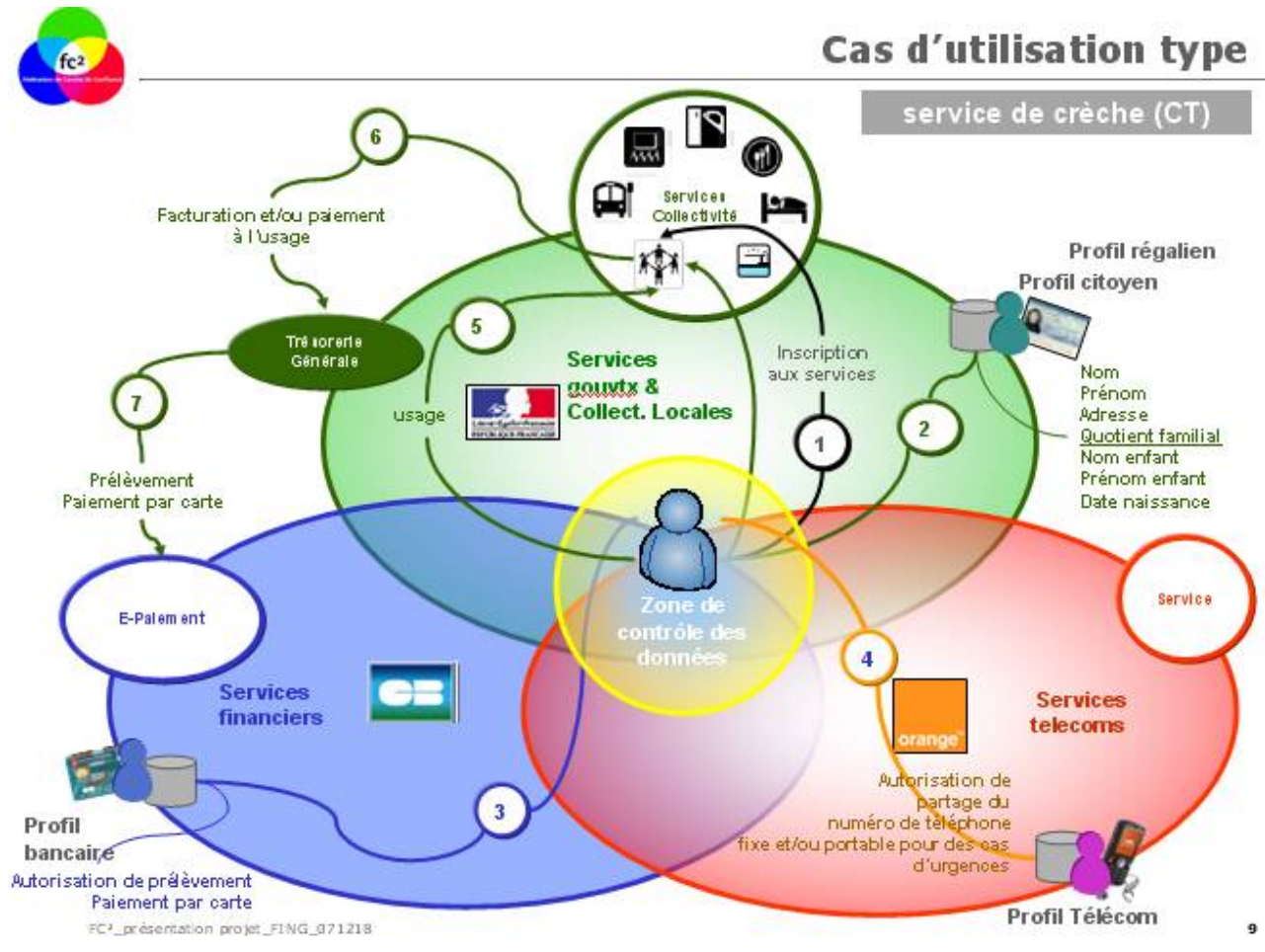
- Service de l'état et des collectivités locales
- Services financiers et bancaires
- Services telecom

1. Accès à ses données 2. Transfert de ses données 3. Accès aux services



Une vingtaine de cas d'usage visant à dématérialiser toutes les procédures de la "vie réelle" ont été identifiés : abonnement de téléphonie mobile, ouverture de compte bancaire en ligne, achat en ligne, commerce électronique, etc.

Exemple de la gestion d'un service de réservation de crèche.



Dans ce cas, la collectivité locale est fournisseur de service : elle récupère des attributs du demandeur. Le service étant payant, le passage dans la sphère financière impose la récupération d'un numéro de compte.

Daniel Kaplan remarque néanmoins que, dans cet exemple, il s'agit plus d'un cas ad hoc plutôt que d'un cas générique.

L'exemple est d'autant moins bien choisi que le processus peut s'avérer un peu lourd pour des usages de type crèche que l'individu lambda utilisera au mieux une fois dans l'année...

3-2 Intervention d'Eric LExcellent, Orange : stratégies d'implantation de fédération d'identité

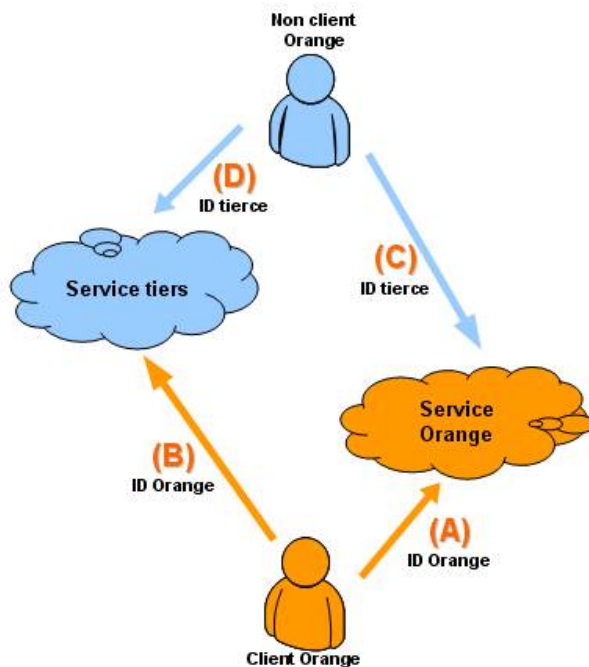
Eric LExcellent, chef de produit identités fédérées chez Orange, témoigne ensuite du changement de stratégie opéré par Orange en terme de fourniture d'identité, mettant en exergue les problématiques de fédération d'identité vu par un opérateur.

Du SSO au sein des portails Orange jusqu'à l'accès aux services tiers

Jusqu'alors, Orange se "contentait" de fournir à ses clients un dispositif de SSO (Single Sign On) leur permettant de naviguer entre les différents services des portails du groupe et cela, indépendamment du canal utilisé (Web, Wap, TV, etc.). Il s'agissait en fait de gérer les utilisateurs sur les services Orange.

En 2007, Orange s'oriente vers des services tiers en "ouvrant" l'identité Orange sur les solutions OpenID et Liberty Alliance.

Lancé en septembre 2007, le service OpenID d'Orange² permet aux usagers disposant d'un compte OpenID chez Orange d'accéder à des services tiers permettant l'identification via leur serveur, une stratégie visant entre autre à fidéliser les clients d'Orange (si ce dernier quitte Orange, il perd son mel, son accès à d'autres services, etc.). Quelques mois après sa mise en place, si la facilité d'implémentation et l'universalité du service (possibilité d'utiliser sa propre clef sur d'autres services OpenID) ont été vérifiées, la stratégie se heurte à deux écueils : l'éducation des utilisateurs nécessaires pour qu'ils détectent le logo OpenID et ... s'en servent, mais aussi le fait qu'OpenID – malgré de nombreuses promesses de services tiers, n'est pas encore assez implantée sur de "gros" services. De fait, le service demeure limité à des services de type blog ou réseaux sociaux ; beaucoup de sites type Netvibes ont annoncé une implémentation OpenID sans le faire.



La 2^{ème} étape de cette "ouverture d'identité" consistera en l'ouverture au 1^{er} trimestre 2008 un service basé sur les spécifications Liberty Alliance, protocole plutôt bien adapté à l'univers du mobile. Dans ce cas, la difficulté réside pour l'opérateur de devoir convaincre chaque partenaire.

S'il est un peu tôt pour tirer des enseignements de cette stratégie (encore plus au niveau de

² <http://openid.orange.fr>

Liberty / SAML qui n'a pas encore démarré...), la difficulté principale réside dans le fait que ces solutions de fédération d'identité "effraient" les services tiers ; malgré l'outil livré clef en main, ceux-ci restent effrayés de voir le lien direct avec leurs clients "court circuités" par des dispositifs de fédération d'identité. D'autant plus si celle-ci est compliquée... Enfin, la sécurité reste une épée de Damoclès en cas de vol d'identité (phishing).

Pour quoi aller vers des services tiers ?

Le besoin de remplissage automatique est très fort : car c'est une grosse demande utilisateur et cela permet au service tiers de disposer d'informations plus fiables. Pas de collecter des données sans savoir qu'en faire. Plutôt de faciliter l'accès à des services, notamment extérieurs à Orange.

De l'ouverture aux services tiers à l'ouverture des services Orange aux non clients

Enfin, au 2^{ème} trimestre 2008, Orange offrira la possibilité d'utiliser directement une identité OpenID ainsi que d'autres identités fournies par des fournisseurs de service d'accéder aux services Orange (les services de partage de photo par exemple).

3-3 Intervention de Marc Van Coillie, EIfEL : le projet "CV Universel"

> www.ethique-et-recrutement.org

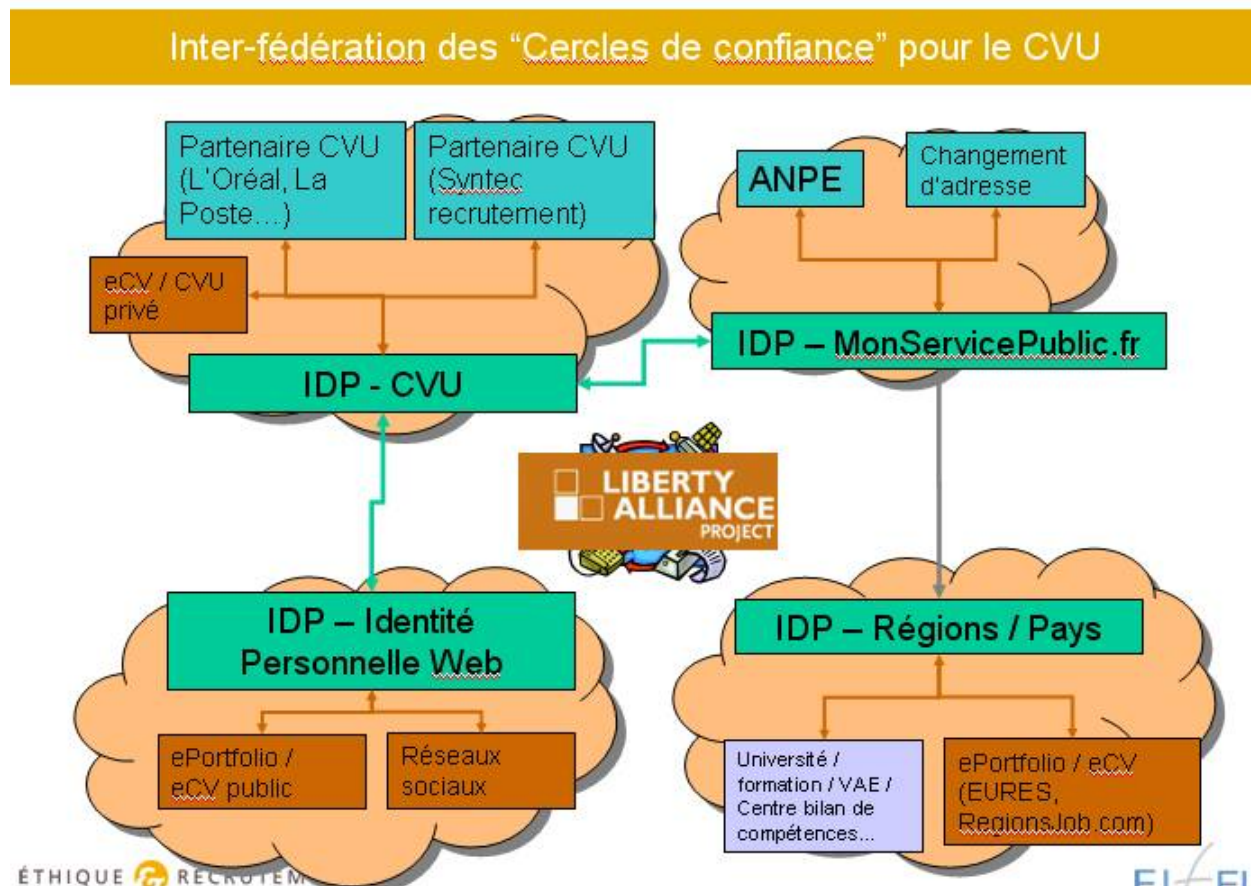
Pour clore les présentations, Marc Van Coillie, directeur des technologies à EIfEL (European Institute for E-Learning) mentionne le projet "CV Universel" porté par l'association *Ethique et recrutement*, et qui se constituera courant 2008 (la mise en ligne opérationnelle en phase pilote est prévue début avril).

Il s'agit de créer un standard, basé sur les standards du CV européen, qui s'apparenterait à une forme de portfolio simplifiée.

Le projet s'appuie sur des constats forts :

- La majorité des sites corporate ou des jobboards demandent aux candidats de remplir un formulaire de candidature pour être intégrés en base de données ou pour répondre à une annonce (c'est notamment le cas de l'APEC...)
- 80% des informations demandées sur ces sites sont les mêmes (Civilité, expériences, formations, langues, etc...),
- Remplir un formulaire de candidature sur un site prend plus de 15 minutes,
- Dans le cas où l'acte de candidature peut être fait par mail, tous les candidats n'ont pas la possibilité de créer un CV car ils n'ont pas accès aux logiciels de traitement de textes, même gratuits (notamment parce qu'il faut disposer d'un PC),
- Le mode « web » est le plus égalitaire pour postuler (à contrario du mode mail qui demande de coller un fichier joint de type .doc ou .pdf) car il est accessible de n'importe quel cyber café,
- Les candidats discriminés n'envoient plus leurs candidatures car ils anticipent la réponse négative.
- Le manque de confidentialité des bases du marché est un frein au dépôt de CVs.

Le CVU est basé sur une architecture Liberty Alliance, qui offre ainsi une possibilité d'anonymat (des bouts d'attributs seront à différents endroits).



Le CV Universel présentera des caractéristiques parmi lesquelles :

- Il est basé sur un format exploitable via le web – HR XML,
- Le CV du candidat est hébergé sur une plateforme sécurisée à laquelle le candidat peut accéder de partout dans le monde,
- Le CV contient 80% des informations demandées par les sites corporate ou jobboard,
- Les formulaires des sites corporate ou des jobboard sont remplis automatiquement lors de l'acte de candidature,
- Le CV peut être exporté au format Word, Html, pdf, etc si nécessaire,
- Il présente les informations de manière structurée et structurante, égale pour tous les candidats.

4- DEBAT, PARTAGE D'IDEES ET DE PROJETS : QUELLES SUITES DONNER A L'ATELIER ?

⇒ Point clef

Une suite possible de l'atelier pourrait consister à élaborer un panel de scenarios d'usage. Dans un deuxième temps, un travail de "mapping" des différentes solutions de fédération d'identité pourrait compléter ce travail.

A la suite de ces interventions, la phase d'échange a permis de conclure l'atelier autour de 3 points :

- Comment formaliser et rendre lisible un travail de cartographie des solutions de fédération d'identité ?
- Sur quels travaux antérieurs s'appuyer pour réaliser un glossaire, dont le manque se fait cruellement ressentir, notamment en français ?
- Quels projets stimulants peut-on identifier en la matière, pouvant servir de base à la réalisation d'actions collectives courant 2008 ?

A l'issue des échanges, **une proposition d'action se dégage plus particulièrement.**

Elle consisterait d'abord à élaborer des scenarios d'usage. Dans un deuxième temps, un travail de "mapping" des différentes solutions de fédération d'identité serait utile pour voir ce qui marche (ou non). Idéalement, le travail pourrait être prolongé par le recensement d'expérimentations pouvant s'inscrire (ou no) dans les cases ainsi définies par le travail de mapping.

Dans l'ensemble, il s'agirait de créer des niveaux d'abstraction (quelles philosophies derrière ces solutions appliquées à un projet ?) afin que chacun puisse ensuite se réappropriier ces enseignements en fonction de ces besoins propres.

D'autres manques ont été pointés, pouvant donner lieu à des actions qui restent à formaliser :

- Donner à l'utilisateur les moyens de contrôler ses données afin qu'il choisisse de tout gérer seul ou bien d'en déléguer la gestion à un tiers de confiance
- Besoin d'un lexique en langue française explicitant les différents termes évoqués lors de la journée et surtout, d'en cerner les différentes acceptations
- Créer un panel de solutions à présenter de manière la plus simple possible à l'utilisateur final ; poursuivre par un travail d'évaluation

- La question de la faible participation aux groupes de travail francophones sur les nouveaux standards est également pointée ; la mutualisation de ressources humaines au sein du programme ne permettrait-elle pas une représentation plus efficace ?
- La question de la réversibilité de l'utilisateur par rapport à son fournisseur est également montrée du doigt ; elle est une source d'innovation à creuser
- Enfin, les modèles économiques doivent être regardés avec plus d'attention. Quand on parle de fédération d'identité, il y a bien sûr le point de vue des usagers, qui utilisent ou pas la technologie, mais il y a aussi le point de vue de celui qui paye...



ANNEXE : PARTICIPANTS DE L'ATELIER

- 1 Kim Minh Kaplan - Afnic
- 2 Alexandre Israel – Bloggy Business
- 3 Daniel Breton - Cabestan
- 4 Alain Coetmeur - Caisse des Dépôts et Consignations
- 5 Arnaud Belleil - Cecurity.com
- 6 Thierry Cardona - CNIL
- 7 Olivier Salaün - CRU (Comité réseau des universités)
- 8 Bruno Deschemps - DGME
- 9 Marc Van Coillie - EifEL
- 10 Christophe Boutet - Entr'ouvert
- 11 Sylvie Sassi - ephi-formation
- 12 Renaud Francou - FING
- 13 Charles Nepote - FING
- 14 Daniel Kaplan - FING
- 15 Thierry Marcou – FING
- 16 Véronique Routin - FING
- 17 Ludovic Francesconi - GIE Cartes Bancaires
- 18 Thierry Nabeth - INSEAD
- 19 Eric Julien - kiosque-edu.com
- 20 Olivier Auber - KM2
- 21 Frederic Engel – Livo Market
- 22 Nicolas Guillaume - Microsoft
- 23 Bernard Ourghanlian - Microsoft
- 24 Charles Nouyrit – MyID.is
- 25 Christophe Ducamp - Fondation Open ID
- 26 Snorri Gorgietti - Fondation Open ID
- 27 Eric L'excellent - Orange
- 28 Emmanuel Kessous - Orange Labs
- 29 Sébastien Bertrand - Orange Labs
- 30 Alban Martin - Orange Labs
- 31 Aymeric Castelin - Orange Labs
- 32 Stéphane Guilloteau - Orange Labs
- 33 Alexis Davoux – Orange Labs
- 34 Anne-Sophie Pignol – Orange Labs
- 35 Laure De Ricqles – Orange Labs
- 36 Stéphanie Fodor – Orange Labs
- 37 Cristina Hoffmann – Orange Labs
- 38 Alexis Mons – Groupe Reflect
- 39 Mylene Ramm - Renupi (Repères numériques de Picardie)
- 40 Fulup Ar Foll - SUN / Liberty Alliance
- 41 Guillaume de Maussion - Teleneo
- 42 Pierre Levy - Ville de Paris
- 43 Didier Perret - Ville de Paris
- 44 Jean-Michel Planche - Witbe
- 45 Jean-François Ruiz – Ziki
- 46 Jean-Christophe Capelli

