La vie privée dans les environnements fédérés

Kheira Bekara, Maryline Laurent

La vie privée dans les environnements fédérés

Kheira BEKARA, Maryline LAURENT
Institut Télécom, Télécom SudParis, SAMOVAR UMR 5157,
9 rue Charles Fourier, 91011 Evry, France

Cet article présente la problématique de la vie privée telle qu'appliquée aujourd'hui dans les systèmes de fédération d'identité Liberty Alliance et CardSpace. Il présente ensuite de façon succincte le projet FC^2 de fédération de cercle de confiance et les principaux éléments fonctionnels du module Privacy permettant de contrôler la bonne application de la législation en matière de vie privée.

I. La fédération d'identité et le besoin de respect de la vie privée

A. Fédération d'identité

L'identité numérique peut être définie comme la représentation numérique de l'ensemble des informations connues sur une personne. Elle comprend les logins de cette personne, ainsi que ses données personnelles couramment appelées « attributs d'identité » ou « attributs ». Depuis plusieurs années, l'idée de gérer des identités numériques sur plusieurs domaines d'administration a émergé et est plus connue sous le nom de « fédération » [1] [2]. Concrètement elle consiste à établir des liens (dits fédérations) entre les différentes identités d'un utilisateur donné.

Deux schémas de fédération d'identités se présentent actuellement : celui centré sur l'utilisateur et celui centré sur le fournisseur d'identité (Identity Provider ou IdP). Dans le premier schéma d'architecture, la gestion des liens de fédération d'identités est à la charge de l'utilisateur. Quant au deuxième schéma, les liens de fédération sont gérés par l'IDP.

L'objectif de la fédération est de fournir aux utilisateurs un environnement sécurisé leur permettant de fédérer leurs identités et de gérer leurs attributs.

Les systèmes de fédération reposent généralement sur deux entités principales : les fournisseurs d'identités qui gèrent les identités des individus, et les fournisseurs de services (Service Provider - SP), qui offrent des services applicatifs aux abonnés. Notez que SP est également connue sous le nom de « RP » (Relying Party) dans les approches de type InfoCard [3]. Notez également que la notion de cercle de confiance fait référence à l'ensemble des IDP et SP ayant établi, par le biais de contrats, des relations de confiance pour fournir aux utilisateurs un environnement sécurisé de fédération.

Deux solutions majeures appelées InfoCard [3] et Liberty Alliance [4][5][6] mettent en œuvre la fédération d'identités.

Le projet Liberty Alliance (ultérieurement dénommée Liberty) a abouti à la définition d'une norme ouverte et de certaines spécifications techniques. Il vise à rendre interopérables des cercles de confiance hétérogènes et établit des guides de bonne pratique de la fédération d'identité. Liberty est basé sur un modèle de fédération de type centralisé autour d'IdP. Elle repose essentiellement sur SAML et des mécanismes Single Sign On (SSO) [7] avec introduction de la vie privée et définition de pseudonymat et d'intraçabilité. Les pseudonymes peuvent être utilisés à la place des identifiants réels dans les communications entre IdPs et SPs.

InfoCard est un standard de gestion d'identités mise en place par Microsoft. Il est basé sur le concept de « méta-système d'identité ». Ce standard (inspiré des travaux de Kim Cameron [7]) est conçu pour se conformer aux lois/règles sur l'identité.

Le méta-système associé (CardSpace) fournit une représentation de l'identité sous la forme de cartes virtuelles. L'architecture InfoCard est centrée sur l'utilisateur, ce qui signifie que les différents échanges entre l'IDP et le SP passent par l'utilisateur.

Le standard InfoCard est basé sur des échanges XML et un protocole sécurisé compatible Web Service (WS-Security, WS-Trust, WS-MetadataExchange et WS-SecurityPolicy).

Le concept de l'InfoCard est assez simple car il se réfère à l'identification telle que nous la connaissons dans le monde réel avec nos cartes d'identité physiques. Dans une architecture à base d'InfoCards, un IdP fournit à un utilisateur des métadonnées qui lui permettent d'obtenir un certificat au travers de son client WS-Trust. L'IdP à l'origine de ce certificat est représenté graphiquement, dans l'implémentation Cardspace, sous la forme d'une carte (appelée InfoCards).

Chaque carte correspond donc à un profil, qui peut être utilisé dans une ou plusieurs situations. L'information exprimée par la carte (appelée claims) est stockée au niveau de l'IdP, contrairement aux métadata permettant la recherche des données (stockées au niveau du sélecteur d'identité). Un utilisateur peut ensuite utiliser l'une

de ses cartes pour s'identifier auprès d'un RP qui fait confiance à l'émetteur IdP. Une interface permet à l'utilisateur de sélectionner l'une de ses cartes.

B. Problématique de vie privée dans la fédération d'identité

Dans l'approche Liberty centrée IDP, le stockage des données des utilisateurs, et la fédération de leurs identités se passent au niveau des IdPs. Ainsi, l'utilisateur possédant un simple navigateur peut décider de fédérer ses identités à deux instants, lorsqu'il s'authentifie auprès d'un IdP et plus tard quand il interagit avec un SP.
Après avoir obtenu le consentement de l'utilisateur pour réaliser la fédération, le SP fait une demande de fédération à l'IdP, et il peut ensuite demander à l'IdP d'authentifier l'utilisateur.

Les échanges d'attributs associés à un utilisateur entre l'IdP et le SP au sein de Liberty font appel à un pseudonyme connu des deux entités (appelé alias), via un canal externe. Toutefois, le passage direct des attributs est possible dans les premiers messages d'authentification de l'utilisateur.

La norme précise aussi si l'utilisateur donne son consentement pour une authentification SSO seule, ou pour le partage d'attributs.

Un utilisateur peut retirer son consentement de fédération à un IdP ou SP en pratiquant la défédération (section 5.4.1.2 de [4] et section 3.4 de [6]). C'est-à-dire, il peut faire une défédération auprès d'un IdP et ainsi empêcher un SP de recouper ses actions préalables avec les suivantes. Comme l'usage simultané de pseudonymes différents avec un SP n'est pas possible, la défédération offre à l'utilisateur la possibilité d'interagir avec un SP sous deux pseudonymes différents à deux moments différents. Si la fédération se produit deux fois pour un même compte connu du SP, alors SP peut relier toutes les interactions à un même utilisateur (à condition qu'au moins une information commune permette d'associer les deux intéractions).

Le modèle de protection de la vie privée de l'utilisateur adopté par Liberty (notamment pour le framework IDWSF «Identity Web Services Framework»), se base principalement sur le modèle de sécurité associé à ce dernier [11].

Certaines fonctionnalités de protection de la vie privée sont assurées par ce modèle (authentification de l'utilisateur et du SP, confidentialité et intégrité des attributs pendant le transit), mais d'autres ne le sont pas encore [11] (intégrité des politiques stockées, agrégation des données, etc.)

La problématique principale en termes de protection de la vie privée dans l'approche Liberty est le traçage possible des activités de l'utilisateur par l'IdP, cependant une solution a été apporté avec les nouvelles spécifications Liberty, où les attributs de l'utilisateur sont stockés localement par ce dernier.

Dans l'approche InfoCard, via son environnement riche, l'utilisateur prend la décision d'accorder sa confiance au SP au moment où on lui demande de consentir à s'authentifier auprès du SP. Ceci est rendu possible par le fait que toutes les transactions liées à l'identité transitent systématiquement par l'utilisateur au travers de son sélecteur d'identité.
Aussi, lorsqu'un SP a besoin d'accéder à des informations provenant de plusieurs IdPs d'un même utilisateur, aucun lien entre les identités de l'utilisateur ne pourra être fait. Seul le SP, dans le cadre du besoin spécifique associé au service rendu à l'utilisateur et sous le contrôle de ce dernier, peut croiser des informations.

Côté fournisseurs de service, le seul inconvénient reste que les SPs sont incapables de vérifier les signatures électroniques de l'ensemble des IdPs dont il a besoin pour valider le niveau de confiance des informations reçues.

II. Le projet FC^2

A. Description

Le projet FC^2 (Fédération de cercles de confiance) [8] a débuté en 2007 pour une durée de trois ans. C'est un projet français qui vise à assurer l'interopérabilité entre les solutions CardSpace et Liberty et de fédérer des identités gérées per des systèmes hétérogènes. Dans ce cadre, une collaboration a été établie entre le projet FC^2, et le projet Higgins [12] qui a pour vocation la gestion d'authentification et d'identité. L'expérience utilisateur, l'architecture de fédération d'identité et l'intéropérabilité des systèmes hétérogènes fut les principaux axes de collaboration entre les consortiums des deux projets. Une plate-forme FC^2 est en cours de développement. Elle vise à démontrer que plusieurs cercles de confiance (Circle of Trust - CoT) hétérogènes – CoT bancaire, CoT télécom, CoT gouvernementaux (voir Fig. 1) - peuvent collaborer à l'émergence de nouveaux services en ligne sécurisés. Les difficultés techniques sont principalement dues à l'hétérogénéité des niveaux de sécurité auxquels il faut faire face lors du partage des identités et des attributs. De plus, de nouveaux modèles économiques sont à définir.

FC^2 propose une approche centrée sur l'utilisateur qui laisse une certaine latitude dans la gestion de

leurs identités. Un sélecteur d'identité au niveau du terminal aide les utilisateurs à sélectionner l'identité adéquate et à remplir les formulaires requis par le fournisseur de service visité de façon semi-automatique (mais toujours sous le contrôle de l'utilisateur). Ces identités sont connues par le système comme des « cartes virtuelles » ou « méta carte » (carte de cartes). Ces cartes sont gérées par un composant appelé « porte-feuille InfoCard ». Les cartes incluent des « cartes personnelles » qui sont hébergées dans le terminal de l'utilisateur, et des cartes « gérées ou auto-générées » qui contiennent des liens vers l'IdP (IP/STS) [3] en charge de la carte et des identités numériques de l'utilisateur.

B. La vie privée dans le projet FC²

Aujourd'hui, les politiques de vie privée au sens de la directive vie privée de l'UE [9] [10] doivent être appliquées. Les informations liées à l'identité ont besoin d'une protection forte dans la plate-forme FC² de gestion d'identité fédérée. Cet article propose un module Privacy qui suit le modèle centré sur l'utilisateur et qui vise à appliquer de façon technique la protection de la vie privée des utilisateurs dans les systèmes d'identité fédérée.

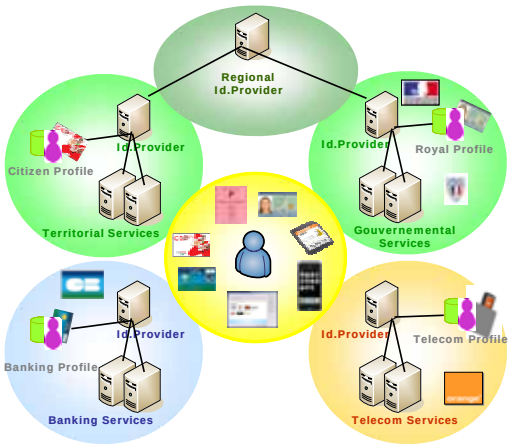


Fig.1. Vue globale de l'architecture du projet FC²

Le module Privacy a pour objectif de garantir le contrôle total sur les données personnelles. Chaque donnée personnelle est filtrée par le module Privacy avant d'être divulguée à un SP. En tant que tel, le risque d'accès non autorisé et d'utilisation abusive de ces données est en théorie éliminé.

Le module Privacy proposé explicite tous les flux transportant des données personnelles et donne à leur propriétaire un plus grand degré de contrôle. Le contrôle par l'utilisateur est géré par une interface conviviale présentée dans les Fig.2 et Fig.4. Le principe de base de notre architecture est de donner aux utilisateurs les principaux éléments liés à l'application de la vie privée sous formes d'onglets (voir Fig. 2) et un aperçu synthétique des données à caractère personnel en jeu (voir Fig . 4).

III. Module Privacy de FC²

Cette section présente le module Privacy [13], défini dans le projet FC² pour la mise en œuvre de la vie privée. Les fonctions relatives à la vie privée sont présentées dans la section III.A. L'exemple d'une transaction de commerce électronique décrit à la section III.B aide à mieux comprendre le rôle joué par le module Privacy.

A. Fonctions relatives à la vie privée

Fonction de définition de politiques
Cette fonction est requise à la fois du côté de l'utilisateur et du côté du serveur RP. Elle permet au serveur de définir sa politique de vie privée [4] par l'utilisation d'un éditeur spécifique. Elle aide l'utilisateur à définir / modifier ses préférences en matière de vie privée par le biais de menus déroulants.

Fonction de décision
Cette fonction génère une décision d'accès positive (autorisation) ou négative (ou interdiction) de façon semi-automatique. Pour cela, elle vérifie la compatibilité entre la politique de vie privée du RP et les préférences définies par l'utilisateur et attachées à une carte électronique sélectionnée par l'utilisateur pour la transaction.

Fonction de consentement
Cette fonction demande le consentement explicite de l'utilisateur à travers les deux fenêtres suivantes (voir Fig. 2) :

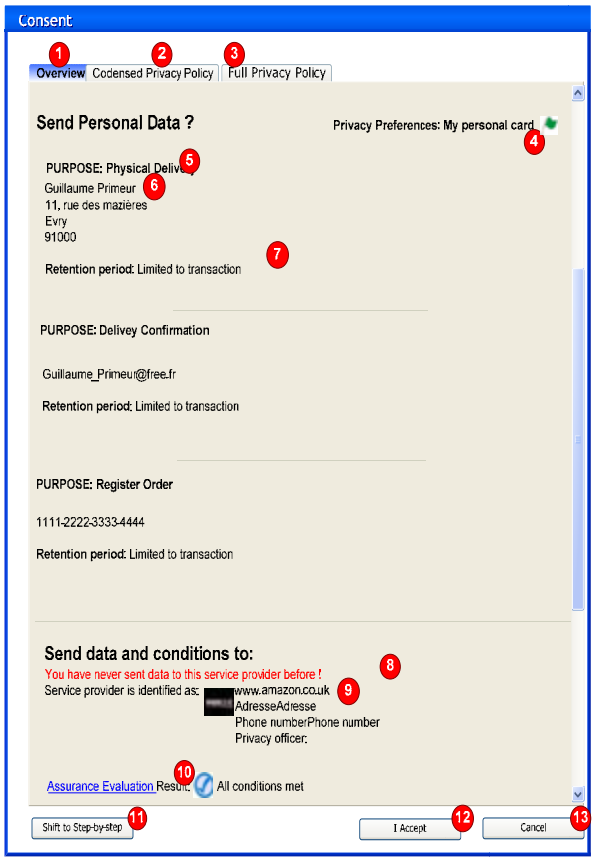
- La fenêtre de consentement simplifiée,
- La fenêtre de consentement avancée, qui contient les usages spécifiés par le RP pour les données requises, avec trois niveaux de détails (simple, moyen, avancé). Cette décomposition de la politique de vie privée du RP en trois niveaux permet aux utilisateurs avertis d'obtenir le détail de la politique et aux utilisateurs novices d'en obtenir une version simplifiée.

Fonction de log
Cette fonction enregistre tout l'historique des transactions.

Fonction d'assurance
Cette fonction définit un niveau d'assurance qui est présenté à l'utilisateur comme gage du bon respect de sa vie privée par le RP, c'est-à-dire en conformité vis-à-vis des conditions et exigences qu'il a lui-même fixées.

Fonction d'audit

Cette fonction effectue un contrôle périodique sur les décisions prises par la fonction de décision.



1. Overview tag : résumé des attributs demandés, les objectifs et période de rétention pour lesquels les attributs sont demandés par le RP
2. Condensed privacy policy tag : second niveau de présentation de la politique de confidentialité du RP
3. Full privacy policy tag : politique de confidentialité du RP dans sa totalité
4. My personal card : nom de la carte en service pour la transaction. Cliquer sur le drapeau conduit à accéder au profil: « Ma carte personnelle »
5. Purpose : objectif pour lequel des données sont demandées
6. Value : valeur des attributs demandés, fournie par la carte sélectionnée
7. Retention period : période pendant laquelle les données seront stockées par RP
8. Alarm : messages d'avertissement à l'utilisateur
9. Information : informations relatives au RP
10. Assurance level : niveau d'assurance minimale fournies par le RP
11. Shift to Step-by-step : les utilisateurs avertis ont la possibilité d'obtenir la politique de vie privée du RP et de valider cette politique étape par étape
12. I Accept : acceptation de la politique de vie privée du RP
13. Cancel : annulation de la transaction en cours

Fig. 2. Fenêtre de consentement de l'utilisateur et légende associée

B. Module Privacy illustré sur l'exemple d'une transaction électronique

Le module Privacy se présente sous la forme d'un intergiciel qui vise à respecter la législation en matière de vie privée. Comme le montre le scénario de commerce électronique présenté à la Fig. 5, le module est distribué sur le terminal de l'utilisateur ainsi que les fournisseurs de services (SP ou RP). L'approche centrée utilisateur CardSpace suivie dans FC^2 implique que le module Privacy interfère avec le sélecteur d'identité et le portefeuille de cartes du côté de l'utilisateur.

Le scénario choisi met en scène une application en ligne de vente de livres. Trois cercles de confiance (COT) sont impliqués dans le scénario, le CoT bancaire, le CoT Télécom et le CoT e-commerce.

Comme le montre la Fig. 2, les données personnelles demandées par le fournisseur de service pour rendre le service comprennent : le nom de l'utilisateur, son adresse, et son numéro de carte de crédit. Nous supposons que l'utilisateur visite ce site de vente en ligne pour la toute première fois.

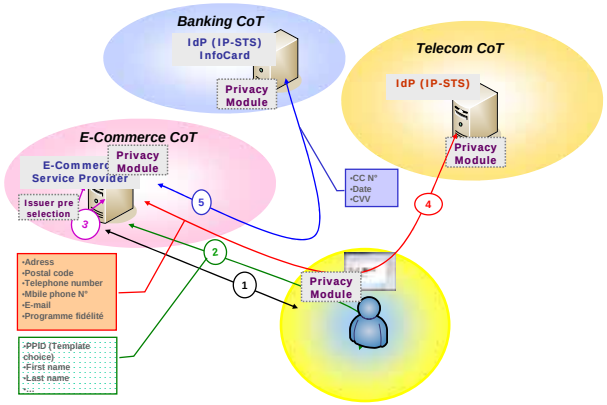


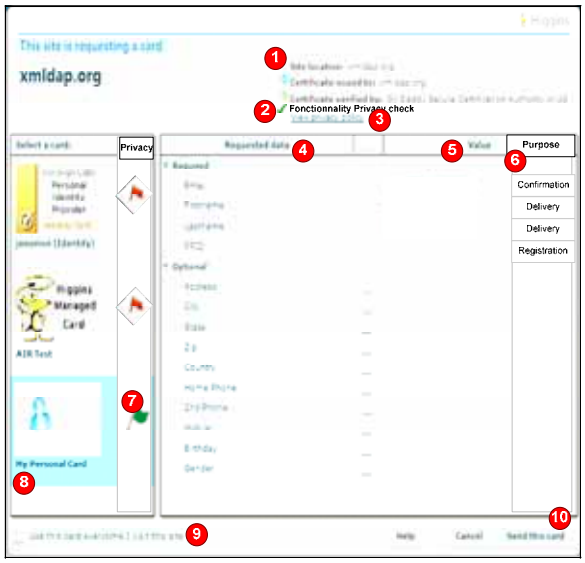
Fig.3 . Scénario de commerce électronique avec les différents échanges

La Fig. 3 illustre les étapes nécessaires à la prestation de vente en ligne de la plate-forme FC^2. La procédure débute par l'utilisateur qui demande l'accès au fournisseur de service RP de commerce électronique (étape 1). À la réception de la demande, le RP demande des données personnelles (Nom, Prénom – cf. Fig.3 étape 2). À supposer que l'utilisateur est en cours d'utilisation d'une carte personnelle, il n'a donc pas besoin de s'authentifier et peut accéder au site Web de façon anonyme en fournissant un identifiant PPID (Private Personal Identifier) généré aléatoirement par la carte.

Par la suite, d'autres données certifiées à caractère personnel sont demandées, et une carte gérée ou

auto-générée (cf. section II.A s'avère nécessaire. Le RP sélectionne un IdP de confiance avec lequel il a déjà établi un contrat de confiance (Telecom IdP) (Fig.3 étape 3), et se connecte à celui-ci (CoT Télécom - Fig.3 étape 4). Le RP demande les données nécessaires par l'envoi d'un message ClaimsRequest qui contient une balise « Object » (pour démarrer le sélecteur d'identité) et un en-tête P3P qui aide à localiser la politique de vie privée du RP (par exemple URI) pour le service demandé (Fig.3 étape 5).
Du côté utilisateur, à la réception de la demande du RP, le sélecteur d'identité affiche les cartes du portefeuille et les attributs obligatoires (et optionnels). Les cartes liées à l'IDP sélectionné par le RP sont alors activées.

Une fois une carte sélectionnée, le module Privacy de l'utilisateur vérifie ensuite la compatibilité entre la politique de vie privée du RP (à savoir sa politique de collecte et de traitement des attributs) et les préférences de l'utilisateur pour la carte sélectionnée. Ces préférences sont récupérées auprès du portefeuille de cartes. Par le biais de l'interface mentionnée à la Fig.4, le module Privacy interfère avec l'utilisateur. Il affiche certains éléments associés à la gestion de la vie privée du RP, comme son statut (Privacy status – cf. Fig.4). Il affiche aussi les attributs demandés par le RP, l'objectif pour lequel ils sont collectés, et le drapeau « privacy check flag » qui permet en un coup d'œil à l'utilisateur de savoir si une carte de son portefeuille satisfait ou non, par les préférences qui y sont associées, la politique de vie privée du RP. L'utilisateur peut ainsi contrôler ses attributs qui sont sur le point d'être communiquées au RP et peut décider de transmettre les attributs obligatoires uniquement.
Avant d'accepter la transaction, l'utilisateur peut visualiser la politique de vie privée du RP grâce à la fenêtre de la Fig. 4 en cliquant sur « View privacy policy ». Il peut également afficher la politique de vie privée du RP liées aux attributs demandés en cliquant sur l'un des drapeaux à côté d'une carte.
Notons que le module Privacy prend certaines décisions de façon semi automatique après vérification de la compatibilité entre la politique de la vie privée du RP et les préférences de l'utilisateur. Comme l'illustre la Fig.4, l'utilisateur ne peut activer que l'une des cartes dont la compatibilité a pu être vérifiée pour interagir avec le RP.



1. Site location : informations sur le RP requérant les attributs de l'utilisateur
2. Privacy status : score calculé après avoir confronté en local la politique de vie privée du RP vis-à-vis des préférences de l'utilisateur
3. Privacy policy : lien vers la politique de vie privée du RP
4. Requested data : attributs obligatoires ou optionels demandés qui ne sont pas encore remplis
5. Purpose : objectif pour lequel les attributs sont demandés
6. Privacy check flag : vérification de la compatibilité de la politique du RP vis-à-vis des profils attachés aux cartes
7. Personal card : la carte personnelle dont les préférences sont compatibles avec la politique de vie privée du RP est présélectionnée par le système. Ici, seule la troisième carte "My Personal Card" est compatible, comme le montre le drapeau « Privacy check flag » qui est de couleur verte (alors que les deux autres sont rouges)
8. Use everytime : possibilité offerte à l'utilisateur de déterminer une carte spécifique (et donc un profil) pour les transactions suivantes avec ce même RP
9. Send this card : consentement global de l'utilisateur pour envoyer les attributs demandés attachés à cette carte

Fig. 4. Sélecteur d'identité illustrant les attributs demandés par le RP et la légende associée

IV. Conclusions

Cet article présente la problématique de la vie privée dans les systèmes de fédération d'identités, et notre contribution pour assurer la protection des données personnelles dans les environnements fédérés. Ce travail se réfère à la loi actuelle sur le respect de la vie et propose une solution technique pour faire appliquer cette législation. Un prototype du module Privacy est en cours de développement. Des travaux de recherche complémentaires sont également en cours sur la négociation de politiques de vie privée.

Remerciements

Les auteurs tiennent à remercier les autorités régionales et nationales pour le soutien financier du projet FC^2, et le consortium FC^2 pour les discussions fructueuses.

Références

[1] http://shibboleth.internet2.edu. Shibboleth, internet2.
[2] http://www.projectliberty.org. Liberty alliance project.
[3] *CardSpaceFramework* en ligne: http://msdn.microsoft.com/fr-fr/netframework/bb902784.aspx
[4] *Liberty Alliance Project: Liberty Architecture Overview*, Version 1.0, 11 July 2002
[5] *Liberty Alliance Project: Liberty Protocols and Schemas Specification*, Version 1.0, 11 July 2002
[6] *Liberty Alliance Project: Liberty Bindings and Profiles Specification*, Version 1.0, 11July 2002
[7] K. Cameron (2005) "*The laws of identity*", Microsoft Corporation
[8] http://www.fc2consortium.org/project.html
[9] *Directive 95/46/EC of the European Parliament* and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Official Journal* L No.281, 23 Nov 1995. En ligne: http://www.cdt.org/privacy/eudirective/EU Directive .html.
[10] *Directive 2002/58/EC of the European Parliament* and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector, brussels. *Official Journal* L No.201, 31 Jul 2002. En ligne: http://www.etsi.org/public-interest/Documents/Directives/Standardization/Data Privacy Directive.pdf.

[11] http://www.projectliberty.org/liberty/content/download/327/2405/file/liberty-idwsf-security-privacy-overview-v1.0.pdf
[12] http://www.eclipse.org/higgins/index.php
[13] http://wss.fc2.copilotpartners.com/sp2/Docs%20SP1Lot4GT1/Forms/AllItems.aspx?RootFolder=%2fsp2%2fDocs%20SP1Lot4GT1%2fGT1%20-%20Sp%C3%A9cification%20des%20composants%20innovants&FolderCTID=&View={F184B13A-B1D1-488D-9B98-4702CC343C93}