



Méta-système et mash-up des identités avec les produits et technologies Microsoft

Version 1.0

Publication : Décembre 2010

Auteur : Philippe Beraud (Microsoft France), Stéphane Goudeau (Microsoft France), Benjamin Guinebertière (Microsoft France)

*Copyright*

*© 2010* [*Microsoft Corporation*](http://www.microsoft.com)*. Tous droits réservés.*

Résumé

Ce livre blanc permet de mieux appréhender les scénarios qui peuvent se matérialiser aujourd’hui par la simple concrétisation du méta-système d’identités au sein de l’entreprise, entre organisations, dans le nuage et avec les réseaux sociaux.

Dans ce cadre, le document revient sur les différentes initiatives, et standards relatifs à l’identité et met en évidence les axes d’interopérabilité tels que rendus possibles par les produits et technologies Microsoft.



© 2010 Microsoft Corporation. Tous droits réservés.

Les informations contenues dans ce document représentent le point de vue actuel de Microsoft Corporation sur les sujets traités à la date de publication. Etant donné que Microsoft doit s’adapter aux conditions changeantes du marché, ces informations ne doivent pas être interprétées comme un engagement de la part de Microsoft, et Microsoft n’est pas en mesure de garantir l’exactitude de toute information présentée après la date de publication.

MICROSOFT NE DONNE AUCUNE GARANTIE EXPRESSE OU IMPLICITE DANS CE DOCUMENT.

Les autres noms de produits ou de sociétés cités dans ce document peuvent être des marques de leurs propriétaires respectifs.

Microsoft Corporation • One Microsoft Way • Redmond, WA 98052-6399 • Etats-Unis

**Sommaire**

[1 Notions de méta-système et de mash-up d’identités 2](#_Toc282507755)

[2 Protocoles et formats de jetons de sécurité 7](#_Toc282507756)

[2.1 Identités numériques d’entreprise 7](#_Toc282507757)

[2.1.1 Fédération des identités « Front-Channel » 7](#_Toc282507758)

[2.1.2 Fédération des identités « Back-Channel » 10](#_Toc282507759)

[2.1.3 Sélection du fournisseur d’identité 19](#_Toc282507760)

[2.2 Identités numériques sociales/grand public 20](#_Toc282507761)

[2.2.1 Windows Live ID 20](#_Toc282507762)

[2.2.2 Open ID 21](#_Toc282507763)

[3 Scénarios de mise en œuvre 23](#_Toc282507764)

[3.1 Cadre d’illustration avec les technologies Microsoft 23](#_Toc282507765)

[3.1.1 Microsoft Windows Identity Foundation (WIF) 1.0 24](#_Toc282507766)

[3.1.2 Microsoft Active Directory Federation Services (AD FS) 2.0 27](#_Toc282507767)

[3.1.3 Microsoft Windows Azure AppFabric platform Access Control Services (ACS) 2.0 30](#_Toc282507768)

[3.2 Scénarios B2B de collaboration fédérée entre organisations 31](#_Toc282507769)

[3.2.1 Accès à un site de collaboration SharePoint 2010 31](#_Toc282507770)

[3.2.2 Accès à sa boîte aux lettres Outlook Web Access 2010 33](#_Toc282507771)

[3.2.3 Accès à une application Web 35](#_Toc282507772)

[3.2.4 Accès à un service Web RESTful 36](#_Toc282507773)

[3.3 Scénarios B2C/G2C pour le grand public 36](#_Toc282507774)

[3.4 Expérimentation de ces scénarios au MTC Paris 39](#_Toc282507775)

[4 Et le respect de la vie privée ? 40](#_Toc282507776)

[5 En guise de synthèse 44](#_Toc282507777)

[6 Pour en savoir plus… 45](#_Toc282507778)

[7 Restons en contact 46](#_Toc282507779)

# Notions de méta-système et de mash-up d’identités

La complexité de mise en œuvre et de gestion de l’authentification et du contrôle d’accès aux applications et aux autres ressources d’une organisation rend difficile la tâche des développeurs et des professionnels de l’informatique pour satisfaire aux besoins de leur organisation.

La plupart des applications, quels que soient la plateforme logicielle et l’environnement technique, s’appuient sur des identités. Une identité numérique est, d’une façon générale, un ensemble d’informations à propos d’une entité, telle qu’un utilisateur. Les informations d’identité influencent le comportement des applications - elles déterminent ce qu’un utilisateur est autorisé à faire, contrôlent la façon dont l’application interagit avec l’utilisateur, par exemple.

La notion d'identité est essentielle, mais travailler avec les identités est devenu difficile : en fonction de la situation et du contexte d’accès à mettre à disposition, de très nombreux choix de technologies (et de standards) en matière d’identité sont possibles, avec à la clé de multiples représentations (et protocoles), ainsi qu’une diversité de modèles de programmation fonction des éléments précédents et/ou des environnements techniques.

Cette multiplicité de technologies d’identité, de protocoles et de formats de jetons de sécurité induit une complexité et un coût d’implémentation notable dans un contexte donné, sans pour autant parvenir à satisfaire l’ensemble des scénarios d’accès souhaités que ce soit au sein d’un même domaine de sécurité et/ou , entre domaines de sécurité, et ce avec les exigences associées en termes de sécurité.

Il n’est donc pas rare de voir une solution tactique bloquer une interopérabilité future : les applications deviennent dépendantes d’une technologie…ET bornées par les contraintes de la technologie choisie.

S’ajoute à cela la difficulté à interopérer avec des applications et des systèmes hétérogènes et à adapter ces mêmes applications à de nouveaux scénarios émergents comme les services hébergés, etc. ; les architectures orientées service (*Service Oriented Architecture* en anglais ou SOA en abrégé) amplifiant les défis ainsi posés.

Kim Cameron, architecte en chef de l’identité numérique chez Microsoft, lançait, il y a maintenant plus de quatre ans au travers de son blog <http://www.identityblog.com>, une large initiative visant à améliorer la sécurité et l’interopérabilité des identités en ligne.

Suite à l’expérience Microsoft Passport ou Windows Live ID (aujourd’hui) (Cf. section éponyme § 2.2.1) qui est un succès en termes de fournisseur d’identités pour MSN (avec plus de 520 millions d’utilisateurs et plus d’un milliard d’ouvertures de session/jour) mais également un échec comme fournisseur d’identités pour l’Internet, cette initiative s’est d’abord concentrée sur le développement et le partage d’une compréhension formelle des dynamiques amenant des systèmes d’identités numériques en ligne à être couronnés succès ou, au contraire à échouer et ce, dans différents contextes. Les larges discussions qui s’en sont suivi avec l’industrie, les associations de défense des libertés individuelles, etc. ont conduit à établir un consensus autour de 7 lois de l’identité qui sont discutées dans le livre blanc [The Laws of Identity](http://www.identityblog.com/?p=354)[[1]](#footnote-1).



Prises dans leur ensemble, ces lois définissent un « méta-système d’identités unifié » qui offre à l’Internet les fondations d’une couche Identité qui, de façon évidente, lui fait défaut. La réponse à un tel défi offre la possibilité de créer, sur la toile, des solutions et des services interopérables très sécurisés à même d’offrir à leur tour au grand public, aux administrations et aux entreprises plus de choix, de flexibilité et de sécurité dans leur utilisation d’Internet au quotidien. Elle est donc bénéfique pour tous.

Un méta-système d’identités (système de systèmes d’identités) constitue une architecture interopérable pour l’identité numérique qui présume que les personnes disposent de plusieurs identités numériques basées sur de multiples technologies/protocoles, implémentations et fournisseurs sous-jacents.

Une telle approche permet de transcender les frontières dans de multiples dimensions et simultanément entre :

* Les secteurs industriels, le secteur public, etc. fonction du scénario ;
* Les entreprises et les institutions dans le contexte du scénario considéré ;
* Les protocoles mis en œuvre dans ce cadre ;
* Les environnements techniques et plateformes utilisées ;
* Les produits et technologies d’identités et de sécurité mis en œuvre pour rendre le service ;
* Et bien sûr les exigences en termes d’identité (allant d’une vérification forte de l’identité à un commentaire anonyme).

Elle permet non seulement, pour les scénarios visés, aux personnes d’être au contrôle, au travers le cas échéant de la notion de « sélecteur d’identités » ou d’autres agents utilisateur, de leurs identités et de l’usage qui en est fait, mais également aux organisations de pouvoir continuer à utiliser et bénéficier de leur investissements existants en termes d’infrastructure d’identités, de choisir la technologie d’identités qui leur est la mieux appropriée, et de plus de migrer facilement d’anciennes technologies vers de nouvelles technologies sans pour autant sacrifier l’interopérabilité avec les autres.

Les organisations recherchent l’interopérabilité pour pouvoir utiliser la mosaïque de technologies la plus proche de leurs besoins. L’interopérabilité (de la gestion) des identités entre plateformes et le Web (sites Web et services Web) est particulièrement importante pour l’amélioration de la valeur des technologies pour les administrations, les entreprises et le grand public.

Le livre blanc [The Identity Metasystem](http://www.identityblog.com/?p=355)[[2]](#footnote-2) présente, en partant des conclusions et du large consensus des lois de l’identité, une architecture ouverte et interopérable pour construire un tel méta-système et décrit comment participer à ce méta-système d’identités qui, par nature, n’appartient à et n’est contrôlé par personne en particulier.

L’approche ainsi proposée vise à la base à :

1. Définir l’identité numérique comme un ensemble de revendications (*claims* en anglais) qui caractérise un utilisateur (ou entité) dans le monde numérique ;
2. Externaliser l’authentification de l’application (voir également le contrôle d’accès).

*« Stop hard-coding security into applications and stop creating operating system (OS)-level accounts on servers. Consume these as services external to the application.* »

Neil MacDonald 13 April 2006

Gartner Group: Achieving agility: building blocks for a policy-driven, agile security services infrastructure

Différentes parties participent au méta-système de diverses façons.

Comme illustré dans la Figure 1, les trois rôles canoniques au sein du méta-système sont les suivants :

* *Le Sujet (personne ou entité autre) sur lequel des revendications sont effectuées* : « *Ce que vous dites sur vous-mêmes ou ce que d’autres disent sur vous* »- Des exemples de sujets sont des utilisateurs particulier et/ou professionnel, des entreprises, des administrations, etc.
* *Le Fournisseur d’identités qui émet les identités numériques (Identity Provider en anglais ou IdP en abrégé)* - Par exemple, les gouvernements peuvent émettre des identités pour leurs citoyens, les sites de commerce en ligne peuvent émettre des identités pour leurs clients, les fournisseurs de cartes de crédit peuvent émettre des identités permettant le paiement, et les utilisateurs finaux peuvent utiliser des identités auto-émises dans les contextes où cela est acceptable comme lors de l’ouverture de session sur des sites Web.

Schématiquement, un fournisseur d’identités constitue une autorité qui fait des revendications sur un sujet. Ces revendications sont physiquement transportées dans ce que nous allons appeler des jetons (d’authentification et/ou d’autorisations). Pour cela, le fournisseur d’identités implémente un service de distribution de jetons (*Security Token Service* en anglais ou STS en abrégé) qui émet les jetons. En d’autres termes, un jeton représente l’identité émise par le fournisseur d’identités. Les demandes (authentifiées) de jetons sont effectuées à l’aide de protocoles standards.

Les jetons sont utilisés par des consommateurs d’identités qui font confiance au STS.

* *Les Parties en confiance ou Consommateurs d’identités (Relying Party en anglais ou RP en abrégé) qui requiert des identités* - Par exemple, une application comme un site Web d’une organisation qui utilise des identités offertes et validées par d’autres organisations dignes de confiance pour la délégation de l’authentification (voir des autorisations).



*Figure 1 – Rôles canoniques du méta-système.*

Aujourd’hui, une application récupère typiquement une seule information d’identité simple telle qu’un nom d’utilisateur. Pour avoir davantage d’informations, l’application doit interroger un référentiel distant tel qu’un service d’annuaire et/ou une base de données locale.

Avec une identité fondée sur des revendications, chaque application peut demander exactement les revendications dont elle a besoin ; un STS les place dans le jeton qu’il crée. Dans la pratique, une revendication peut :

* Identifier un utilisateur,
* Véhiculer l’appartenance à un groupe ou à un rôle,
* Transporter des informations de personnalisation comme le nom à afficher pour un utilisateur,
* Donner ou dénier le droit de faire quelque chose comme l’accès à une information particulière ou l’invocation de méthodes spécifiques,
* Limiter le droit de faire quelque chose comme un montant de délégation,
* Etc.

Ceci peut supposer, le cas échéant, pour le consommateur d’identités, une évolution bénéfique de l’application considérée de façon à externaliser, dans les faits, son authentification.

Dans de nombreux cas, les participants dans le méta-système sont susceptibles de jouer plus d’un rôle. De ce fait, le méta-système d’identités contribue à établir au global un écosystème de confiance.

A ce titre, un quatrième rôle peut être introduit dans ce modèle, en l’occurrence celui de Fournisseur d’attributs (*Attribute Provider* en anglais ou *AtP* en abrégé) qui émet des revendications additionnelles vis-à-vis de l’identité numérique considérée dans le contexte. En effet, pour un scénario donné, le fournisseur d’identité ne dispose pas forcément des informations nécessaires pour produire l’ensemble des revendications nécessaire pour satisfaire la politique de sécurité du consommateur d’identité.

L’authentification initiale auprès d’un fournisseur d’identité et l’émission sur cette base d’un jeton d’authentification peut servir à l’obtention, sous forme d’un autre jeton, de revendications complémentaires en fonction du contexte auprès d’un tel fournisseur de façon à disposer au final d’une identité composite qui réponde aux exigences du consommateur d’identité. On parle ici de « mash-up» d’identité comme suggéré par la Figure 2.

Cette identité composite peut se présenter sous la forme :

* D’un nouveau jeton dans lequel l’identité résultante est fondée sur les revendications issues du fournisseur d’identité et sur celles additionnelles en provenance d’un ou de plusieurs fournisseurs d’attributs ;

-ou-

* Du jeton émis initialement par le fournisseur d’identité et du ou des jetons émis par le ou les fournisseurs d’attributs. L’identité résultante est portée par l’ensemble des jetons. Il peut s’avérer nécessaire dans cette seconde situation de prouver la corrélation entre ces jetons.



*Figure 2 – Rôles étendus du méta-système.*

Au-delà de ces principes fondateurs, abordons à présent la diversité des protocoles (et des jetons de sécurité à embrasser) avant d’illustrer dans un second temps au travers d’un certain nombre de scénarios concrets combien il est facile de participer au méta-système d’identités quelle que soit la plateforme ou la technologie utilisée.

La mise en œuvre des produits et technologies Microsoft sera mise en perspective dans ce cadre à la section § 3 Scénarios de mise en œuvre.

# Protocoles et formats de jetons de sécurité

## Identités numériques d’entreprise

[Wikipedia](http://en.wikipedia.org/wiki/Federated_identity)[[3]](#footnote-3) définit la fédération des identités comme suit:

« *Federated identity, or the ‘federation’ of identity, describes the technologies, standards and use-cases which serve to enable the portability of identity information across otherwise autonomous security domains. The ultimate goal of identity federation is to enable users of one domain to securely access data or systems of another domain seamlessly, and without the need for completely redundant user administration.* »

Cette première section s’intéresse aux standards de fédération qui permettent de matérialiser au travers de leurs diverses implémentations une identité « portable » entre domaines de sécurité.

Les collaborations de type B2B (Business to Business en anglais) ou G2G (Government to Government en anglais) entrent typiquement dans ce cadre.

### Fédération des identités « Front-Channel »

La fédération d’identité est bien souvent perçue en premier lieu comme le moyen de disposer d’une authentification Web unique (*Web Single Sign-on* en anglais ou Web SSO en abrégé) fédérée à destination des portails et sites Web de façon à établir une collaboration fédérée entre organisations et domaines de sécurité afférents, i) l’authentification étant réalisée au sein du domaine de sécurité où l’identité est déclarée et ii) la ressource accédée se situant dans un autre domaine de sécurité qui a délégué l’authentification.

Par rapport à des ressources de type portails et sites Web, on parle ici plus spécifiquement de fédération des identités « Front-Channel » qui est l’objet de cette section.

La section suivante s’intéresse à la fédération des identités « Back-Channel » au-delà des portails et sites Web, à savoir la fédération à destination des échanges de messages/données via services Web entre entités fédérées et l’ensemble des « Back-End » impactés.

**Il existe aujourd’hui différentes approches technologiques de la fédération des identités « Front-Channel », voire potentiellement sous forme de différentes versions pour une même proposition protocolaire. Ceci traduit le fait qu’au demeurant aucune spécification n’est universellement adoptée à ce jour.**

Essayons d’y voir un peu plus clair.



Le projet [Liberty Alliance](http://www.projectliberty.org/)[[4]](#footnote-4) (LA en abrégé), dont l’ensemble du travail et des livrables a été transmis aujourd’hui à l’[Initiative Kantara](http://www.kantarainitiative.org/)[[5]](#footnote-5), au même titre que le projet [Shibboleth](http://shibboleth.internet2.edu)[[6]](#footnote-6) à l’initiative de l’Internet2/[MACE](http://middleware.internet2.edu/MACE)[[7]](#footnote-7) (Middleware Architecture Committee for Education) et d’une façon plus générale la communauté SAML ont profondément contribué à l’analyse et la compréhension de toute une série de cas d'utilisation et d’exigences associées, et les protocoles, formats et concepts proposés par ces groupes de travail ont été une étape importante pour tous ceux impliqués dans (la « portabilité » de) l'identité numérique.

oasis.png On peut ainsi citer les versions 1.0, 1.1 et 2.0 du standard SAML issus du [comité OASIS Security Services (SAML en abrégé) TC](http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security)[[8]](#footnote-8) ainsi que les spécifications ID-FF (*Identity Federation Framework* en anglais) 1.x du projet Liberty Alliance et Shibboleth 1.x du projet éponyme, qui constituent des extensions des versions 1.x du standard SAML.

Ces groupes de travail et projets doivent être remerciés pour leur contribution qui a fait indéniablement avancer la réflexion sur les différentes dimensions que recouvrent la définition précédente, notamment sur le plan des conditions relatives à la collaboration entre différentes entités, l’établissement d’un cadre de confiance intégrant les engagements et zones de responsabilité (juridique) de chacun, etc.

Sur le plan technique, si les spécifications SAML 1.x, ID-FF 1.x, Shibboleth 1.x et SAML 2.0 reposent sur des principes similaires, ces spécifications n’en ont pas pour autant systématiquement les mêmes fonctionnalités, les mêmes périmètres en termes de profils et de liaisons (*binding* en anglais), loin s’en faut. Par voie de conséquence, des implémentations potentielles de ces spécifications ne sont pas forcément interopérables entre elles. Principes et fonctionnement similaires ne sont pas synonymes d’interopérabilité.

L’initiative Kantara a repris l’activité de tests d’interopérabilité développée à l’origine par le projet Liberty Alliance pour les protocoles ID-FF et SAML.

Nous souhaitons souligner, au passage, que le projet Shibboleth désigne à la fois une spécification et une implémentation, à savoir un système distribué sous licence de logiciel libre. En tant que spécification, Shibboleth 1.x constitue à l’origine une extension du standard SAML 1.x ; ce dernier définissant un protocole pour échanger des informations liées à la sécurité de façon à traiter la problématique d'authentification unique Web. L’implémentation Shibboleth 2.x repose sur les spécifications SAML 2.0. Notons au passage que Shibboleth est aujourd’hui largement utilisé au sein des Universités en France dans le cadre de la [fédération Education-Recherche](http://federation.cru.fr/)[[9]](#footnote-9), un service rendu par le GIP RENATER.

Dans la pratique, la version 1.1 du standard OASIS SAML et les différentes versions de la spécification ID-FF, ont été prises en compte au même titre que d’autres contributions comme les spécifications Shibboleth 1.x, pour donner lieu à la version 2.0 du standard OASIS SAML.

Finalisé en 2005, le standard SAML 2.0 est désormais adopté aujourd’hui en lieu et place des propositions initiales du projet Liberty Alliance. Il en est de même pour le projet Shibboleth comme souligné ci-avant.

Parallèlement aux évolutions protocolaires précédentes, le protocole WS-Federation Passive Requestor Profile (WS-Fed PRP en abrégé) a été développé à l’origine par IBM, BEA Systems, Microsoft, VeriSign, et RSA Security en tant que branche à destination des navigateurs dans le cadre d’une initiative plus vaste à destination des services Web (Cf. section § 2.1.2.1 Prise en compte de la sécurisation des services Web de type SOAP et les besoins associés). Cette spécification a démontré en effet son large potentiel d’interopérabilité depuis 2004 avec l’atelier WS-Fed Protocol workshop (Microsoft, IBM, RSA, Oracle (Oblix), BMC (OpenNetwork), CA (Netegrity), Ping Identity).

oasis.png Ce protocole souvent appelé WS-Fed Passive est aujourd’hui repris, comme dérivé simplifié (profil à destination des navigateurs), à la section § 13 Web (Passive) Requestors du standard OASIS [Web Services Federation Language (WS-Federation) Version 1.2](http://docs.oasis-open.org/wsfed/federation/v1.2/ws-federation.pdf)[[10]](#footnote-10) issu du [comité technique OASIS Web Services Federation (WSFED)](http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wsfed)[[11]](#footnote-11). Il connait également aujourd’hui une audience certaine.

Pour autant, l’interopérabilité entre applications dans des environnements technologiques hétérogènes est une dimension essentielle de la collaboration entre organisations.

**Dans ce contexte et compte tenu des éléments précédents, le support simultané des protocoles SAML 2.0 et WS-Fed Passive et la disponibilité d’une passerelle entre les deux s’impose de façon à pouvoir réunir au sein d’un même scénario des organisations ayant effectué des choix protocolaires différents.**

Ainsi, dans le contexte d’une transaction donnée, et en fonction des acteurs en présence, une partie du dialogue peut s’effectuer selon l’un des protocoles supportés, et l’autre partie selon un autre protocole.

Ainsi, plus de 76% des plateformes d’identité proposent aujourd’hui une implémentation des standards SAML 2.0 et de WS-Fed Passive pour le support des identités fédérées « Front-Channel ». C’est le cas notamment avec Microsoft Active Directory Federation Services (AD FS) 2.0 (Cf. section éponyme § 3.1.2).

Il convient de noter au passage que l’authentification réalisée au niveau du fournisseur d’identité peut être déléguée à son tour en s’appuyant sur un autre protocole d’authentification Web unique, cette fois non fédéré, comme le protocole [CAS (Central Authentication Service)](http://www.yale.edu/tp/auth)[[12]](#footnote-12) développé à l’origine par l’université de Yale et dont les évolutions sont gérées aujourd’hui dans le cadre du [projet Jasig](http://www.jasig.org/cas)[[13]](#footnote-13). On retrouve ce type d’approche typiquement dans le contexte du projet Shibboleth (en tant que système distribué sous licence de logiciel libre), mais pas uniquement.

Ceci étant, disposer d’une identité fédérée pour des scénarios de Web SSO fédéré entre portails et sites Web constitue certes un premier pas important mais à l’évidence aujourd’hui insuffisant.

En effet, la notion de services accessibles dans un cadre de fédération ne se limite à l’accès des pages Web (statiques ou dynamiques) situées sur des sites Web fédérés. Il y a au-delà du site lui-même, pour le service invoqué, des échanges de messages avec des services (Web) de l’entité accédée (ou d’autres entités potentiellement situées au-delà du domaine de sécurité courant).

Ne serait-ce que vu d’un client passif (navigateur), de nombreuses questions restent sans réponse ou une réponse très limitée : sous quelle identité ces pages invoquent des services Web situés dans d’autres domaines de sécurité ? Quelle information d’identité véhiculent-ils ? Est-elle intelligible et digne de confiance pour le service invoqué ? Etc.

On sort ici du cadre d’application stricte des spécifications mentionnées précédemment et, en particulier, des spécifications SAML 2.0 et/ou WS-Federation Passive précédentes.

Le recours ici à une autre spécification, comme par exemple la spécification Liberty Alliance ID-SWF, induit un degré de complexité supplémentaire à ne pas négliger. Cette dernière repose en effet sur des fondements différents, introduit d’autres protocoles et n’adresse malheureusement la problématique posée que de façon très parcellaire.

En effet, que dire alors de services invocables directement sous forme de services Web depuis un client actif (client « intelligent » ou smart client en anglais) ?

Par ailleurs, la notion même de cercle de confiance statique introduit en son temps par ID-FF ne répond que très partiellement à la réalité des scénarios de mise en œuvre.

Pour embrasser la diversité des scénarios (et des acteurs potentiels), il apparaît nécessaire de supporter aussi bien des schémas de confiance directe, indirecte, par courtage (*brokering* en anglais) ainsi que la délégation.

Dès lors, une notion de cercle de confiance statique vole en éclat au profit d’un modèle de fédération complètement dynamique basé sur les cadres de confiance établis unitairement entre les acteurs et sur l'exposition, l'échange de métadonnées (politiques) (et potentiellement différents types de jetons de sécurité, etc.).

La diversité des cas d’usage (scénarios) de la fédération des identités (« *Front Channel* » vs. « *Back Channel* ») impose, en conséquence, de disposer d’une approche technologique ou d'un « *Framework* » plus vaste et offrant une flexibilité accrue :

* Support non seulement de clients passifs (navigateur) mais également et principalement de clients actifs (clients « intelligents » ou smart client en anglais) à même de consommer intelligemment les métadonnées exposées par les portails, les sites et/ou les services Web ;
* Consommation (et exploitation) dynamique des métadonnées (politiques de sécurité, de fédération, etc.) exposées par les portails, les sites et/ou les services Web ;
* Support (émission, échange, validation, etc.) de multiples formats de jetons de sécurité (SAML évidemment mais au même titre les certificats X.509, les tickets Kerberos, etc. ou d’autre futurs formats selon les contextes) et abstraction de ce dernier pour les sites et services Web au travers de la notion de collection de revendications (claims en anglais).
* Consommation des métadonnées et le support (dynamique) de l’ensemble des schémas de confiance qui peuvent se présenter  (confiance directe (avec ou sans nécessité de multiples jetons de sécurité émanant de multiples fournisseurs d’identités), confiance indirecte avec présence d’inter-médiateur(s) de confiance, délégation avec confiance directe, délégation avec confiance indirecte) ; ceci permet de passer d’un modèle fondé sur ce que l’identité possède (ses crédentités ou informations de sécurité) à un modèle basé sur ce que la ressource fédérée accédée exige. Ceci induit une voie d’extension sans précédent pour la prise en compte de nouveaux partenaires ;
* Support de scénarios avec ou SANS liaison/mappages de comptes. Beaucoup de scénarios ne justifient pas en effet la maintenance d’un compte (et ses coût afférents) au niveau du fournisseur de services pour les ressources exposées.

Il s’avère donc nécessaire d’aller au-delà pour embrasser la diversité des situations à prendre en considération.

### Fédération des identités « Back-Channel »

Afin de considérer la diversité des cas d’usage, sortons à présent du cadre de fédération frontal plus directement lié aux portails et sites Web pour aborder celui esquissé au chapitre précédent de la fédération à destination des échanges de messages/données entre entités fédérées et l’ensemble des « Back-End » impactés.

#### Prise en compte de la sécurisation des services Web de type SOAP et les besoins associés

Dans le contexte de la sécurisation des services Web de type SOAP, la nature autonome des services Web met l’accent sur la gestion explicite des cadres de confiance entre les applications et services. Ceci nécessite que des processus ou des systèmes qui étaient centralisés évoluent de facto vers un modèle fédéré.

Nous sommes intimement convaincus qu’un tel modèle fédéré implique qu’une information d’identité et/ou d’autorisation de confiance pour le service accédé soit véhiculée dans chaque message SOAP de façon sécurisée et standard. Cette information d’identité et/ou d’autorisation de confiance est véhiculée sous forme d’un ou plusieurs jetons (d’authentification et/ou d’autorisations) exprimant des revendications.

oasis.png Au-delà de la possibilité de signer/chiffrer tout ou partie d’un message SOAP, le standard OASIS Web Services Security: SOAP Message Security (WS-Security) 1.x permet de véhiculer de façon agnostique un ou plusieurs jeton(s) de sécurité (avec le cas échéant une preuve de possession associée). C’est à notre sens, cette dimension qu’il convient de privilégier pour la sécurisation des services Web de type SOAP.

Le profil [Basic Security Profile 1.1](http://www.ws-i.org/deliverables/workinggroup.aspx?wg=basicsecurity)[[14]](#footnote-14) défini par le groupe de travail éponyme au niveau de l’organisation WS-I constitue un socle de référence pour garantir l’interopérabilité entre les différentes implémentations[[15]](#footnote-15).

WS-Security fait partie du corpus des standards des services Web avancés, à savoir la pile WS-\* (STAR pour *Secured, Transacted, Asynchronous & Reliable* en anglais) constitué d’un ensemble de recommandations du W3C et de standards de l’OASIS.



Il convient de noter, au passage, que le WS-I vient d’annoncer la fin et la conclusion de ses travaux sur l’interopérabilité des services Web avancés initiés en 2002 avec la publication désormais en version finale des profils élémentaires (Basic Profile) 1.2 et 2.0 ainsi que le profil sécurisé et fiable (Reliable and Secure Profile) 1.0 :

« *WAKEFIELD, Mass., USA – November 10, 2010 – After nearly a decade of work and industry cooperation, the Web Services Interoperability Organization (WS-I;* <http://www.ws-i.org>*) has successfully concluded its charter to document best practices for Web services interoperability across multiple platforms, operating systems and programming languages.*

*The release of WS-I member approved final materials for Basic Profile (BP) 1.2 and 2.0, and Reliable Secure Profile (RSP) 1.0 fulfills WS-I’s last milestone as an organization. By publishing the final three profiles, WS-I marks the completion of its work.* »

Communiqué de presse [WS-I Completes Web Services Interoperability Standards Work](http://www.ws-i.org/docs/press/pr_101110.pdf)[[16]](#footnote-16)

Comme indiqué, ces profils seront maintenus par l’OASIS dans le cadre de la transition en cours.

Pour revenir aux éléments constituants de la pile WS-\*, le standard OASIS Web Services Trust Language (WS-Trust) issu du [comité technique OASIS Web Services Secure Exchange (WS-SX)](http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=ws-sx)[[17]](#footnote-17) définit pour cela un modèle de service de jetons de sécurité (*Security Token Service* en anglais ou STS en abrégé) auprès duquel de tels jetons (d’authentification, d’autorisations, d’attributs, de pseudonymes) peuvent être obtenus ainsi que le protocole pour converser avec ce service de jetons de sécurité.

Un tel service est à même d’émettre, de valider et d’échanger des jetons de sécurité, d’émettre dans ce dernier cas par exemple un jeton de délégation (élément *Act As*). Ainsi, par exemple, un demandeur émet une requête et, si les règles exprimées par sa politique et celles du destinataire le permettent, le demandeur reçoit en retour un jeton de sécurité.

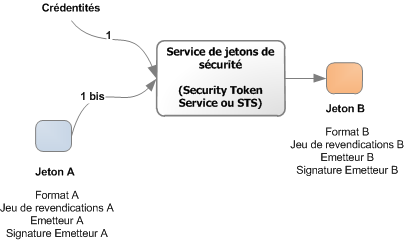
Un jeton de sécurité contient un ensemble de revendications dont le type et la sémantique sont fonction du cadre de confiance courant considéré :

* Informations d’identité résultant de l’authentification telles que le niveau et le type d’authentification ;
* Information du genre « Autorisé pour X », par exemple une liste de services cibles ;
* Toute autre information valide dans le contexte du cadre de confiance considéré.

Il est du ressort spécifique du service et/ou de l’organisation destinataire de faire confiance ou non aux revendications ainsi produites ; ces dernières étant des déclarations et/ou affirmations de fait. Autrement dit, la confiance à placer dans l’information ainsi reçue est à la discrétion du service et/ou de l’organisation destinataire.

Le STS émetteur peut signer par un procédé cryptographique (recommandation W3C [XML Signature Syntax and Processing (Second Edition)](http://www.w3.org/TR/xmldsig-core/)[[18]](#footnote-18) (XML-DSig en abrégé) par exemple) les jetons afin de garantir leur intégrité (il n'est plus possible de modifier le contenu du jeton à partir de l’instant de sa signature) et de permettre la vérification de leur origine. Lorsque l’authentification et, le cas échéant, l’autorisation effectuées par le STS sont réussies, un jeton de sécurité est envoyé au demandeur.

La Figure 3 suivante résume les différents rôles d’un STS.



*Figure 3 - Service de jetons de sécurité ou STS.*

La notion d’échange induit la capacité de transformation de jetons en termes de type de confiance, de format, de sémantique et de (valeurs des) revendications véhiculées par un jeton.

En fonction du rôle particulier du STS considéré et de son emplacement dans la topologie globale, le type et la sémantique des revendications contenues dans le jeton de sécurité varient. Il est aussi possible d’émettre plusieurs jetons pour des services cibles différents.

Un STS peut jouer plusieurs rôles distincts et participer à différents types de topologies de schémas de confiance :

* *STS fournisseur d’identités demandeur* - L’authentification effectuée par le STS vis-à-vis du référentiel d’authentification du fournisseur d’identités produit un jeton de sécurité à destination du service cible afin d’obtenir un accès autorisé.
* *STS consommateur d’identités* - Le STS vérifie les jetons de sécurité présentés par les demandeurs et génère des jetons donnant accès au service cible.
* *STS courtier en confiance entre deux ou plusieurs parties* - Dans ce cas, le cadre de confiance établie entre chaque partie et le négociant crée un cadre de confiance entre les parties elles-mêmes.

La Figure 4 montre un exemple des flux entre les parties impliquées. Voici une description des étapes numérotées dans la figure :

1. Le demandeur présente les informations de sécurité ou crédentités nécessaires au STS fournisseur d’identités demandeur A.
2. Le STS fournisseur d’identités demandeur A valide l’identité et renvoie un jeton de sécurité au demandeur.
3. Le demandeur présente ce jeton au STS consommateur d’identités cible B.
4. Le STS consommateur d’identités cible B vérifie la validité et l'origine du jeton, et renvoie au demandeur un jeton d'accès pour le service cible C. Il n’a pas besoin de reconnaître directement le demandeur ou son identité. Il fait confiance au STS fournisseur d’identités demandeur A et accepte par conséquent son jeton.
5. Le demandeur présente le jeton d’accès au service cible C (dont la sécurité est gérée par le STS consommateur d’identités B) et accède à cette ressource.

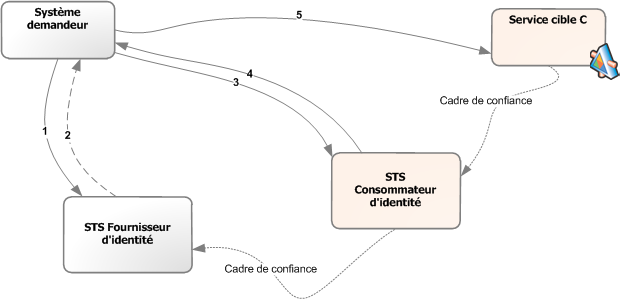


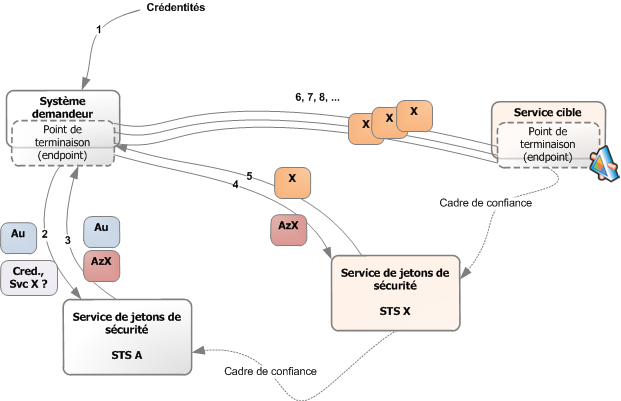
Figure 4 – Authentification fédérée.

L’interaction entre plusieurs STS et les rôles associés varient en fonction de la topologie et du modèle. La Figure 5 montre quelques variations possibles :

1. Un système demandeur s’exécute dans le contexte de sécurité d’un compte utilisateur et doit montrer ses informations de sécurité ou crédentités.
2. Le système envoie une requête au STS A. Il présente les crédentités du compte utilisateur sous lequel il s’exécute et spécifie le service demandé, X.
3. Après l’authentification réussie de l’utilisateur et l’autorisation pour le service X, le STS émet et renvoie deux jetons :

* Un jeton d’authentification (**Au**) qui confirme l’authentification réussie de l’utilisateur (et donc du système demandeur). Il pourra être utilisé pour obtenir ultérieurement des autorisations complémentaires sans nécessiter une nouvelle authentification complète de l’utilisateur auprès du STS A.
* Un jeton d’autorisation (**AzX**) pour l’utilisateur (en l’occurrence le système demandeur) du service X. Il contient les identificateurs appropriés qui définissent le contexte de la relation entre l'utilisateur (le système) et le service X.

1. Le système contacte pour la première fois le service X et présente le jeton d'autorisation **AzX** émis par le STS A.
2. Le STS X vérifie la validité du jeton AzX et émet un nouveau jeton X, spécifique au STS X, qui contient des revendications appropriées pour accéder au service X. Par exemple, le STS X peut traduire les identificateurs contenus dans le jeton **AzX** en informations plus spécifiques liées à un rôle dans le contexte du service X.
3. Les appels suivants (6, 7, 8, etc.) en provenance du système présentent le jeton X dont la validité peut être vérifiée très rapidement, bien plus rapidement que le contrôle du jeton **AzX** et la traduction des revendications. Le transfert via le jeton X des identificateurs appropriés spécifiques au service X, permet aussi de prendre des décisions d’autorisation au sein du service.



*Figure 5 – Rôles des STS et échange de jeton.*

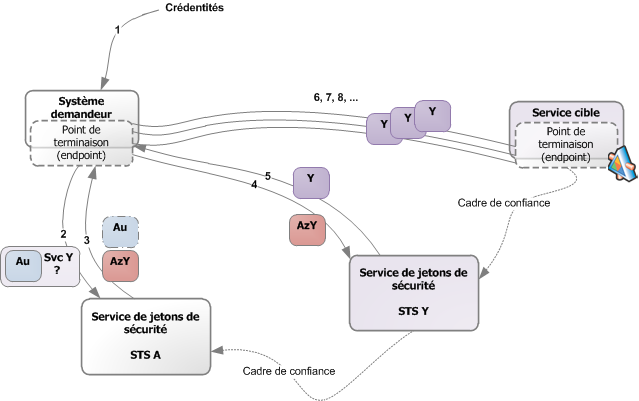
Après avoir interagi avec le service X, le système demandeur a besoin d’accéder à un autre service Y. La Figure 6 illustre cette situation où de petites différences apparaissent par rapport à l’exemple précédent.

En supposant que le jeton d’authentification (**Au**) précédemment émis par le STS A soit toujours valide et qu’il ait été stocké de façon fiable et sécurisée par un intermédiaire ou par le système demandeur lui-même, l’obtention d’un jeton pour accéder à un autre service Y peut être très simple et n’exige pas la présentation des informations de sécurité complètes de l’utilisateur. C’est le principe même d’une ouverture de session unique pour accéder à plusieurs services. Les flux échangés sont les suivants (Figure 6) :

1. Le contexte applicatif du système demande l’accès à un autre service Y.
2. Le système émet une requête à destination du STS A, présentant le jeton d’authentification **Au** précédemment émis par ce dernier, tout en précisant le service cible Y.
3. Après les vérifications réussies de la validité du jeton d’authentification **Au** et de l’autorisation de l’utilisateur (le système) pour le service X, le STS A émet et renvoie deux jetons:

* Un jeton d'authentification **Au** rafraîchi ou renouvelé (optionnel), avec une durée de validité éventuellement modifiée afin de permettre le prolongement de l'authentification d'origine. (Cela dépend de la définition des stratégies et de l’équilibre souhaité entre sécurité et aspect pratique.)
* Un jeton d’autorisation **AzY** qui contient les identificateurs appropriés, propres au service Y et définissant le contexte de la relation entre l’utilisateur et le service Y.

1. Le système demandeur contacte pour la première fois le service Y et présente le jeton d'autorisation **AzY** émis par le STS A.
2. Le STS Y vérifie la validité du jeton **AzY** et émet un nouveau jeton **Y**, propre au STS Y, contenant les revendications appropriées pour accéder au service Y.
3. Les appels suivants (6, 7, 8, etc.) en provenance du système présentent le jeton **Y** dont la validité peut être vérifiée très rapidement, bien plus rapidement que le contrôle du jeton **AzY** et la traduction des attributs. Le transfert via le jeton **Y** des identificateurs appropriés spécifiques au service Y, permet aussi de prendre des décisions d’autorisation au sein du service.



*Figure 6 – Rôles des STS et échange de jeton, nouveau service.*

**L'idée de transformation de jetons et de revendications introduite par ce standard constitue très certainement l'avancée technique la plus significative dans l'informatique distribuée depuis au moins les dix dernières années.**

L’impact et les réponses qui sont ainsi apportées n’ont d’ailleurs pas été complètement anticipés au début des travaux dans ce domaine.

Compte tenu de la diversité des scénarios (et des acteurs potentiels) à prendre en considération, il apparaît nécessaire de supporter aussi bien des schémas de confiance directe, indirecte, par courtage ainsi que la délégation. Ceci exige un modèle de fédération qui ne peut être autrement que complètement négocié dynamiquement via un pilotage par les métadonnées.

En complément du standard OASIS WS-Trust, le standard OASIS WS-Federation propose notamment une extension des métadonnées de SAML 2.0 (décrites dans la spécification [Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0](http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf)[[19]](#footnote-19)) adaptée au contexte des services Web.

La spécification WS-Federation permet, par ailleurs, le développement et le déploiement de services de fédération avancés (services d’authentification, d’autorisations, d’attributs, de pseudonymes, etc.) comme une simple variation du modèle de transformation de revendications d’un service de jetons WS-Trust.

Dès lors, pour une transaction donnée, au travers de la chorégraphie d’invocation en cours, le cadre de confiance est dynamique et fondé sur la prise en charge de politiques de confiance (métadonnées de fédération) établies et exposées par les différentes parties impliquées et sur la transmission (et l’échange) de jetons de sécurité (d’authentification, d’autorisations, d’attributs, de pseudonymes) :

* Les (intermédiaires et les) ressources fédérées comprennent des jetons (d’authentification, d’autorisations, d’attributs, de pseudonymes) spécifiques (en termes de format et de sémantique pour les revendications ainsi véhiculées),
* Les STS émettent des jetons ou bien traduisent les jetons émis par d’autres services de jetons, tiers de confiance en d’autres jetons (depuis ce que le demandeur initial possède vers ce que le service Web accédé en final exige/a besoin pour prendre (ou en déduire) ses décisions d’autorisation).

Les jetons de sécurité résultants de cette transaction sont partagés, soit directement soit indirectement, entre les parties impliquées dans le traitement du message. En conséquence, ces jetons de sécurité sont émis par un STS, racine approuvée (de confiance) ou par un STS, nœud de la chaîne de confiance et/ou de délégation.

**Les standards OASIS WS-Security, WS-Trust et WS-Federation rendent possible pour la fédération l’émergence d’un modèle complètement distribué et dynamique piloté par l'exposition, l'échange de politiques de fédération (métadonnées de fédération) avec, à la clé, une très large variété de schéma de confiance applicables.**

La gestion, la découverte et l'accès à de tels services Web sécurisés s’en trouvent notablement simplifiés lorsque ces derniers reposent tous sur un modèle de traitement commun et parlent le même protocole.

#### Considérations additionnelles vis-à-vis des standards OASIS WS-Federation 1.2 et SAML 2.0

La spécification WS-Federation doit être considérée comme une spécification évolutive des spécifications SAML, et non pas comme une alternative.

Le livre blanc [Understanding WS-Federation](http://msdn2.microsoft.com/en-us/library/bb498017.aspx)[[20]](#footnote-20), publié conjointement par IBM et Microsoft, tous deux membres du comité OASIS WSFED donne une appréciation du périmètre fonctionnel de la spécification. Cette spécification permet typiquement de constituer une identité composite sous forme de multiples jetons obtenus depuis différents fournisseurs (d’identités et/ou d’attributs) comme évoqué à la fin du premier chapitre vis-à-vis du méta-système d’identités.

Comme souligné en introduction de la section précédente, le travail de la communauté SAML a constitué une étape importante pour tous ceux impliqués dans (la « portabilité » de) l'identité numérique. Rien dans la spécification WS-Federation n’invalide ce travail.

Pour autant, une proposition technologique n’apporte pas forcément de façon immuable une réponse pertinente dans le temps. Si l’on se souvient un instant du moment où SAML a été introduit et positionné comme une alternative à l’« authentification » LDAP, aucun des contributeurs LDAP de l’époque n’a considéré la proposition faite comme la réponse ultime au domaine de l’identité et des attributs. Des personnes comme Mark Wahl, Bob Morgan ou encore Keith Hazelton, profondément impliquées dans Kerberos et LDAP, et vues par beaucoup comme des « gourous » LDAP, se sont alors au contraire montrées prêtes à embrasser de nouvelles technologies comme SAML en tant que réponse à de nouveaux cas d’usage.

Tout comme SAML a introduit une nouvelle fondation en son temps, WS-Federation est destinée à résoudre un certain nombre de points que nombreux souhaitent voir mieux définies de façon à faciliter l'interopérabilité au niveau de la fédération comme, par exemple, une séparation claire entre les mécanismes de confiance, les formats de jetons de sécurité, et les protocoles pour obtenir ces jetons.

La spécification WS-Federation vient ainsi compléter des standards OASIS comme, en particulier WS-Security et WS-Trust. WS-Security permet de véhiculer de façon agnostique un ou plusieurs jeton(s) de sécurité (avec le cas échéant une preuve de possession associée). WS-Trust définit un modèle de service de jetons de sécurité ou STS.

Ces protocoles n’avaient même pas été inventés lors des évolutions de SAML.

D’ailleurs à ce titre, comment attendre de SAML une adéquation optimale avec ces considérations qui au final émergent depuis peu ? Ceci ne déprécie en aucune façon les succès passés de SAML.

Par ailleurs, comme mentionné précédemment, une section de la spécification WS-Federation définit les règles de codage qui permettent à de nombreuses fonctionnalités du protocole WS-Trust et des extensions WS-Federation d’être utilisées par les navigateurs et les portails et sites Web via des mécanismes standard HTTP. Cette section, initialement connue sous le nom de profil passif de WS-Federation (WS-Fed Passive) duplique la fonctionnalité définie dans la spécification SAML 2.0 abordée précédemment.

Cette superposition trouve sa fondation et justification dans les objectifs même de WS-Federation afin de fournir un protocole commun pour effectuer des opérations de fédération d’identités à destination des services Web mais également des portails et sites Web.

Un même protocole commun assure des économies par rapport au développement, aux tests, au déploiement et à la maintenance des services de fédération, et ce aussi bien pour les fournisseurs de technologies que pour les clients, consommateurs de ces technologies.

L’échec dans l'intégration des scénarios à bases de clients passifs (navigateurs) et de clients actifs multiplie non seulement les coûts mais induit également pour les clients aujourd’hui ou dans un futur proche des problématiques de migration douloureuses.

Le standard WS-Federation se distingue ainsi du standard SAML en proposant à l’industrie des bénéfices qui ne sont disponibles dans aucun autre standard existant.

La fédération des identités « *Back-Channel* » est tout aussi fondamentale en termes d’interopérabilité et impacte en particulier les services Web et leur sécurité en termes d’authentification et de contrôle d’accès.

#### Prise en compte du style d’architecture REST

[Wikipedia](http://en.wikipedia.org/wiki/Representational_State_Transfer)[[21]](#footnote-21) définit REST et les services Web RESTful comme suit:

« *Representational State Transfer (REST) is a style of software architecture for distributed hypermedia systems such as the World Wide Web. The term Representational State Transfer was introduced and defined in 2000 by Roy Fielding in his doctoral dissertation. Fielding is one of the principal authors of the Hypertext Transfer Protocol (HTTP) specification versions 1.0 and 1.1.*

*Conforming to the REST constraints is referred to as being ‘RESTful’.*

…

*A RESTful web service (also called a RESTful* [*web API*](http://en.wikipedia.org/wiki/Web_API)*) is a simple web service implemented using HTTP and the principles of REST. It is a collection of resources, with three defined aspects:*

* *the base URI for the web service, such as http://example.com/resources/*
* *the MIME type of the data supported by the web service. This is often JSON, XML or YAML but can be any other valid MIME type.*
* *the set of operations supported by the web service using HTTP methods (e.g., POST, GET, PUT or DELETE).*

»



De façon à pouvoir étendre le méta-système d’identité aux consommateurs d’identités conformes au style d’architecture REST ainsi décrit, Microsoft, Google, et Yahoo ont investi conjointement sur la définition d’un profil du standard ouvert OAuth (Open Authorization) issu d’une initiative communautaire pour les autorisations démarrée en 2006.

Pour mémoire, OAuth est destiné à l’origine au partage de ressources proposées par un site depuis un autre site sans avoir à gérer des crédentités (*credentials* en anglais). OAuth permet aux utilisateurs de fournir des jetons en lieu et place de leur crédentités pour accéder aux ressources souhaitées. Chaque jeton confère ainsi un accès pour un site donné vis-à-vis de ressources spécifiques et sur une période donnée. OAuth constitue un service complémentaire mais distinct d’OpenID (Cf. section éponyme § 2.2.2). Le protocole OAuth 1.0 correspond à la [RFC 5849 The OAuth 1.0 Protocol](http://tools.ietf.org/html/rfc5849)[[22]](#footnote-22). Le guide [The Authoritative Guide to OAuth 1.0](http://hueniverse.com/oauth/guide/)[[23]](#footnote-23) présente une vue d’ensemble sur ce protocole.

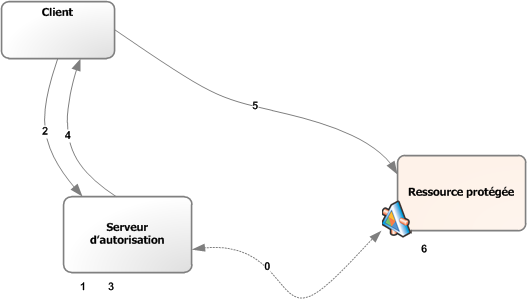
 

Le profil résultant [WRAP (Web Resource Authorization Protocol)](http://tools.ietf.org/html/draft-hardt-oauth-01)[[24]](#footnote-24), également appelé OAuth WRAP, propose, tout en offrant une similitude en termes de pattern à OAuth 1.0A, un nombre important de capacités qui n’étaient pas présentes précédemment dans OAuth. La spécification résultante est désormais en cours de standardisation au sein de l’IETF ([IETF OAuth WG](http://tools.ietf.org/wg/oauth/)[[25]](#footnote-25)) et sert de fondation à la définition d’[OAuth 2.0](http://tools.ietf.org/html/draft-ietf-oauth-v2)[[26]](#footnote-26). L’article [Introducing OAuth 2.0](http://hueniverse.com/2010/05/introducing-oauth-2-0/)[[27]](#footnote-27) propose une vue d’ensemble d’OAuth 2.0.

La définition de WRAP s’est accompagnée de celle d’un nouveau format de jeton d’accès, en l’occurrence le format SWT (Simple Web Token) qui peut être utilisé au sein de WRAP. L’obtention d’un jeton SWT peut se faire sur la base de la fourniture d’un jeton SAML préalablement obtenu dans le cadre, par exemple, d’une fédération d’identité « Front-Channel ».

La Figure 7 illustre les interactions entre les différentes parties impliquées.

1. Un secret périodiquement rafraîchi est échangé entre le serveur d’autorisation et la ressource protégée.
2. Des règles de contrôles d’accès sont définies pour le client.
3. Le client demande un jeton d’accès (revendications) pour l’accès à la ressource protégée.
4. Le serveur d’autorisation mappe les revendications reçues en entrée vers des revendications en sortie sur la base de l’exécution des règles de contrôle d’accès.
5. Le serveur d’autorisation retourne le jeton d’accès avec les revendications en sortie issues de l’étape précédente.
6. Le client envoie son message avec le jeton de contrôle d’accès.



*Figure 7 – Principes de WRAP*

Ce format est également en cours de standardisation au sein du groupe à l’IETF.

Le service ACS (Access Control Services) de la plateforme Windows Azure AppFabric supporte le protocole WRAP et peut émettre des jetons SWT (Cf. section § 3.1.3 Microsoft Windows Azure AppFabric platform Access Control Services (ACS) 2.0).

Par ailleurs, en reconnaissance d’un intérêt substantiel pour représenter un ensemble de revendications dans des jetons JSON (JavaScript Object Notation), une proposition de spécification d’un jeton [JWT (JSON Web Token)](http://self-issued.info/docs/draft-goland-json-web-token-00.html)[[28]](#footnote-28) vient d’être publiée dans la liste OAuth pour y être discutée.

### Sélection du fournisseur d’identité

Dans l’usage fait des identités et le contrôle associé, une composante essentielle du méta-système, tel qu’abordé à la section § 1 Notions de méta-système et de mash-up d’identités, est la notion de cartes d’information et sélecteur d’identités.

Wikipedia définit les cartes d’informations (*Information Card* en anglais) ou [i-cards](http://en.wikipedia.org/wiki/I-Card)[[29]](#footnote-29) comme :

« *A rectangular icon displayed in the user interface of an identity agent that represents a digital identity--a set of claims about a digital subject.* »

En d’autres termes, une carte d’informations constitue un artefact permettant d’obtenir auprès d’un fournisseur d’identités, après identification/authentification, une preuve d’identité sous forme de revendications (claims en anglais).

Le sélecteur d’identités contient les cartes d’informations relatives aux différentes identités de l’utilisateur.

Une telle approche permet non seulement aux personnes d’être en contrôle, au travers de la notion de « sélecteur d’identités », de leurs identités (manipulées sous forme de cartes d’informations) et de l’usage qui en est fait.

Le sélecteur d’identités permet, en effet, à l’utilisateur, dans le cadre d’une fédération centrée sur lui-même :

* De s’assurer de l’identité du fournisseur de services accédé,
* De sélectionner dans le contexte courant de la transaction son identité (via la sélection d’une carte d’informations), et par la même le fournisseur d’identités de son choix,
* De la communiquer, après son consentement explicite, au fournisseur de services accédé ou consommateur d’identités.

Avec la disponibilité de cartes d’information et d’un sélecteur d’identité, le méta-système d’identités :

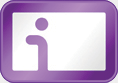
* Repositionne les identités numériques d’un sujet sous son contrôle direct et explicite,
* Offre une expérience utilisateur prévisible, cohérente et reconductible quels que soient les fournisseurs d’identités et de services impliqués dans le contexte de la transaction courante,
* Élimine les coûteuses intégrations pas toujours des plus ergonomiques ni des plus cohérentes tant au niveau fournisseur d’identités que fournisseur de services.

Le standard OASIS [Identity Metasystem Interoperability Version 1.0](http://docs.oasis-open.org/imi/identity/v1.0/identity.html)[[30]](#footnote-30) issu du [comité technique OASIS Identity Metasystem Interoperability (IMI)](http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=imi)[[31]](#footnote-31) définit les cartes d’information et leur modalité d’usage au sein du méta-système d’identité. Ce standard est issu du profil d'interopérabilité pour le sélecteur d’identités ([Identity Selector Interoperability Profile (ISIP) 1.x](http://www.microsoft.com/downloads/details.aspx?FamilyID=b94817fc-3991-4dd0-8e85-b73e626f6764&DisplayLang=en)[[32]](#footnote-32) publié à l’origine par Microsoft et couvert par l’[Open Specification Promise](http://www.microsoft.com/interop/osp)[[33]](#footnote-33) (OSP en abrégé) de Microsoft.

L’ensemble des problématiques adressées par le sélecteur d’identités (au sein d’un écosystème de confiance), en permettant aux utilisateurs de gérer leurs propres identités (quelles soient omni ou non directionnelles), et les problèmes que rencontre la fédération des identités sont dans l’ensemble orthogonaux.

Le méta-système d’identités n’est donc pas positionné contre tel ou tel protocole de fédération, mais au contraire supprime les frictions qui peuvent exister et résout des problématiques connexes et complémentaires. Il s’agit donc d’une approche orthogonale. Il convient de noter à ce titre le profil SAML 2.0 suivant en cours d’élaboration : [SAML V2.0 Information Card Token Profile](http://www.oasis-open.org/committees/download.php/29019/draft-sstc-saml2-infocard-02.pdf)[[34]](#footnote-34).

Le livre blanc [The Information Card Ecosystem: The Fundamental Leap from Cookies & Passwords to Cards & Selectors](http://wiki.informationcard.net/files/icf-information-card-ecosystem-white-paper.pdf) propose une vue d’ensemble sur les cartes d’information et les sélecteurs d’identité.



La constitution de l’[Information Card Foundation](http://informationcard.net/)[[35]](#footnote-35) (ICF en abrégé) en juin 2008 (Cf. [communiqué de presse](http://informationcard.net/files/ICFPressRelease6-24-08.pdf)[[36]](#footnote-36) associé) permet de :

* Fédérer la collaboration de l'industrie qui a émergé autour du méta-système d’identités et des cartes d'information ;
* Et promouvoir l’usage des cartes d’informations quels que soient les environnements, les socles technologiques et les langages considérés pour les sélecteurs, les fournisseurs et consommateurs d’identité.

Parmi son comité directeur, on trouve Google, Microsoft, Novell, Oracle et PayPal.

De nombreuses solutions logicielles développées par des éditeurs, des communautés et des contributions individuelles à destination de l’ensemble des principales plateformes de développement sont ainsi proposées. Le sélecteur d’identité proposé par Microsoft s’appelle Windows CardSpace.



L’interopérabilité de ces solutions a pu être testée via les divers ateliers d’interopérabilité organisés par l’[OSIS (Open-Source Identity System)](http://osis.idcommons.net/wiki/Main_Page)[[37]](#footnote-37).

## Identités numériques sociales/grand public

### Windows Live ID



Windows Live ID (initialement Microsoft Passport) est un service d’authentification Web unique (et un protocole) développé et opéré par Microsoft qui permet aux utilisateurs de se connecter à plusieurs sites Web à l'aide d'un seul identifiant Windows Live ID. Plus de 520 millions d’utilisateurs utilisent au quotidien ce service avec plus d’un milliard d’ouvertures de session/jour).

L’article [Introduction to Windows Live ID](http://msdn.microsoft.com/en-us/library/bb288408.aspx)[[38]](#footnote-38) propose une vue d’ensemble du service Windows Live ID.

La majorité des sites qui utilisent des identifiants Windows Live ID sont des services Microsoft comme Hotmail, Office Web Apps, SkyDrive, Messenger, Xbox LIVE, etc., mais plusieurs autres sociétés affiliées avec Microsoft utilisent ce service. Les services Microsoft précédents sont communément appelés MSN, dans la mesure où de nombreux services supportant les identifiants (Passport/) Windows Live ID sont ou ont été précédemment proposés sous la marque MSN.

Le service Windows Live ID permet par ailleurs l’accès aux offres et solutions Cloud de Microsoft dans le nuage comme la [plateforme Windows Azure](http://www.windowsazure.com/)[[39]](#footnote-39) (Windows Azure, SQL Azure, et Windows Azure AppFabric) ou [Microsoft Online Services](http://www.microsoft.com/online/fr-fr/default.mspx)[[40]](#footnote-40) comme l’offre de collaboration [Microsoft Office 365](http://office365.microsoft.com/)[[41]](#footnote-41) (Microsoft Office, SharePoint Online, Exchange Online et Lync Online).

Dans ce contexte, et vis-à-vis d’une organisation, le service Windows Live ID permet de mapper, au travers de la passerelle de fédération Microsoft (Microsoft Federation Gateway ou MFG en abrégé), des identités fédérées issues d’autres fournisseurs d’identités de façon à pouvoir accéder à ces offres et solutions Microsoft dans le nuage.

Comme décrit dans l’article [Microsoft Federation Gateway](http://msdn.microsoft.com/en-us/library/cc287610.aspx)[[42]](#footnote-42), cette passerelle qui constitue un service d'identité qui s'exécute dans le nuage, c'est-à-dire sur Internet, et au-delà du domaine de sécurité d’une organisation, agit, en effet, comme un hub pour l’ensemble des connexions que l'organisation souhaite établir, qu’il s’agisse de l’accès à Microsoft Online Services et/ou à une application ou un service développé au-dessus de la plateforme Windows Azure. Pour cela, un tel hub assure la connexion des utilisateurs et d'autres identités aux applications et services avec lesquels il opère ; ainsi, une organisation n’a à gérer qu’un seul cadre de confiance (avec ce hub) pour permettre à ses identités numériques d’accéder dans le nuage à l’ensemble des services Microsoft et/ou à des services fondés sur la plateforme Windows Azure.

La passerelle de fédération Microsoft supporte les standards OASIS WS-Federation, WS-Trust, WS-Security et SAML 2.0 abordé précédemment. A ce titre, il convient de noter que le support de SAML 2.0 est aujourd’hui destiné aux étudiants utilisateur du service Microsoft Live@edu au travers de l’environnement Shibboleth.

Le service Windows Live ID propose en Beta le support des cartes d’information comme abordées à la section § 2.1.3 Sélection du fournisseur d’identité.

Le service Windows Live ID s’expose désormais en Beta sous forme d’un fournisseur OpenID. Ceci permet aux utilisateurs d'utiliser leur identifiant Windows Live ID pour se signer sur tout site Web qui prend en charge l'authentification OpenID. Ceci nous amène directement à la section suivante.

### Open ID

[](http://openid.net/wp-content/uploads/2007/10/openid_big_logo_text.png)

« *OpenID is a free and easy way to use a single digital identity across the Internet* »

[OpenID Foundation (OIDF)](http://openid.net/)[[43]](#footnote-43)

OpenID est une manière facile et de plus en plus populaire de communiquer l’identité en ligne d’un utilisateur auprès d’un consommateur d’identité sur Internet sur la base d’un seul identifiant, à savoir une adresse OpenID de la forme d’une URL gérée par un fournisseur (d’identité) OpenID qui assure l’authentification ; l’idée de base d’OpenID est de prouver qu’on est capable d’écrire à telle URL, par exemple un weblog, ce qui implique que je suis l’auteur de tel weblog. La méthode d’authentification varie d’un fournisseur OpenID à un autre allant d’un simple mot de passe au support d’une authentification forte (comme pour un weblog d’ailleurs).

OpenID constitue donc un système (et protocole) d’authentification léger et décentralisé qui permet l’authentification Web unique, ainsi que le partage d’attributs (via l’extension AX[[44]](#footnote-44)) entre un fournisseur OpenID et des sites Web consommateurs d’identités (supportant la technologie et le protocole afférent) comme plaxo.com, wikispaces.com, etc.

Ceci suppose l’établissement préalable de cadres de confiance entre ledit fournisseur OpenID et les sites Web consommateurs d’identités considérés. Le site [OpenID Explained](http://openidexplained.com/)[[45]](#footnote-45) offre une vue synthétiques d’OpenID.

La Fondation OpenID est une organisation internationale à but non lucratif constituée d’entreprises et de particuliers engagée dans la mise en œuvre, la promotion et la protection des technologies OpenID.

Microsoft est membre du conseil d’administration de la fondation et fournisseur OpenID 2.0 (Cf. section précédente), au même titre que Google, Orange, PayPal, Yahoo, myopenid, etc.

Sa conception d’origine expose le protocole OpenID à des attaques de type « man-in-the-middle ». Pour tenter de lutter contre de possibles attaques par hameçonnage, certains fournisseurs OpenID imposent que l’utilisateur soit déjà authentifié auprès d’eux avant une authentification avec le consommateur d’identité. Cela repose sur la connaissance par l’utilisateur de la politique de sécurité du fournisseur OpenID.

A ce titre, la spécification [OpenID Provider Authentication Policy Extension (PAPE)](http://openid.net/specs/openid-provider-authentication-policy-extension-1_0.html)[[46]](#footnote-46), une proposition initiale de Microsoft, approuvée par la fondation en décembre 2008 permet aux consommateurs d’identité de demander que les fournisseurs OpenID reposent lors de l'authentification des utilisateurs sur des politiques d'authentification spécifiées et que ces mêmes fournisseurs OpenID informent les consommateurs d’identités des politiques effectivement utilisées.  Ainsi, un consommateur d’identité peut demander que l'utilisateur final soit authentifié au niveau du fournisseur OpenID, par exemple, en utilisant une méthode d'authentification forte (multi-facteurs) et/ou résistante à l'hameçonnage comme une authentification fondée sur l’utilisation par carte d’information (Cf. section § 2.1.3 Sélection du fournisseur d’identité). Ceci permet d’inhiber les vecteurs d’attaques de type « man-in-the-middle ». Le livre blanc [Open Trust Frameworks for Open Government: Enabling Citizen Involvement through Open Identity Technologies](http://wiki.informationcard.net/files/Open-Trust-Frameworks-for-Open-Gov-2009-08-10.pdf)[[47]](#footnote-47) illustre l’utilisation conjointe des cartes d’information et d’OpenID.

Dans cette même dynamique de durcissement du protocole OpenID, Microsoft a fait d’autres propositions comme la spécification [OAuth 2.0 bearer token](http://self-issued.info/?p=420)[[48]](#footnote-48), ou encore la spécification émergeante [JSON Web Token (JWT)](http://self-issued.info/?p=349)[[49]](#footnote-49) précédemment mentionnée (Cf. section § 2.1.2.3 Prise en compte du style d’architecture REST) et destinée à être utilisée dans la spécification de liaison [OpenID Artifact Binding 1.0](https://openid4.us/specs/ab/)[[50]](#footnote-50).

# Scénarios de mise en œuvre

**Le succès des situations précédentes et des standards et initiatives qui les sous-tendent dépend grandement de l’adhésion des utilisateurs d’un (méta-)système fédéré et par là même de la confiance que ces derniers portent dans le système pris dans son ensemble.**

Pourquoi irais-je donner mes identifiants ? Que va-t-il en être fait ? Autant de questions que l’usager est amené à se poser et ce dernier ne comprend pas pourquoi il doit faire tout cela. **La confiance ne se décrète pas, elle se mérite !**

Pour autant, le besoin de mécanismes d’authentification forte et de dispositif anti-hameçonnage/vol d’identité est croissant. Les statistiques proposées sur le site de l’[Anti-Phishing Working Group](http://www.antiphishing.org)[[51]](#footnote-51) sont, à ce titre, édifiantes. Les fournisseurs de services sont aujourd’hui beaucoup plus intéressés par la fédération d’identité qu’il y a encore 2 ou 3 ans. Pour l’entreprise désormais étendue, et reposant, le cas échéant en termes d’optimisation de ces coûts, sur des services et solutions dans le nuage, cela devient une obligation !

Encore faut-il que les technologies disponibles permettent de mettre en place facilement ce genre de scénario et de participer ainsi aisément à un tel méta-système d’identité…

## Cadre d’illustration avec les technologies Microsoft

Fondée sur les services d'annuaire Active Directory et destinée aussi bien aux développeurs qu'aux professionnels de l’information, Microsoft propose aujourd’hui un ensemble de technologies ouvertes et interopérables permettant de rendre concrète les notions d’identité fondée sur les revendications, de méta-système et mash-up d’identités introduites à la section § 1 Notions de méta-système et de mash-up d’identités.

Ces technologies pour l’identité et l’authentification unique aide à simplifier l’accès aux applications, aux services Web, et à d’autres systèmes :

* au sein de l’entreprise,
* entre organisations,
* sur le Web et dans le nuage comme avec la plateforme Windows Azure ou Microsoft Online Services.



Ces technologies sont mises en perspectives vis-à-vis de tel ou tel scénario type à mettre en œuvre dans le guide [A Guide to Claims–based Identity and Access Control](http://msdn.microsoft.com/en-us/library/ff423674.aspx)[[52]](#footnote-52).

Il s’agit pour l’essentiel, à l’exception des services dans le nuage comme Microsoft Windows Azure AppFabric platform Access Control Services (ACS) 2.0, de composants de la plateforme Windows (Server) et, à ce titre, leur droit d’utilisation est inclus dans le coût des licences associées.

Les sections suivantes présentent ces différentes technologies. Nous vous invitons à consulter à titre de complément le kit de formation [Identity Developer Training Kit](http://www.microsoft.com/downloads/en/details.aspx?displaylang=en&FamilyID=c3e315fa-94e2-4028-99cb-904369f177c0)[[53]](#footnote-53) et/ou à visionner les [différents webcasts associés](http://channel9.msdn.com/tags/WIF-Workshop/)[[54]](#footnote-54).

### Microsoft Windows Identity Foundation (WIF) 1.0

#### Vue d’ensemble



[Windows Identity Foundation (WIF en abrégé) 1.0](http://msdn.microsoft.com/en-us/security/aa570351.aspx)[[55]](#footnote-55) constitue un ensemble d'API, ou une bibliothèque d’identité, à destination des développeurs ASP.NET et Windows Communication Foundation (WCF en abrégé) pour la conception respectivement d’applications Web et de services Web à même de consommer directement des revendications et d’établir un cadre de confiance dans un contexte de fédération. WIF supporte également la notion de délégation d’identité. Les guides [AD FS 2.0 Federation with a WIF Application Step-by-Step Guide](http://go.microsoft.com/fwlink/?LinkId=179631)[[56]](#footnote-56) et [Identity Delegation with AD FS 2.0 Step-by-Step Guide](http://go.microsoft.com/fwlink/?LinkId=196715)[[57]](#footnote-57) illustrent ces fonctionnalités en relation avec AD FS 2.0 (Cf. section éponyme § 3.1.2).

A ce titre, WIF propose nativement le support des standards OASIS WS-Federation et WS-Trust. L’extension [Windows Identity Foundation Extension for OAuth CTP Version 1](https://connect.microsoft.com/site1168/Downloads/DownloadDetails.aspx?DownloadID=32719)[[58]](#footnote-58) apporte, comme son nom le suggère, le support du protocole OAuth 2.0.

WIF constitue également un socle d’accueil pour des applications existantes nécessitant un contexte de sécurité donné comme Kerberos. Pour cela, WIF permet d’utiliser les revendications obtenues afin de constituer un tel contexte et le transmettre à l’application considérée au travers du service WIF Claims to Windows Token Service (C2WTS en abrégé).

WIF propose enfin une fondation pour l’écriture de STS personnalisés.

Le livre blanc [Microsoft Windows Identity Foundation (WIF) Whitepaper for Developers](http://download.microsoft.com/download/7/D/0/7D0B5166-6A8A-418A-ADDD-95EE9B046994/WindowsIdentityFoundationWhitepaperForDevelopers-RTW.pdf)[[59]](#footnote-59) offre une première vue du Framework. Pour aller plus loin, l’ouvrage [Programming Windows Identity Foundation](http://download.microsoft.com/download/B/E/0/BE063DDD-2E1B-43F5-A7A5-290DD5F62472/9780735627185_SampleChapters.pdf)[[60]](#footnote-60) est à a conseiller vivement à tout développeur WIF.

Le [SDK (Software Development Kit) WIF](http://www.microsoft.com/downloads/en/details.aspx?FamilyID=c148b2df-c7af-46bb-9162-2c9422208504&displaylang=en)[[61]](#footnote-61) propose des modèles de projet pour développer facilement des applications Web et des services Web fondés sur les revendications ainsi que des STS personnalisés.

Le forum WIF[[62]](#footnote-62) regroupe les échanges de la communauté s’intéressant à cette technologie.

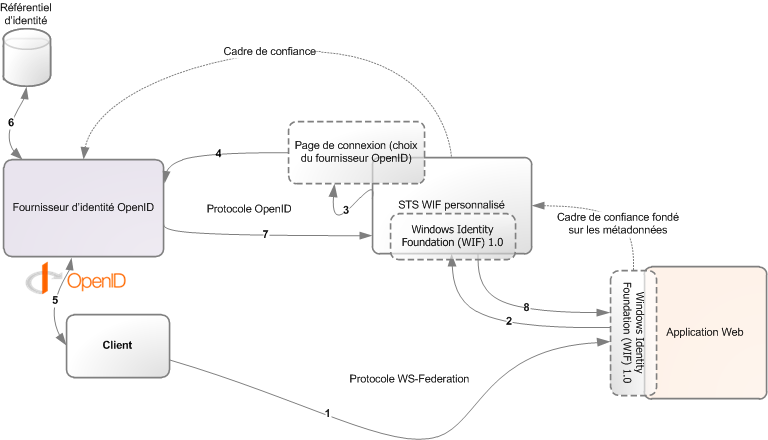
#### S’interfacer avec d’autres protocoles et standards

Au-delà des standards supportés nativement par le Framework WIF, il peut s’avérer intéressant de capitaliser sur la fondation proposée par WIF pour l’écriture de STS personnalisés et d’utiliser un tel socle pour mettre à disposition un STS passerelle protocolaire.

Ainsi, pour permettre, par exemple, une authentification OpenID (Cf. section éponyme § 2.2.2) auprès d’un fournisseur OpenID (Google, Orange, PayPal, Yahoo, myopenid, etc.) au niveau d’une application Web supportant le protocole WS-Fed Passive (via le Framework WIF par exemple), on peut envisager un STS personnalisé qui assure la transition/traduction entre le protocole OpenID et le protocole WS-Fed Passive et vice versa.

Un tel STS développé avec WIF doit fournir une page de connexion qui fera la « poignée de main » (*handshake* en anglais) avec le fournisseur OpenID. Pour cela, la bibliothèque [DotNetOpenAuth](http://www.dotnetopenauth.net/)[[63]](#footnote-63) peut être utilisée pour faire apparaitre le STS comme un consommateur d’identité OpenID. Ce STS peut ensuite être déclaré comme un STS de confiance au niveau de l’application considérée. Sur cette base, des utilisateurs authentifiés par un fournisseur OpenID reconnu par le STS personnalisé peuvent ensuite accéder aux ressources de ladite application en fonction des permissions qui leur seront conférées.

Un tel exemple de STS est proposé, avec une application exemple, dans le billet [OpenID – WS-Fed Protocol Transition STS](http://blogs.southworks.net/mwoloski/2009/07/14/openid-ws-fed-protocol-transition-sts/)[[64]](#footnote-64). Le kit [thinktecture Starter STS (Community Edition)](http://startersts.codeplex.com/)[[65]](#footnote-65) disponible sur la forge CodePlex et fondé sur le Framework WIF propose également cette capacité en s’appuyant sur la bibliothèque DotNetOpenAuth.



*Figure 8 - STS Transition de Protocole avec OpenID.*

La Figure 8 illustre les interactions entre les différentes parties impliquées lors de la première connexion. La figure montre les interactions de façon conceptuelle. En réalité, toutes ces flèches sont des requêtes, redirections et réponses HTTP qui passent par le browser client.

1. L’utilisateur navigue vers l’application considérée.
2. Le Framework WIF détecte que l'utilisateur est anonyme et tente d'accéder à une page protégée. De ce fait, il émet une requête WS-Fed SignIn à destination du STS et redirige ainsi l’utilisateur vers ce dernier.
3. Au niveau de la page de connexion du STS chargée de faire la poignée de main avec un fournisseur OpenID, l'utilisateur précise son identifiant OpenID.
4. Le STS émet une requête d'authentification à destination du fournisseur OpenID et de rediriger ainsi l’utilisateur vers ce dernier.
5. Le fournisseur OpenID demande le mot de passe correspond à l’identifiant OpenID précisé.
6. Le fournisseur OpenID valide l’identité de l’utilisateur.
7. Le fournisseur OpenID retourne une réponse d'authentification au STS, avec la redirection associée.
8. Le STS extrait les revendications émises par le fournisseur OpenID et génère un jeton SAML avec les revendications OpenID. Le STS renvoie une réponse WS-Fed SignIn avec le jeton SAML avec la redirection de l’utilisateur vers l’application accédée à l’origine.

Le Framework WIF récupère le jeton SAML, le valide et génère sur cette base un principal de sécurité. L'utilisateur peut accéder maintenant à la page protégée puisqu’il est authentifié. Des informations de profil sont également potentiellement disponibles (si l'utilisateur a rempli son profil dans le fournisseur OpenID).

Cette même approche peut également constituer une voie d’intégration pour des applications reposant sur un socle non Microsoft. Ainsi, une authentification Web unique peut être proposée au-delà des applications reposant sur le Framework WIF à des applications PHP ou Java sur Linux par exemple. Ces applications pourront utiliser pour cela la bibliothèque [simpleSAMLphp](http://simplesamlphp.org/)[[66]](#footnote-66) respectivement la bibliothèque [OpenSAML](https://spaces.internet2.edu/display/OpenSAML/Home/)[[67]](#footnote-67).

Le STS précédent peut être étendu pour augmenter les revendications d’identité venant du fournisseur OpenID avec d’autres revendications obtenues via l’interrogation d’un référentiel local ou une interaction avec un autre fournisseur de revendication via WS-Trust par exemple. Le STS construit une identité composite ou mash-up d’identité. Une telle approche est décrite dans le billet [Using Consumer Identities for Business Interactions](http://blogs.technet.com/b/privacyimperative/archive/2010/07/14/using-consumer-identities-for-business-interactions.aspx)[[68]](#footnote-68) avec une identité PayPal.

Le projet de STS multi-protocoles [Protocol Bridge Claims Provider](https://github.com/southworks/protocol-bridge-claims-provider/)[[69]](#footnote-69) utilisé dans ce contexte et disponible sous licence libre [Ms-PL](http://opensource.org/licenses/ms-pl.html)[[70]](#footnote-70) utilise différents fournisseurs de revendication. Un fournisseur de revendications est une source faisant autorité pour les revendications qui parle un protocole spécifique (OpenID avec l’extension AX ([OpenID Attribute Exchange](http://openid.net/specs/openid-attribute-exchange-1_0.html)[[71]](#footnote-71)), OpenID avec SReg ([OpenID Simple Registration Extension](http://openid.net/specs/openid-simple-registration-extension-1_0.html)[[72]](#footnote-72)), OAuth 2.0, un protocole personnalisé, etc.). Au sein du STS multi-protocoles, un fournisseur de revendications est ainsi lié à un gestionnaire de protocole, une classe qui implémente le protocole. Le STS multi-protocoles a été testé avec succès avec les fournisseurs de revendication Yahoo, Facebook et Windows Live ID.

Au-delà de la mise à disposition d’un STS personnalisé supportant d’autres protocoles, le Framework WIF peut également être étendu de façon à ce qu’une application reposant sur WIF supporte d’autres protocoles comme le standard OASIS SAML 2.0. C’est ce que propose en substance par exemple le Framework [SAML 2.0 for Windows Identity Foundation](http://safewhere.net/1124)[[73]](#footnote-73) de la société SafeWhere. Ce Framework permet à une application ASP.NET + WIF d’être vue comme un fournisseur de services SAML 2.0 conforme au mode opérationnel SP Lite. (Le [Framework OIOSAML.NET](http://saml.codeplex.com/Thread/View.aspx?ThreadId=38008) sous licence libre [MPL](http://opensource.org/licenses/mozilla1.1.php)[[74]](#footnote-74) sur la forge Codeplex propose une implémentation .NET respectant le profil danois eGovernment OIOSAML 2.0. Cette implémentation ne repose pas sur WIF.)

### Microsoft Active Directory Federation Services (AD FS) 2.0

#### Vue d’ensemble

[Microsoft Active Directory Federation Services (AD FS en abrégé) 2.0](http://www.microsoft.com/adfs2)[[75]](#footnote-75) constitue fondamentalement un STS à destination des services d’annuaires Active Directory, en l’occurrence Active Directory Domain Services (AD DS en abrégé) ou Active Directory Lightweight Directory Services (AD LDS en abrégé), et d’autres référentiels.

AD FS offre aux utilisateurs finaux une expérience d’authentification unique (Web mais pas uniquement) entre applications, plateformes et organisations.

Comme présenté précédemment, un tel service est à même d’émettre, de valider et d’échanger des jetons de sécurité, d’émettre dans ce dernier cas par exemple un jeton de délégation d’identité. La notion d’échange induit la capacité de transformation de jetons en termes de type de confiance, de format, de sémantique et de (valeurs des) revendications véhiculées par un jeton.

En fonction du rôle particulier du STS considéré et de son emplacement dans la topologie globale de confiance, le type et la sémantique des revendications contenues dans le jeton de sécurité varient. Il est aussi possible d’émettre plusieurs jetons pour des services cibles différents.

Comme tout STS, AD FS 2.0 peut jouer (simultanément) à ce titre plusieurs rôles distincts et participer à différents types de topologies de schémas de confiance :

* *STS fournisseur d’identités demandeur (IdP)* - L’authentification effectuée par le STS vis-à-vis du référentiel d’authentification du fournisseur d’identités produit un jeton de sécurité à destination du service cible afin d’obtenir un accès autorisé. AD FS 2.0 agit en tant que fournisseur de revendications (*Claims Provider* en anglais) ;
* *STS consommateur d’identités (SP)* - Le STS vérifie les jetons de sécurité présentés par les demandeurs et génère des jetons donnant accès au service cible. AD FS 20 agit en tant que consommateur d’identité (*Relying Party* en anglais) ;
* *STS courtier en confiance entre deux ou plusieurs parties* - Dans ce cas, le cadre de confiance établie entre chaque partie et le négociant établit un cadre de confiance entre les parties elles-mêmes. AD FS 20 agit dans les deux rôles précédents.

Dans ce contexte, AD FS 2.0 propose une interopérabilité native intégrée via des standards de fédération d’identités, comme OASIS WS-Trust, WS-Federation, SAML 2.0, IMI 1.0, et des revendications.

Au niveau SAML 2.0 par exemple, AD FS 2.0 supporte plus précisément, les modes opérationnels IdP Lite et SP lite (Cf. document [OASIS Conformance Requirements for the OASIS Security Assertion Markup Language (SAML) V2.0](http://docs.oasis-open.org/security/saml/v2.0/saml-conformance-2.0-os.pdf)[[76]](#footnote-76)) ainsi que le profil eGovernment harmonisé Liberty Alliance version 1.5 (Cf. [Liberty Alliance eGovernment profile for SAML 2.0](http://www.projectliberty.org/liberty/content/download/4711/32210/file/Liberty_Alliance_eGov_Profile_1.5_Final.pdf)[[77]](#footnote-77)).

AD FS 2.0 a passé avec succès les tests d’interopérabilité SAML 2.0 pour ces modes opérationnels IdP Lite, SP Lite et profil GSA 1.5comme décrit dans le document [Liberty Interoperability Testing Procedures for SAML 2.0 version 3.2.2](http://www.projectliberty.org/liberty/content/download/4709/32204/file/Liberty_Interoperability_SAML_Test_Plan_v3.2.2%20.pdf)[[78]](#footnote-78) (Cf. communiqué de presse Liberty Alliance  [Entrust, IBM, Microsoft, Novell, Ping Identity, SAP and Siemens Pass Liberty Alliance SAML 2.0 Interoperability Testing](http://www.projectliberty.org/liberty/news_events/press_releases/entrust_ibm_microsoft_novell_ping_identity_sap_and_siemens_pass_liberty_alliance_saml_2_0_interoperability_testing)[[79]](#footnote-79)).

Le livre blanc [Utiliser AD FS 2.0 pour une authentification unique Web fédérée fondée sur SAML 2.0](http://go.microsoft.com/fwlink/?LinkId=207915)[[80]](#footnote-80) décrit la configuration relative au standard SAML 2.0 d’une façon générale et une [série de livres blancs](http://technet.microsoft.com/en-us/library/dd727938(WS.10).aspx)[[81]](#footnote-81) décrit, plus particulièrement, la mise en œuvre d’AD FS 2.0 avec CA Federation Manager, Oracle Identity Manager, Ping Identity PingFederate, Shibboleth 2, etc. et ce, que ce soit en tant qu’IdP et/ou SP.

Par ailleurs, AD FS 2.0 est à même d’agir comme passerelle protocolaire entre les standards OASIS WS-Federation et SAML 2.0 ; dans le contexte d’une transaction courante, et en fonction des acteurs en présence, une partie du dialogue peut s’effectuer selon l’un de ces deux protocoles, et l’autre partie selon l’autre protocole.

Tant le support du protocole SAML 2.0 que cette capacité de passerelle protocolaire ont été accueillis des plus favorablement par Scott Cantor :

« *As a Shibboleth and OpenSAML project developer, and a deployer of the Shibboleth software at The Ohio State University, I’m excited and gratified that Microsoft is implementing the SAML 2.0 Web SSO profile in its upcoming products. Throughout the life of the Shibboleth project, and my work on the SAML 2.0 standard, our goal has been to leverage open standards to foster broad interoperability in federated identity within the higher education community and between it and its many commercial and non-commercial partners. Microsoft is clearly one of those critical partners, and as a key technology supplier, its support for the SAML standard reflects an understanding of our community’s needs and goals, and will expand the scope and impact of our efforts.*

*Our users will benefit by obtaining access to the broadest potential set of federated applications and services, and our worldwide community will benefit from the opportunity to deploy Microsoft’s identity solutions with the knowledge that they will interoperate with Shibboleth. Microsoft’s willingness to listen to our requirements and suggestions demonstrates a commitment to real-world compatibility. I look forward to continuing the dialog with Microsoft as we drive further interoperability in the use of federation metadata to scale and simplify both SAML 2.0 and WS-Federation deployments.* »

Toutes ces caractéristiques d’AD FS 2.0 s’inscrivent dans la suite logique de l’[annonce majeure](http://www.microsoft.com/presspass/press/2008/feb08/02-21ExpandInteroperabilityPR.mspx)[[82]](#footnote-82) faite par Microsoft en février 2008 dans le but d’améliorer l’ouverture de ses produits, d’offrir une meilleure interopérabilité et de créer des opportunités pour les développeurs, les partenaires, les clients et les concurrents.

L’échange d’information entre personnes et organisations, l’interopérabilité entre applications et services sont devenus en effet des besoins essentiels. Microsoft a pris depuis déjà un certain temps des engagements concernant l’interopérabilité. Nous avons échangé avec nos clients au sujet de leurs besoins d’interopérabilité et nous les avons écoutés sur la manière dont les solutions Microsoft pourraient devenir encore plus ouvertes et interopérables.

Pour répondre à ces enjeux et ces besoins, Microsoft applique quatre principes d’interopérabilité à ses produits à large diffusion comme Windows Vista (y compris le Framework .NET), Windows Server 2008, SQL Server 2008, Exchange Server 2007, Office SharePoint Server 2007 et Office 2007, ainsi que toutes les futures versions de ces produits :

* Garantir une connexion ouverte à ces produits ;
* Promouvoir la portabilité des données ;
* Améliorer le support des standards de l’industrie ;
* Favoriser l’échange et la collaboration avec l’industrie y compris les différentes communautés Open Source autour des questions d’interopérabilité et de standards.

Ces principes s’appliquent en particulier à AD FS 2.0 compte tenu de ses objectifs.

Cette plateforme ouverte offre aux utilisateurs finaux une expérience d’authentification unique (Web mais pas uniquement) entre applications, plateformes au sein de l’entreprise, entre organisations, sur le Web et dans les nuages comme avec la plateforme Windows Azure ou avec les services Microsoft Online Services via la passerelle de fédération Microsoft dans le nuage (Cf. section § 2.2.1 Windows Live ID).

Ces capacités sont reconnues par le marché. En effet, à l'occasion de la conférence EIC (European Identity Conference) 2009, le principal événement européen pour l'identité et la gestion des accès ainsi que pour la gouvernance, la gestion des risques et la conformité, l’analyste Kuppinger Cole a attribué le prix [European Identity Award 2009](http://www.id-conf.com/blog/2009/05/07/awards-for-outstanding-identity-management-projects/)[[83]](#footnote-83), dans la catégorie « Meilleure Innovation », à Microsoft pour le projet Geneva (AD FS 2.0 et WIF 1.0), dans laquelle la fédération devient partie intégrante des conteneurs utilisateur : « *one of the most significant enhancements for future use and dissemination of the Identity Federation* ».

À l'occasion de la conférence EIC 2010, le prix [European Identity Award 2010](http://www.id-conf.com/blog/2010/05/05/outstanding-projects-and-initiatives-in-im-honored/)[[84]](#footnote-84), cette fois dans la catégorie « Meilleur projet B2C », a été attribué à l'Université de Washington (UW). UW a été honoré pour sa solution de Fédération d'identité fondée sur AD FS 2.0 et WIF 1.0 dans la Recherche et l'éducation qui a été développée en partenariat avec Microsoft et qui vise à faire partie de l'initiative Microsoft Live@Edu mentionnée précédemment.

« *The University of Washington is delighted to have its work with Microsoft on federation services honored by Kuppinger Cole »*, a déclaré Bob Morgan, architecte identité pour les technologies de l’information à UW et membre de l’équipe projet Shibboleth:

« *At UW, we are committed to standards-based federation to extend the value of UW identity to the services our users need. It is great to partner with Microsoft since they too are making a commitment to federation for Windows Live and Live@edu. Live@edu's support of higher-education federations including InCommon is a key differentiator. Making it all work has many challenges, but it's essential so the higher-ed community can collaborate seamlessly and securely in cloud environments. »*

Nathan Dors, responsable de l’identité et la gestion des accès pour les technologies de l’information à UW, a ajouté :

« *We agree with Microsoft on the importance of being both standards-oriented and pragmatic. Choice of federating technology is key and we appreciate Microsoft's striving to reach parity between AD FS 2.0 and Shibboleth solutions*. *»*

Le [Centre de ressources Microsoft TechNet AD FS 2.0](http://technet.microsoft.com/en-us/library/adfs2(WS.10).aspx)[[85]](#footnote-85) et le [Weblog du groupe produit](http://blogs.msdn.com/b/card/)[[86]](#footnote-86) proposent l’ensemble des informations nécessaires à la mise en œuvre d’AD FS 2.0.



A ce propos, dans un contexte de Microsoft Online Services, l’établissement d’un cadre de confiance entre un serveur AD FS 2.0 en entreprise et Microsoft Office 365 Beta, ainsi que ses conditions de mise en œuvre, est décrit au travers d’une [série d’articles](http://g.microsoftonline.com/0BD00en-US/72)[[87]](#footnote-87). Ce contenu est destiné aux professionnels de l'informatique qui veulent tester ou implémenter une authentification unique Web de bout en bout avec des applications pour Microsoft Office 365 beta avec les applications clientes riches et Web.

#### S’interfacer avec d’autres référentiels, protocoles et standards

L’utilisation pour l’authentification, au niveau d’un serveur AD FS 20 dans le rôle d’un fournisseur de revendication d’un référentiel autre que les services d’annuaires Active Directory (AD DS ou AD LDS) peut s’appuyer sur la mise en œuvre d’un STS personnalisé développé avec le Framework WIF comme cela a été présenté précédemment (Cf. section § 3.1.1.2 S’interfacer avec d’autres protocoles et standards).

Comme également abordé dans ce cadre, un STS personnalisé permet de pouvoir s’appuyer sur des fournisseurs d’identité utilisant des protocoles autres que les standards OASIS supportés nativement, comme le protocole OpenID par exemple et vis-à-vis desquels un cadre de confiance ne peut pas être établi directement sur les bases supportées par AD FS 2.0.

Dans les deux cas de figure, le STS personnalisé doit être déclaré comme un fournisseur de revendication au niveau d’AD FS 2.0 de façon à ce que les jetons SAML émis soient reconnus comme étant dignes de confiance.

Ceci suppose par ailler de modifier la logique des pages d’authentification d’AD FS 2.0 pour collecter, le cas échéant, les crédentités nécessaires au niveau de la page et intégrer un rebond vers le STS personnalisé pour obtenir un jeton SAML contenant les revendications souhaitées. La logique d’interaction avec le référentiel ou le fournisseur est propre au STS ainsi développé.

Ces principes sont décrits dans le billet [Customizing the AD FS 2.0 Sign-in Web Pages](http://blogs.msdn.com/b/card/archive/2010/01/27/customizing-the-ad-fs-2-0-sign-in-web-pages.aspx)[[88]](#footnote-88). Ce billet précise également les pointeurs vers le contenu pertinent du [SDK AD FS 2.0](http://msdn.microsoft.com/en-us/library/ee914589.aspx)[[89]](#footnote-89).

Pour donner une autre illustration que le cas d’utilisation avec un fournisseur OpenID vu précédemment, ce type d’approche peut être également utilisé au niveau du serveur AD FS 2.0 (dans son rôle de fournisseur de revendications) pour déléguer l’authentification à réaliser à son tour en s’appuyant sur un autre protocole d’authentification Web unique, cette fois non fédéré, comme le protocole [CAS (Central Authentication Service)](http://www.yale.edu/tp/auth)[[90]](#footnote-90), comme cela est fait typiquement dans le cadre de la mise en œuvre du projet Shibboleth (en tant que système distribué sous licence de logiciel libre) pour un fournisseur d’identité. L’approche consiste à utiliser, pour cela, le [client CAS .NET](https://wiki.jasig.org/display/CASC/.Net+Cas+Client)[[91]](#footnote-91) qui s’intègre directement avec les applications ASP.NET.

Le STS personnalisé passif développé avec le modèle pour ASP.NET utilise la bibliothèque CAS.NET pour intercepter et d’authentifier l’utilisateur s’il n’est pas connecté et enrichir la session ASP.NET avec les informations résultantes. Ces informations peuvent ensuite être utilisées pour réémettre un jeton SAML grâce au Framework WIF.

### Microsoft Windows Azure AppFabric platform Access Control Services (ACS) 2.0



Le service [Access Control Services (ACS) 2.0](http://portal.appfabriclabs.com)[[92]](#footnote-92) de la plateforme Windows Azure AppFabric, annoncé lors de la [Microsoft Developer Conference 2010](http://bit.ly/8ZnXbT)[[93]](#footnote-93) constitue fondamentalement un STS d’autorisation à destination des applications Web et de services Web SOAP et RESTful en entreprise ou située dans le nuage avec la plateforme Windows Azure.

Cette version 2.0 propose nombre d’améliorations et d’évolutions significatives vis-à-vis de la version actuellement en production.

Au-delà d’une intégration poussée avec le Framework WIF et son outillage, d’un support natif d’AD FS 2.0 à la fois comme fournisseur de revendications ou consommateur d’identité, ACS 2.0 supporte nativement les fournisseurs d’identité sociale populaires : Windows Live ID, Google, Yahoo, et Facebook. ACS 2.0 permet de réaliser une transition de protocole entre ces principaux fournisseurs (et le protocole sous-jacent utilisé) et le protocole WS-Federation par exemple.

Les fonctions que pourraient réaliser un STS personnalisé pour interagir avec un fournisseur OpenID (Cf. section § 3.1.1.2 S’interfacer avec d’autres protocoles et standards) constituent une fonction native du service, ce qui comprend également :

* La notion de découverte de domaine de sécurité (*Home Realm Discovery* en anglais ou HRD en abrégé) ou *Where Are You From?* (WAYF en abrégé) qui permet à un utilisateur de choisir son fournisseur d’identité est intégré et personnalisable,
* Un portail Web qui permet un accès administratif à la configuration ACS,
* Un service de gestion fondé sur le protocole [OData[[94]](#footnote-94)](http://www.odata.org/) qui fournit un accès programmatique à la configuration ACS.

En termes de protocoles, le STS ACS 2.0 supporte WS-Trust, WS-Federation, OpenID et OAuth 2.0 (draft 10). Pour ce qui est des formats de jetons, il s’agit de SAML 1.1, SAML 2.0, et SWT.

Dans ces conditions, ACS 2.0 peut être utilisé dans de très nombreux contextes et situations qu’il serait difficile de résumer ici compte tenu de la souplesse apportée.

Au moment de la rédaction de ce livre-blanc, la documentation de ce service est en cours de mise à disposition sur la forge [Codeplex](http://acs.codeplex.com/)[[95]](#footnote-95). Le billet [Shaping Windows Azure AppFabric Access Control Service 2.0 Documentation on Codeplex](http://blogs.msdn.com/b/alikl/archive/2010/12/14/shaping-windows-azure-appfabric-access-control-service-2-0-documentation-on-codeplex.aspx)[[96]](#footnote-96) précise où trouver toutes les informations, guides étapes-par-étapes et exemples.

## Scénarios B2B de collaboration fédérée entre organisations

Cette section illustre quelques-uns des scénarios de collaboration fédérée rendus aisément possibles avec les produits et technologies précédentes. Bien d’autres combinaisons peuvent être construites…

Avec des entreprises désormais étendues, ces scénarios illustrent comment les collaborateurs d’une organisation peuvent concrètement accéder à des ressources proposées par une autre organisation. Ces scénarios sont envisagés sous l’angle de produits et technologies Microsoft et non Microsoft. C’est le cas notamment pour la technologie utilisée pour les fournisseurs d’identités.

### Accès à un site de collaboration SharePoint 2010

Le support par AD FS 2.0 du protocole SAML 2.0 et sa capacité d’agir comme passerelle protocolaire entre les standards OASIS WS-Federation et SAML 2.0 (Cf. section § 3.1.2.1 Vue d’ensemble) permet d’exposer très simplement un portail SharePoint 2010, qui utilise WS-Federation, à des fournisseurs d’identité s’appuyant sur SAML 2.0 pour la fédération des identités.

En effet, la plateforme SharePoint 2010 tire bénéfice du Framework WIF et externalise l’authentification en reposant sur la mise en œuvre d’un STS interne prenant en charge :

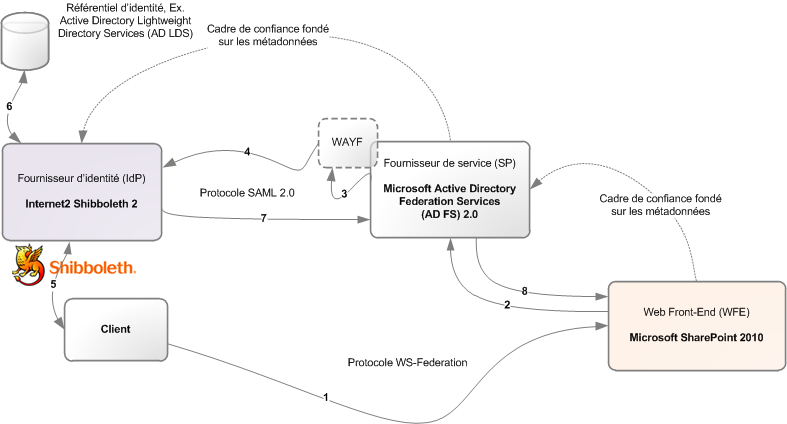
* L’authentification Windows intégrée (NTLM ou Kerberos),
* L’authentification par formulaire (Form Based Authentication en anglais ou FBA en abrégé),
* L’authentification déléguée à un STS (de jeton d’identité) de confiance (Trusted Identity Token Provider dans la terminologie SharePoint 2010) sur la base du protocole WS-Fed Passive.

Quel que soit le mécanisme utilisé pour l’authentification, l’identité numérique résultante est ensuite représentée comme un ensemble de revendications.

Il suffit de déclarer le serveur AD FS 2.0 comme un STS de confiance vis-à-vis du STS interne de SharePoint. AD FS 2.0 agit comme un fournisseur de revendication vis-à-vis de SharePoint 2010 qui est un consommateur d’identité. La communication entre AD FS 2.0 et SharePoint 2010 et vice versa utilise le standard WS-Federation.

Dans le même temps, ce même serveur AD FS 2.0 agit comme un consommateur d’identité/fournisseur de service du fournisseur d’identité SAML 2.0. La communication entre AD FS 2.0 et le fournisseur SAML 2.0 et vice versa utilise le standard SAML 2.0.

Le livre blanc [Guide étape-par-étape Collaboration fédérée avec Shibboleth 2.0 et SharePoint 2010](http://go.microsoft.com/fwlink/?LinkId=207916)[[97]](#footnote-97). Propose une description complète de la mise en œuvre d’une telle configuration avec le projet Shibboleth 2 (en tant que système distribué sous licence de logiciel libre) dans le rôle de fournisseur d’identité. Cette version de Shibboleth propose une implémentation du standard SAML 2.0.



*Figure 9* *- Accès à un site SharePoint 2010.*

La Figure 9 résume les interactions. La figure montre les interactions de façon conceptuelle. En réalité, toutes ces flèches sont des requêtes, redirections et réponses HTTP qui passent par le browser client.

1. L’utilisateur navigue vers le site SharePoint 2010.
2. Le site SharePoint 2010 détecte que l'utilisateur est anonyme et tente d'accéder à une page protégée. De ce fait et compte tenu de sa configuration, il émet une requête WS-Fed SignIn à destination du serveur de fédération AD FS 2.0 et redirige ainsi l’utilisateur vers ce dernier.
3. L'utilisateur précise son domaine de sécurité.
4. Le serveur de fédération AD FS 2.0 émet une requête d'authentification SAML 2.0 à destination du fournisseur d’identité Shibboleth 2 et redirige ainsi l’utilisateur vers ce dernier.
5. Le fournisseur d’identité Shibboleth 2 demande à l’utilisateur ses crédentités.
6. Le fournisseur d’identité Shibboleth 2 valide l’identité de l’utilisateur.
7. Le fournisseur d’identité Shibboleth 2 retourne une réponse SAML 2.0 au serveur de fédération AD FS 2.0, avec la redirection associée.
8. Le serveur de fédération AD FS 2.0 extrait les revendications émises par le fournisseur d’identité Shibboleth 2 et génère un jeton SAML à destination de la partie SharePoint 2010. Le STS renvoie une réponse WS-Fed SignIn avec le jeton SAML avec la redirection de l’utilisateur vers le site SharePoint 2010 accédée à l’origine.

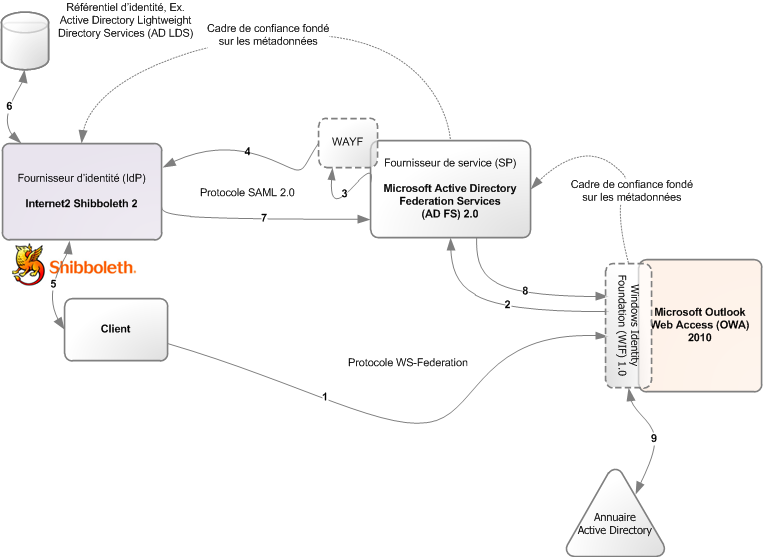
Le STS interne de SharePoint récupère le jeton SAML, le valide et génère sur cette base un principal de sécurité. L'utilisateur peut maintenant accéder au site en fonction de ses permissions.

### Accès à sa boîte aux lettres Outlook Web Access 2010

Outlook Web Access (OWA) 2010 (avec Exchange 2010) peut également être configuré de façon à reposer sur WIF pour obtenir un contexte de sécurité via le service C2WTS sur la base des revendications reçus (Cf. section § 3.1.1.1 Vue d’ensemble).

Un cadre de confiance peut être établi entre WIF et un serveur de fédération AD FS 2.0 pour l’organisation considérée ; ce dernier vise à contrôler les ressources exposées par cette organisation vis-à-vis d’autre organisation partenaires. La communication entre le serveur AD FS 2.0 et la ressource OWA 2010/WIF et vice versa utilise le standard WS-Federation. Le livre blanc [Exposing OWA 2010 with AD FS 2.0 to other organizations](http://download.microsoft.com/documents/France/Interop/2011/Exposing_OWA2010_ADFS20_Other_Organizations.docx)[[98]](#footnote-98) propose une vue d’ensemble de la configuration associée.

Le serveur AD FS 2.0 peut ensuite établir des cadres de confiance avec d’autres organisations utilisant les standards OASIS SAML 2.0 et/ou WS-Federation ou d’autres protocoles comme abordés précédemment.

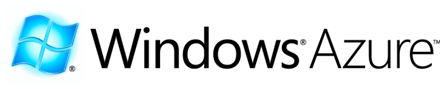


*Figure 10 - Accès à sa boîte aux lettres OWA 2010.*

La Figure 10 résume les interactions. La figure montre les interactions de façon conceptuelle. En réalité, toutes ces flèches sont des requêtes, redirections et réponses HTTP qui passent par le browser client.

1. L’utilisateur navigue vers l’application OWA 2010 pour accéder à sa boîte aux lettres.
2. L’application OWA 2010 configurée pour fonctionner avec les revendications via le Framework WIF détecte que l'utilisateur est anonyme. De ce fait et compte tenu de sa configuration, elle émet une requête WS-Fed SignIn à destination du serveur de fédération AD FS 2.0 et redirige ainsi l’utilisateur vers ce dernier.
3. L'utilisateur précise son domaine de sécurité.
4. Le serveur de fédération AD FS 2.0 émet une requête d'authentification SAML 2.0 à destination du fournisseur d’identité Shibboleth 2 et redirige ainsi l’utilisateur vers ce dernier.
5. Le fournisseur d’identité Shibboleth 2 demande à l’utilisateur ses crédentités.
6. Le fournisseur d’identité Shibboleth 2 valide l’identité de l’utilisateur.
7. Le fournisseur d’identité Shibboleth 2 retourne une réponse SAML 2.0 au serveur de fédération AD FS 2.0, avec la redirection associée.
8. Le serveur de fédération AD FS 2.0 extrait les revendications émises par le fournisseur d’identité Shibboleth 2 et génère un jeton SAML à destination de la partie OWA 2010. Le serveur de fédération AD FS 2.0 renvoie une réponse WS-Fed SignIn avec le jeton SAML avec la redirection de l’utilisateur vers l’application OWA 2010 accédée à l’origine.
9. Le Framework WIF récupère le jeton SAML, le valide et génère sur cette base un principal de sécurité. Il s’appuie pour cela sur le service WIF Claims to Windows Token Service (C2WTS en abrégé) pour constituer une identité Windows correspondant à sa boîte aux lettres. L'utilisateur peut accéder maintenant à l’application OWA 2010 et à sa boîte aux lettres.

### Accès à une application Web

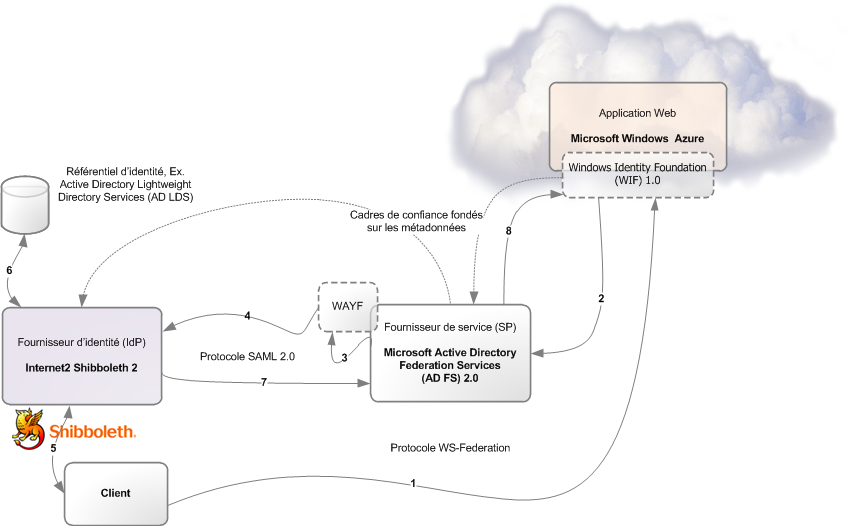


Au-delà de ce qui a été mentionné précédemment à la section § 3.1 Cadre d’illustration avec les technologies Microsoft, le livre blanc [Single Sign-On from Active Directory to a Windows Azure Application Whitepaper](http://www.microsoft.com/downloads/en/details.aspx?FamilyID=1296e52c-d869-4f73-a112-8a37314a1632)[[99]](#footnote-99) illustre comment utiliser AD FS 2.0, avec le Framework WIF, et la plateforme Windows Azure pour atteindre une authentification unique entre des applications Web déployées à la fois en en entreprise et dans le nuage.

La Figure 11 résume les interactions. La figure montre les interactions de façon conceptuelle. En réalité, toutes ces flèches sont des requêtes, redirections et réponses HTTP qui passent par le browser client.

1. L’utilisateur navigue vers l’application Web de l’organisation située dans Windows Azure.
2. L’application considérée détecte que l'utilisateur est anonyme. De ce fait et compte tenu de sa configuration, elle émet une requête WS-Fed SignIn à destination du serveur de fédération AD FS 2.0 de l’organisation et redirige ainsi l’utilisateur vers ce dernier.
3. L'utilisateur précise son domaine de sécurité.
4. Le serveur de fédération AD FS 2.0 émet une requête d'authentification SAML 2.0 à destination du fournisseur d’identité Shibboleth 2 et redirige ainsi l’utilisateur vers ce dernier.
5. Le fournisseur d’identité Shibboleth 2 demande à l’utilisateur ses crédentités.
6. Le fournisseur d’identité Shibboleth 2 valide l’identité de l’utilisateur.
7. Le fournisseur d’identité Shibboleth 2 retourne une réponse SAML 2.0 au serveur de fédération AD FS 2.0, avec la redirection associée.
8. Le serveur de fédération AD FS 2.0 extrait les revendications émises par le fournisseur d’identité Shibboleth 2 et génère un jeton SAML à destination de l’application Web. Le serveur de fédération AD FS 2.0 renvoie une réponse WS-Fed SignIn avec le jeton SAML avec la redirection de l’utilisateur vers l’application Web dans Windows Azure accédée à l’origine.

Le Framework WIF récupère le jeton SAML, le valide et génère sur cette base un principal de sécurité. L'utilisateur peut accéder maintenant au site en fonction de ses permissions fondées sur les revendications reçues.



*Figure 11 - Accès à une application Web dans Windows Azure.*

### Accès à un service Web RESTful

Le billet [Protecting and consuming REST based resources with ACS, WIF, and the OAuth 2.0 protocol](http://blogs.msdn.com/b/card/archive/2010/11/29/protecting-and-consuming-rest-based-resources-with-acs-wif-and-the-oauth-2-0-protocol.aspx)[[100]](#footnote-100) propose un exemple de bout en bout qui montre comment utiliser OAuth avec ACS 2.0 et la nouvelle extension WIF OAuth mentionnée précédemment (cf. section § 3.1.1.1 Vue d’ensemble).

La même approche de configuration s’applique pour un service Web RESTful non WCF à la condition que le socle technique propose un support du protocole OAuth comme en Java avec la bibliothèque [OAuth for Java](http://code.google.com/intl/fr-FR/appengine/docs/java/oauth/)[[101]](#footnote-101).

## Scénarios B2C/G2C pour le grand public

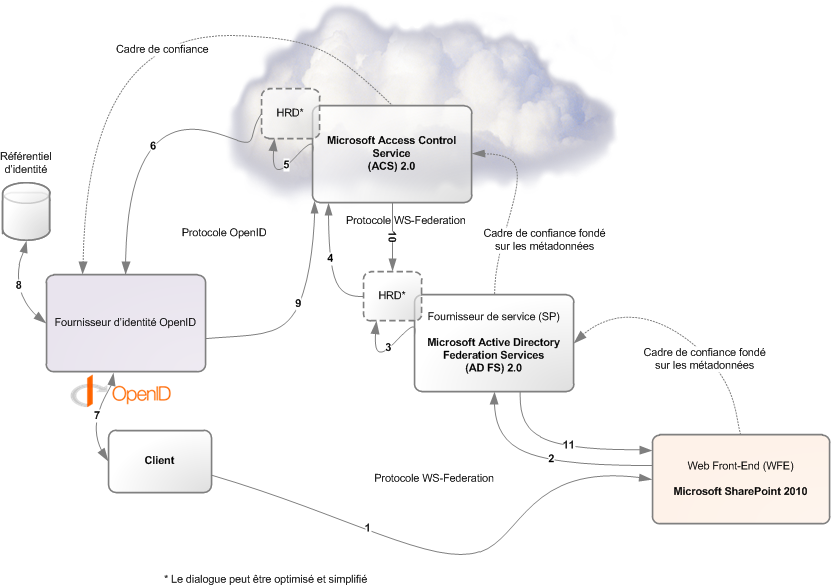
Cette section reprend à titre d’illustration le premier scénario de collaboration fédérée envisagé entre organisations, à savoir l’accès à un site de collaboration grand public, et illustre comment une identité sociale peut facilement être utilisée dans ce contexte avec les mêmes fondations architecturales et techniques. Le propos est identique pour les autres types de ressources.

A titre d’illustration, l’utilisation d’un fournisseur OpenID pour l’authentification au niveau de SharePoint 2010 peut s’appuyer sur :

* Un STS WIF personnalisé comme décrit dans la section § 3.1.1.2 S’interfacer avec d’autres protocoles et standards). Le billet [How to make use of a custom IP-STS with SharePoint 2010? (Part 1)](http://blogs.msdn.com/b/chunliu/archive/2010/04/02/how-to-make-use-of-a-custom-ip-sts-with-sharepoint-2010-part-1.aspx)[[102]](#footnote-102) décrit comment déclarer un tel STS avec SharePoint 2010 ;
* Une personnalisation d’AD FS 2.0 comme décrit dans la section § 3.1.2.2 S’interfacer avec d’autres référentiels, protocoles et standards.

Au-delà de ces approches qui demandent personnalisation et développement, le service ACS 2.0 peut directement être utilisé en lieu et place. Il ne s’agit alors que de simples configurations.

Il est supposé implicitement dans la configuration précédente qu’un serveur de fédération AD FS 2.0 contrôle l’accès à l’ensemble des ressources exposées par l’organisation. D’un point de vue technique, rien n’empêche d’établir un cadre de confiance directement entre le frontal SharePoint 2010 et le service ACS 2.0 dans le nuage. L’objectif ici consiste à montrer comment une configuration initialement mise en œuvre pour une collaboration entre organisations peut être facilement étendue par simple configuration pour offrir des accès à des identités sociales avec des permissions potentiellement différentes sur la base des revendications reçues.



*Figure 12 - Accès à SharePoint 2010 via ACS 2.0.*

La Figure 12 résume les interactions. La figure montre les interactions de façon conceptuelle. En réalité, toutes ces flèches sont des requêtes, redirections et réponses HTTP qui passent par le browser client.

1. L’utilisateur navigue vers le site SharePoint 2010.
2. Le site SharePoint 2010 détecte que l'utilisateur est anonyme et tente d'accéder à une page protégée. De ce fait et compte tenu de sa configuration, il émet une requête WS-Fed SignIn à destination du serveur de fédération AD FS 2.0 et redirige ainsi l’utilisateur vers ce dernier.
3. L'utilisateur précise qu’il souhaite s’identifier avec un fournisseur OpenID.
4. Le serveur de fédération AD FS 2.0 rediriger l’utilisateur vers l’instance configurée pour l’organisation du service ACS 2.0 dans le nuage.
5. Au niveau de la page de découverte de domaine de sécurité d’ACS, l'utilisateur précise son fournisseur OpenID comme Yahoo! par exemple.
6. L’instance d’ACS 2.0 émet une requête d'authentification à destination du fournisseur OpenID et rediriger ainsi l’utilisateur vers ce dernier.
7. Le fournisseur OpenID sélectionné demande l’identifiant OpenID de l’utilisateur et le mot de passe associé.
8. Le fournisseur OpenID valide l’identité de l’utilisateur.
9. Le fournisseur OpenID retourne une réponse d'authentification à l’instance d’ACS 2.0, avec la redirection associée.
10. L’instance d’ACS 2.0 extrait les revendications émises par le fournisseur OpenID et génère un jeton SAML avec les revendications OpenID. Elle renvoie une réponse WS-Fed SignIn avec le jeton SAML avec la redirection de l’utilisateur vers le serveur de fédération AD FS 2.0.
11. Le serveur de fédération AD FS 2.0 extrait les revendications émises par l’instance d’ACS 2.0 pour l’organisation et génère un jeton SAML à destination de la partie SharePoint 2010. Le serveur de fédération AD FS 2.0 renvoie une réponse WS-Fed SignIn avec le jeton SAML avec la redirection de l’utilisateur vers le site SharePoint 2010 accédée à l’origine.

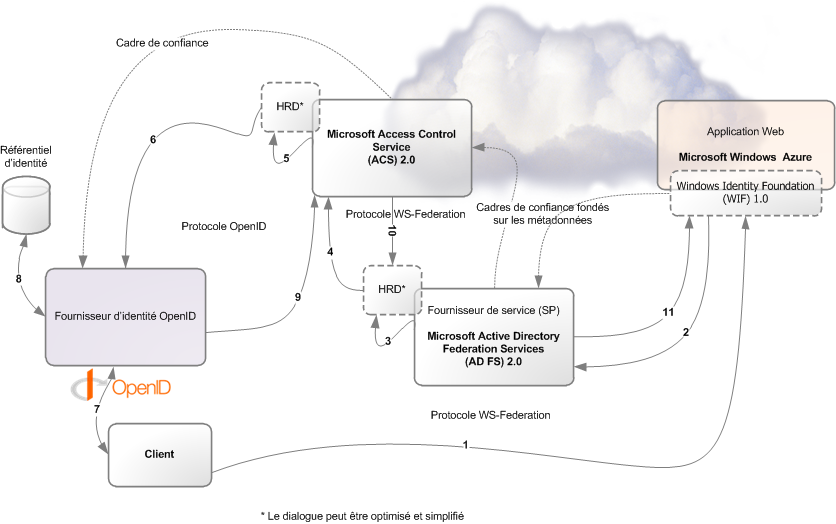
Le STS interne de SharePoint récupère le jeton SAML, le valide et génère sur cette base un principal de sécurité. L'utilisateur peut accéder maintenant au site en fonction de ses permissions.

La même approche vaut également à l’identique pour une application Web de l’organisation située dans le nuage au sein de la plateforme Windows Azure.

La Figure 13 résume les interactions. La figure montre les interactions de façon conceptuelle. En réalité, toutes ces flèches sont des requêtes, redirections et réponses HTTP qui passent par le browser client.

1. L’utilisateur navigue vers l’application Web de l’organisation située dans Windows Azure.
2. L’application considérée détecte que l'utilisateur est anonyme. De ce fait et compte tenu de sa configuration, elle émet une requête WS-Fed SignIn à destination du serveur de fédération AD FS 2.0 de l’organisation et redirige ainsi l’utilisateur vers ce dernier.
3. L'utilisateur précise qu’il souhaite s’identifier avec un fournisseur OpenID.
4. Le serveur de fédération AD FS 2.0 rediriger l’utilisateur vers l’instance configurée pour l’organisation du service ACS 2.0 dans le nuage.
5. Au niveau de la page de découverte de domaine de sécurité d’ACS, l'utilisateur précise son fournisseur OpenID comme Yahoo! par exemple.
6. L’instance d’ACS 2.0 émet une requête d'authentification à destination du fournisseur OpenID et rediriger ainsi l’utilisateur vers ce dernier.
7. Le fournisseur OpenID sélectionné demande l’identifiant OpenID de l’utilisateur et le mot de passe associé.
8. Le fournisseur OpenID valide l’identité de l’utilisateur.
9. Le fournisseur OpenID retourne une réponse d'authentification à l’instance d’ACS 2.0, avec la redirection associée.
10. L’instance d’ACS 2.0 extrait les revendications émises par le fournisseur OpenID et génère un jeton SAML avec les revendications OpenID. Elle renvoie une réponse WS-Fed SignIn avec le jeton SAML avec la redirection de l’utilisateur vers le serveur de fédération AD FS 2.0.
11. Le serveur de fédération AD FS 2.0 extrait les revendications émises par l’instance d’ACS 2.0 pour l’organisation et génère un jeton SAML à destination de l’application Web. Le serveur de fédération AD FS 2.0 renvoie une réponse WS-Fed SignIn avec le jeton SAML avec la redirection de l’utilisateur vers l’application Web dans Windows Azure accédée à l’origine.

Le Framework WIF récupère le jeton SAML, le valide et génère sur cette base un principal de sécurité. L'utilisateur peut accéder maintenant au site en fonction de ses permissions fondées sur les revendications reçues.



*Figure 13 - Accès à une application Web dans Windows Azure.*

Comme cela a déjà été souligné, bien d’autres configurations sont aujourd’hui réalisables de façon à répondre à tel ou tel scénario.

## Expérimentation de ces scénarios au MTC Paris

L’ensemble des scénarios que nous venons de décrire correspondent à ceux que nous avons implémentés sur la plateforme du [Microsoft Technology Center (MTC) Paris](http://www.microsoft.com/mtc/locations/Paris.mspx)[[103]](#footnote-103).

Cet environnement démontrant les mécanismes de la fédération d’identité est une des composantes de l’ « Interop Lab ». Dans ce laboratoire, clients, partenaires et compétiteurs testent des configurations techniques hétérogènes afin d’élaborer les solutions répondant à leurs besoins en termes d’interopérabilité opérationnelle, y compris en termes de gestion d’identité.

# Et le respect de la vie privée ?

Les organisations cherchent de plus en plus à identifier et authentifier avec une force accrue les personnes qui accèdent à leurs services à la fois sur Internet et en mode hors connexion. Ces dernières visent également à apprendre d’autres informations d’identité à l’égard de ces personnes, informations détenues par d'autres organisations. Ces impératifs en termes de d'authentification et de partage de données sont conditionnées non seulement par des considérations de coût et d'efficacité, des nouveaux modèles métier qui s’appuient des données (potentiellement personnelles) mais également par la montée explosive de l’hameçonnage (phishing en anglais), l'usurpation d'identité et autres menaces à la sécurité. Comme cela a déjà été souligné, les statistiques proposées sur le site de l’[Anti-Phishing Working Group](http://www.antiphishing.org)[[104]](#footnote-104) sont, à ce titre, édifiantes.

Les mécanismes conventionnels pour l'authentification des utilisateurs et le partage de données, tels que des « cartes plastiques » et les « certificats papier », sont onéreux, vulnérables à la contrefaçon et problématique quant à une utilisation en ligne. En conséquence, il y a un intérêt croissant rapidement dans les mécanismes qui peuvent être implémentées dans du logiciel ou du matériel, qui peuvent s'exécuter sur des réseaux et sur lesquels de multiples organisations peuvent s’appuyer. Les standards et protocoles abordés précédemment pour l’authentification unique et l’identité fédérée comme les standards SAML 2.0 et WS-Federation (Cf. section § 2 Protocoles et formats de jetons de sécurité), les infrastructures de gestion des clés (Public Key Infrastructure en anglais ou PKI en abrégé), les cartes d'identité électronique (eID cards en anglais), etc. constituent des exemples de mécanismes de plus en plus populaires pour atteindre ces objectifs. La demande pour de tels mécanismes se fait particulièrement urgente dans la gestion des identités et des accès à l’entreprise désormais étendue, la protection des infrastructures essentielles de l'information, les télé-services en ligne de l’administration électronique, la gestion des dossiers patients électroniques de santé, le commerce électronique et les réseaux sociaux.

Si la transition vers des mécanismes numériques pour une authentification sécurisée et le partage de données vérifiables s’avère potentiellement très bénéfique pour les personnes, celle-ci n’est cependant pas sans danger pour la sécurité personnelle, le respect de la vie privée, l’autonomie et la liberté des personnes. Comme une information de plus en plus liés à l'identité est partagée avec et entre les organisations, les personnes perdent tout contrôle sur l'étendue avec laquelle les organisations peuvent surveiller et analyser leurs actions, et les empêcher d'exercer de manière autonome une transaction. Les menaces proviennent non seulement de personnel malveillant et autres initiés, mais aussi de pirates et de logiciels malveillants qui parviennent à obtenir le statut d'initié. Le problème est aggravé par l'incroyable facilité avec laquelle l’information numérique peut être aujourd’hui compilée, partagée et divulguée.

De même, des consommateurs d’identité en s'appuyant sur une authentification déléguée et des revendications liées à l'identité peuvent avoir des préoccupations pour des raisons qui leur sont propres (d’ordre compétitifs, liées à la sécurité ou autres). Faire confiance à une organisation pour être une source faisant autorité pour certaines informations liées à l'identité ne signifie pas pour autant que l’on accepte d’avoir confiance dans cette même organisation pour être hautement disponible, pour ne pas emprunter l'identité des personnes cliente dudit consommateur d’identité ou encore pour ne pas espionner ces mêmes personnes (c'est-à-dire qui accède à quel service de quel consommateur d’identité à quel moment précis).

Les consommateurs d’identités peuvent également être concernés par la capacité des organisations émettrices (et des pirates informatiques et des logiciels malveillants) pour refuser l'accès des personnes à leurs services. Ces risques deviennent plus graves lorsque les personnes sont attachées aux organisations émettrices en ce sens qu'elles doivent récupérer auprès de celles-ci un nouveau jeton à chaque fois qu'elles visitent un consommateur d’identité.

Contrairement à la croyance populaire, les intérêts de la vie privée et l'autonomie dans l'authentification des utilisateurs et les systèmes de partage de données ne sont pas diamétralement opposées aux intérêts de la sécurité.

C'est là que la technologie [U-Prove](http://www.microsoft.com/mscorp/twc/endtoendtrust/vision/uprove.aspx)[[105]](#footnote-105) intervient. U-Prove est une technologie de chiffrement innovante reposant sur des algorithmes cryptographiques sophistiqués (notion de signature aveugle/semi-aveugle) qui permet la délivrance et la présentation de déclarations cryptographiquement protégées d'une manière qui fournit ce qui est connu sous le nom « sécurité multipartite » : organisations émettrices, utilisateurs et les consommateurs d’identité peuvent se protéger non seulement contre les attaques de l'extérieur, mais aussi contre les attaques provenant de l'autre. Dans le même temps, la technologie U-Prove permet tout degré souhaité du respect de la vie privée (y compris l'anonymat authentifié et le « pseudonymat ») sans contrevenir pour autant à la sécurité multipartite. Ces aspects centrés sur l’utilisateur et sur le respect de sa vie privée rendent la technologie U-Prove idéale pour créer l’équivalent numérique des crédentités sur papier et des diverses cartes plastiques présente dans le portefeuille de tout un chacun.

Dans le cadre de la gestion des identités et des accès, la technologie U-Prove permet aux organisations d'échanger des informations liées à l'identité sous une forme cryptographiquement protégée via les personnes auxquelles elles se rapportent ou autres parties d’intermédiation (telles que les courtiers). Ces dernières peuvent voir les informations protégées qui sont partagées, les stocker en vue d’une délivrance (que ce soit pour une utilisation hors connexion ou une réutilisation) et divulguer de manière sélective seulement les aspects strictement nécessaires à une transaction. Cette technologie assure que la véritable identité de la personne, y compris les attributs personnels et des profils de comportement, ne soient jamais exposés à un consommateur d’identité sans le consentement explicite de ladite personne. Une personne peut ainsi par exemple prouver qu’elle répond à une certaine politique sans divulguer les attributs spécifiés dans cette politique. Les organisations ne peuvent apprendre quoi que ce soit au-delà des aspects divulgués, même s'elles agissent de concert dans le cadre d’une collusion et disposent de ressources illimitées pour analyser les données divulguées du protocole.

Plus généralement, cette technologie de divulgation minimale peut servir à concilier des exigences multipartites apparemment contradictoires vis-à-vis de la sécurité et du respect de la vie privée pour toutes sortes de systèmes électroniques de communication et de transaction.

Des exemples comprennent la gestion des droits numériques, les services liés à l'administration électronique, les dossiers de santé patients électroniques, le vote électronique, les instruments de paiement électronique, les banques en ligne, les ventes aux enchères en ligne, les paris et jeux en ligne, etc. La technologie U-Prove peut également être appliquée pour protéger les informations relatives à l'identité se rapportant à des entités non humaines, tels que des processus, des logiciels, des périphériques matériels et ainsi de suite.

En outre, étant donné que les entités peuvent échanger en toute sécurité les informations via toute partie non fiable tout en déléguant le contrôle partiel au travers de leurs communications à cette partie, la technologie U-Prove permet la conception de nouvelles applications avec aucune analogie du monde physique ; un exemple de domaine d'intérêt concerne des services en nuage qui peuvent exécuter des opérations limitées sur des données d'entrée à l’intégrité protégée provenant de différentes sources.

Au-delà de ces éléments, le livre blanc [U-Prove Technology Overview](https://connect.microsoft.com/site642/Downloads/DownloadDetails.aspx?DownloadID=26953)[[106]](#footnote-106) offre une vue d’ensemble de cette technologie. La spécification [U-Prove Cryptographic Specification V1.0](https://connect.microsoft.com/site642/Downloads/DownloadDetails.aspx?DownloadID=26953)[[107]](#footnote-107) décrit les protocoles cryptographiques relatifs pour la technologie U-Prove. Cette spécification a été publiée sous l’[Open Specification Promise (OSP en abrégé)](http://www.microsoft.com/interop/osp/default.mspx)[[108]](#footnote-108) permettant à chacun d’utiliser ou d’implémenter cette technologie.

Afin de permettre tout type d’expérimentation, Microsoft a développé un [SDK C#](http://code.msdn.microsoft.com/uprovesdkcsharp)[[109]](#footnote-109) et [SDK Java](http://code.msdn.microsoft.com/uprovesdkjava)[[110]](#footnote-110) de référence implémentant la spécification cryptographique précédente. Ces deux kits de développement sont mis à disposition sous la licence libre [BSD](http://www.opensource.org/licenses/bsd-license.php)[[111]](#footnote-111).

La spécification [U-Prove Technology Integration into the Identity Metasystem V1.0](https://connect.microsoft.com/site642/Downloads/DownloadDetails.aspx?DownloadID=26953) également publiée sous l’OSP, définit comment les jetons U-Prove peuvent être obtenus et présentés à l'aide du standard OASIS WS-Trust, et comment la technologie s’intègre dans le méta-système d'identité tel qu’abordé à la section § 1 Notions de méta-système et de mash-up d’identités. En particulier, ce document spécifie comment un fournisseur d'identité peut fournir des présentations à partir d'une carte d'information qui prend en charge la technologie U-Prove, comment un sélecteur d'identité peut être utilisé dans ce contexte et comment un consommateur d’identité peut vérifier ces présentations.

Les composants logiciels suivants sont disponibles dans le cadre de la [CTP U-Prove](https://connect.microsoft.com/site642/Downloads/DownloadDetails.aspx?DownloadID=26931)[[112]](#footnote-112) :

* Windows Identity Foundation Extension (U-Prove CTP)[[113]](#footnote-113) – Une extension du Framework WIF (Cf. section § 3.1.1 Microsoft Windows Identity Foundation (WIF) 1.0) qui offre la possibilité de construire un STS personnalisé pour la délivrance de jetons U-Prove (pour les fournisseurs d'identité) et la capacité de vérifier les présentations de jeton U-Prove (pour les consommateurs d’identité) ;
* Active Directory Federation Services 2.0 (U-Prove CTP) – Une version d’AD FS 2.0 (Cf. section § 3.1.2 Microsoft Active Directory Federation Services (AD FS) 2.0) supportant la technologie U-Prove, qui a la capacité de délivrer une carte d'information qui prend en charge U-Prove, et qui peut agir à la fois en tant qu'un fournisseur d'identité U-Prove et un consommateur d’identité ;
* Windows CardSpace 2.0 (U-Prove CTP) – Une version du sélecteur d’identité Windows CardSpace 2.0 (Cf. section § 2.1.3 Sélection du fournisseur d’identité) qui présente la possibilité d'obtenir, de stocker et de présenter des jetons U-Prove associés à une carte d'information.

L’objectif de la CTP est de recueillir des commentaires de la communauté technique sur la technologie.

Cette technologie de divulgation minimale et ses inventeurs ont reçu plusieurs prix. A l’occasion de la conférence EIC 2010, la technologie U-Prove s’est vue attribué le prix [European Identity Award 2010](http://blogs.technet.com/b/forefront/archive/2010/05/11/microsoft-wins-awards-at-the-european-identity-conference-2010.aspx)[[114]](#footnote-114) dans la catégorie « Meilleure Innovation ».

Elle a également reçu le prix dans la catégorie de l'innovation technologique de l'[International Association of Privacy Professionals](https://www.privacyassociation.org/about_iapp/2010_09_30_iapp_honors_top_privacy_innovators/)[[115]](#footnote-115), la plus importante association du monde des professionnels du respect de la vie privée.



Enfin, cette technologie est l’une des composantes du projet de recherche européen [ABC4Trust (Attribute-Based Credentials for Trust)](http://www.ABC4Trust.eu/)[[116]](#footnote-116) dans le cadre du programme FP7 (Seventh Framework Program) de la Commission Européenne. Ce projet peut être perçu, à bien des égards, comme la suite du projet européen [STORK (Secure Identity Across Borders Linked)](https://www.eid-stork.eu/)[[117]](#footnote-117) sur l’interopérabilité des cartes d’identité électroniques. Microsoft Research & Development France est un des acteurs du projet ABC4Trust.

# En guise de synthèse

Les sections précédentes montrent que, vis-à-vis des protocoles et standards qui jouent un rôle prépondérant aujourd’hui, les produits et technologies sont désormais présentes pour en permettre une mise en œuvre facilitée au sein d’un vaste méta-système d’identités. C’est en particulier le cas des produits et technologies Microsoft illustrées dans ce contexte au même titre que d’autres technologies qui ont pu être mentionnée de manière non exhaustive.

Une identité fédérée, composite (mash-up) et portable est utilisable pour le monde en ligne dans le respect à la fois de la (politique de) sécurité des parties de la transaction et du respect de la vie privée pour les personnes à l’origine ou qui prennent part à ces transactions.

**Microsoft France est convaincue que nombre des dangers, des complications, des pertes de temps, des incertitudes liées aux expériences en ligne d'aujourd'hui peuvent s’estomper rapidement. Une adoption et un déploiement étendu du méta-système possède intrinsèquement le potentiel de résoudre la plupart de ces problèmes, bénéficiant ainsi à tout le monde et accélérant la croissance à long terme de la connectivité en rendant le monde en ligne plus sûr, plus digne de confiance et plus facile à utiliser.**

**Le « big-bang » de l’identité fédérée est en marche.**

# Pour en savoir plus…

Pour de plus amples information sur les solutions d’identités proposées par Microsoft, nous vous invitons à consulter le [site portail Web Microsoft IDA](http://www.microsoft.com/identity)[[118]](#footnote-118)(*Identity and Access Solutions* en anglais).

Pour de plus amples informations sur l'interopérabilité technique des produits et technologies Microsoft avec des logiciels et matériels d'autres fournisseurs, nous vous invitons à consulter le [site Microsoft Interopérabilité](http://www.microsoft.com/france/interop)[[119]](#footnote-119). Vous retrouverez notamment l’[annonce majeure](http://www.microsoft.com/presspass/press/2008/feb08/02-21ExpandInteroperabilityPR.mspx)[[120]](#footnote-120) que Microsoft a faite au mois de février 2008 dans le but d’améliorer l’ouverture de ses produits, d’offrir une meilleure interopérabilité et de créer des opportunités pour les développeurs, les partenaires, les clients et les concurrents.

Pour de plus amples informations sur les standards d'interopérabilité que Microsoft soutient ou auxquels Microsoft apporte sa collaboration, nous vous invitons à consulter le [site Microsoft Standards](http://www.microsoft.com/france/standards)[[121]](#footnote-121).

# Restons en contact

 Le groupe LinkedIn [Forum des Architectures Applicatives Microsoft](http://linkd.in/archiappms)[[122]](#footnote-122) regroupe des architectes en informatique qui ont des choix de technologies à faire dans les projets pour lesquels ils travaillent.

L’architecte applicatif, en situation de projet, travaille typiquement aux côtés de la direction de projet pour choisir et assumer des choix techniques en fonction des contraintes du projet (fonctionnalités, délais, ressources). Pour effectuer ces choix à bon escient, il doit connaître ce que le marché offre en termes de technologies. Cela peut prend typiquement deux formes : veille technologique continue, recherches dans le cadre du projet.

L’architecte applicatif a aussi pour rôle de faire le lien entre les équipes de développement et les équipes d’infrastructure et d’exploitation de la future application. Il doit également veiller à ce que ses choix soient bien mis en œuvre pendant le développement.

Ce forum, à l’initiative de Microsoft France, a pour but d’aider les architectes applicatifs dans la dynamique de ce livre blanc, à :

* Faciliter la connaissance de l’offre de Microsoft pour les projets en entreprise (envoi de liens vers des présentations, documents ou livre blanc comme celui-ci, webcasts, conférences, etc.) ;
* Echanger sur des problématique d’architecture ayant un rapport, même partiel, avec la plateforme Microsoft comme :
* *Est-ce que AD FS 2.0 fonctionne dans un environnement SAML 2.0 ?*
* *Comment se passe la réversibilité d’une application développée pour l’informatique en nuage ?*
* *Quelles sont les implications d’un déploiement sur une ferme Web ?*
* Etc.

Cet espace est le vôtre, faites le vivre, nous sommes aussi et surtout là pour vous lire.

1. Livre blanc The Laws of Identity : http://www.identityblog.com/?p=354 [↑](#footnote-ref-1)
2. Livre blanc The Identity Metasystem : http://www.identityblog.com/?p=355 [↑](#footnote-ref-2)
3. Définition Wikipédia de la fédération : http://en.wikipedia.org/wiki/Federated\_identity [↑](#footnote-ref-3)
4. Projet Liberty Alliance : http://www.projectliberty.org [↑](#footnote-ref-4)
5. Initiative Kantara ((kan-TAR-a): Swahili for bridge; Arabic roots in "harmony") : http://www.kantarainitiative.org/ [↑](#footnote-ref-5)
6. Projet Shibboleth : http://shibboleth.internet2.edu [↑](#footnote-ref-6)
7. Middleware Architecture Committee for Education : http://middleware.internet2.edu/MACE [↑](#footnote-ref-7)
8. Comité OASIS Security Services (SAML) TC : http://www.oasis-open.org/committees/tc\_home.php?wg\_abbrev=security [↑](#footnote-ref-8)
9. Fédération Education-Recherche du GIP Renater : https://federation.renater.fr/ [↑](#footnote-ref-9)
10. Spécification Web Services Federation Language (WS-Federation) Version 1.2 : http://docs.oasis-open.org/wsfed/federation/v1.2/ws-federation.pdf [↑](#footnote-ref-10)
11. Comité technique OASIS Web Services Federation (WSFED) : http://www.oasis-open.org/committees/tc\_home.php?wg\_abbrev=wsfed [↑](#footnote-ref-11)
12. Service CAS (Client Authentication Service): http://www.yale.edu/tp/auth [↑](#footnote-ref-12)
13. Projet Jasig : http://www.jasig.org/cas [↑](#footnote-ref-13)
14. WS-I Basic Security Profile : http://www.ws-i.org/deliverables/workinggroup.aspx?wg=basicsecurity [↑](#footnote-ref-14)
15. En raison de la multiplicité des plates-formes et de technologies susceptibles de disposer d’implémentation des standards des services Web (avancés), il est essentiel que les services Web soient capables de fonctionner dans un environnement hétérogène. WS-I peut simplifier cette tâche en définissant des profils qui correspondent un groupe de spécifications compatibles à un certain niveau de version adressant un ensemble cohérent de fonctionnalités et de recommandations d’utilisation à observer. Un profil est un ensemble de spécifications, accompagné de clarifications, interprétations et restrictions de celles-ci de façon à promouvoir l’interopérabilité. Dans le même temps, WS-I crée des protocoles et outils de test (http://www.ws-i.org/deliverables/workinggroup.aspx?wg=testingtools) afin de vérifier le respect effectif de ces profils par les différents produits et solutions du marché. Les éditeurs proposent conjointement des modèles de mise en œuvre qui se conforment aux recommandations précédentes (http://www.ws-i.org/deliverables/workinggroup.aspx?wg=sampleapps). En ce sens, WS-I représente une sorte d’intégrateur de standards qui s’appuie et qui utilise les spécifications de différentes structures de standardisation comme W3C, OASIS ou IETF. [↑](#footnote-ref-15)
16. Communiqué de presse WS-I Completes Web Services Interoperability Standards Work : http://www.ws-i.org/docs/press/pr\_101110.pdf [↑](#footnote-ref-16)
17. Comité technique OASIS Web Services Secure Exchange (WS-SX) : http://www.oasis-open.org/committees/tc\_home.php?wg\_abbrev=ws-sx [↑](#footnote-ref-17)
18. Recommandation W3C XML-DSig : http://www.w3.org/TR/xmldsig-core/ [↑](#footnote-ref-18)
19. Spécification Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0 : <http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf> [↑](#footnote-ref-19)
20. Livre blanc Understanding WS-Federation : http://msdn2.microsoft.com/en-us/library/bb498017.aspx [↑](#footnote-ref-20)
21. Définition Wikipedia du style d’architecture REST : http://en.wikipedia.org/wiki/Representational\_State\_Transfer [↑](#footnote-ref-21)
22. RFC 5849 The OAuth 1.0 Protocol : http://tools.ietf.org/html/rfc5849 [↑](#footnote-ref-22)
23. The Authoritative Guide to OAuth 1.0 : http://hueniverse.com/oauth/guide/ [↑](#footnote-ref-23)
24. Spécification WRAP : http://tools.ietf.org/html/draft-hardt-oauth-01 [↑](#footnote-ref-24)
25. Groupe de travail IETF OAuth WG : http://tools.ietf.org/wg/oauth/ [↑](#footnote-ref-25)
26. Spécification OAuth 2.0 : http://tools.ietf.org/html/draft-ietf-oauth-v2 [↑](#footnote-ref-26)
27. Introducing OAuth 2.0 : http://hueniverse.com/2010/05/introducing-oauth-2-0/ [↑](#footnote-ref-27)
28. Spécification JWT : http://self-issued.info/docs/draft-goland-json-web-token-00.html [↑](#footnote-ref-28)
29. Définition Wikipedia de l’i-card : http://en.wikipedia.org/wiki/I-Card [↑](#footnote-ref-29)
30. Spécification  Identity Metasystem Interoperability Version 1.0 : http://docs.oasis-open.org/imi/identity/v1.0/identity.html [↑](#footnote-ref-30)
31. Comité technique OASIS Identity Metasystem Interoperability (IMI) : http://www.oasis-open.org/committees/tc\_home.php?wg\_abbrev=imi [↑](#footnote-ref-31)
32. Identity Selector Interoperability Profile (ISIP) 1.x : http://www.microsoft.com/downloads/details.aspx?FamilyID=b94817fc-3991-4dd0-8e85-b73e626f6764&DisplayLang=en [↑](#footnote-ref-32)
33. Microsoft Open Specification Promise : http://www.microsoft.com/interop/osp [↑](#footnote-ref-33)
34. SAML V2.0 Information Card Token Profile : http://www.oasis-open.org/committees/download.php/29019/draft-sstc-saml2-infocard-02.pdf [↑](#footnote-ref-34)
35. Information Card Foundation : http://informationcard.net/ [↑](#footnote-ref-35)
36. Communiqué de presse de l’ICF : http://informationcard.net/files/ICFPressRelease6-24-08.pdf [↑](#footnote-ref-36)
37. Open-Source Identity System : http://osis.idcommons.net/wiki/Main\_Page [↑](#footnote-ref-37)
38. Article Introduction to Windows Live ID : http://msdn.microsoft.com/en-us/library/bb288408.aspx [↑](#footnote-ref-38)
39. Plateforme Windows Azure : http://www.windowsazure.com/ [↑](#footnote-ref-39)
40. Microsoft Online Services : http://www.microsoft.com/online/fr-fr/default.mspx [↑](#footnote-ref-40)
41. Microsoft Office 365 : http://office365.microsoft.com/ [↑](#footnote-ref-41)
42. Article Microsoft Federation Gateway: http://msdn.microsoft.com/en-us/library/cc287610.aspx [↑](#footnote-ref-42)
43. Fondation OpenID : http://openid.net/ [↑](#footnote-ref-43)
44. Spécification OpenID Attribute Exchange 1.0 : http://openid.net/specs/openid-attribute-exchange-1\_0.html [↑](#footnote-ref-44)
45. Site OpenID Explained : http://openidexplained.com/ [↑](#footnote-ref-45)
46. OpenID Provider Authentication Policy Extension (PAPE) : http://openid.net/specs/openid-provider-authentication-policy-extension-1\_0.html [↑](#footnote-ref-46)
47. Livre blanc Open Trust Frameworks for Open Government: Enabling Citizen Involvement through Open Identity Technologies : http://wiki.informationcard.net/files/Open-Trust-Frameworks-for-Open-Gov-2009-08-10.pdf [↑](#footnote-ref-47)
48. Spécification OAuth 2.0 bearer token : http://self-issued.info/?p=420 [↑](#footnote-ref-48)
49. Spécification émergeante JSON Web Token (JWT) : http://self-issued.info/?p=349 [↑](#footnote-ref-49)
50. OpenID Artifact Binding 1.0 : https://openid4.us/specs/ab/ [↑](#footnote-ref-50)
51. Anti-Phishing Working Group : http://www.antiphishing.org [↑](#footnote-ref-51)
52. Guide A Guide to Claims–based Identity and Access Control : http://msdn.microsoft.com/en-us/library/ff423674.aspx [↑](#footnote-ref-52)
53. Kit de formation Identity Developer Training Kit : http://www.microsoft.com/downloads/en/details.aspx?displaylang=en&FamilyID=c3e315fa-94e2-4028-99cb-904369f177c0 [↑](#footnote-ref-53)
54. Ateliers WIF : http://channel9.msdn.com/tags/WIF-Workshop/ [↑](#footnote-ref-54)
55. Windows Identity Foundation 1.0 : http://msdn.microsoft.com/en-us/security/aa570351.aspx [↑](#footnote-ref-55)
56. Guide AD FS 2.0 Federation with a WIF Application Step-by-Step Guide : http://go.microsoft.com/fwlink/?LinkId=179631 [↑](#footnote-ref-56)
57. Guide Identity Delegation with AD FS 2.0 Step-by-Step Guide : http://go.microsoft.com/fwlink/?LinkId=196715 [↑](#footnote-ref-57)
58. Windows Identity Foundation Extension for OAuth CTP Version 1 : https://connect.microsoft.com/site1168/Downloads/DownloadDetails.aspx?DownloadID=32719 [↑](#footnote-ref-58)
59. Livre blanc Microsoft Windows Identity Foundation (WIF) Whitepaper for Developers : http://download.microsoft.com/download/7/D/0/7D0B5166-6A8A-418A-ADDD-95EE9B046994/WindowsIdentityFoundationWhitepaperForDevelopers-RTW.pdf [↑](#footnote-ref-59)
60. Chapitres exemples de l’ouvrage Programming Windows Identity Foundation : http://download.microsoft.com/download/B/E/0/BE063DDD-2E1B-43F5-A7A5-290DD5F62472/9780735627185\_SampleChapters.pdf [↑](#footnote-ref-60)
61. Windows Identity Foundation SDK : http://www.microsoft.com/downloads/en/details.aspx?FamilyID=c148b2df-c7af-46bb-9162-2c9422208504&displaylang=en [↑](#footnote-ref-61)
62. Forum WIF : http://social.msdn.microsoft.com/Forums/en-US/Geneva/threads [↑](#footnote-ref-62)
63. Bibliothèque DotNetOpenAuth : http://www.dotnetopenauth.net/ [↑](#footnote-ref-63)
64. Billet OpenID – WS-Fed Protocol Transition STS : http://blogs.southworks.net/mwoloski/2009/07/14/openid-ws-fed-protocol-transition-sts/ [↑](#footnote-ref-64)
65. Kit thinktecture Starter STS (Community Edition) : http://startersts.codeplex.com/ [↑](#footnote-ref-65)
66. Bibliothèque simpleSAMLphp : http://simplesamlphp.org/ [↑](#footnote-ref-66)
67. Bibliothèque OpenSAML : https://spaces.internet2.edu/display/OpenSAML/Home/ [↑](#footnote-ref-67)
68. Billet Using Consumer Identities for Business Interactions : http://blogs.technet.com/b/privacyimperative/archive/2010/07/14/using-consumer-identities-for-business-interactions.aspx [↑](#footnote-ref-68)
69. STS multi-protocolaires Protocol Bridge Claims Provider : https://github.com/southworks/protocol-bridge-claims-provider/ [↑](#footnote-ref-69)
70. Licence libre Microsoft Public License : http://opensource.org/licenses/ms-pl.html [↑](#footnote-ref-70)
71. Spécification OpenID Attribute Exchange 1.0 : http://openid.net/specs/openid-attribute-exchange-1\_0.html [↑](#footnote-ref-71)
72. Spécification OpenID Simple Registration Extension 1.0 :http://openid.net/specs/openid-simple-registration-extension-1\_0.html [↑](#footnote-ref-72)
73. Framework SAML 2.0 for Windows Identity Foundation : http://safewhere.net/1124 [↑](#footnote-ref-73)
74. Licence libre Mozilla Public License : http://opensource.org/licenses/mozilla1.1.php [↑](#footnote-ref-74)
75. Active Directory Federation Services 2.0 : http://www.microsoft.com/adfs2 [↑](#footnote-ref-75)
76. Conformance Requirements for the OASIS Security Assertion Markup Language (SAML) V2.0: http://docs.oasis-open.org/security/saml/v2.0/saml-conformance-2.0-os.pdf [↑](#footnote-ref-76)
77. Liberty Alliance eGovernment profile for SAML 2.0: http://www.projectliberty.org/liberty/content/download/4711/32210/file/Liberty\_Alliance\_eGov\_Profile\_1.5\_Final.pdf [↑](#footnote-ref-77)
78. Liberty Interoperability Testing Procedures for SAML 2.0 version 3.2.2 : http://www.projectliberty.org/liberty/content/download/4709/32204/file/Liberty\_Interoperability\_SAML\_Test\_Plan\_v3.2.2%20.pdf [↑](#footnote-ref-78)
79. Communiqué de presse Liberty Alliance ENTRUST, IBM, MICROSOFT, NOVELL, PING IDENTITY, SAP AND SIEMENS PASS LIBERTY ALLIANCE SAML 2.0 INTEROPERABILITY TESTING : http://www.projectliberty.org/liberty/news\_events/press\_releases/entrust\_ibm\_microsoft\_novell\_ping\_identity\_sap\_and\_siemens\_pass\_liberty\_alliance\_saml\_2\_0\_interoperability\_testing [↑](#footnote-ref-79)
80. Livre blanc Utiliser AD FS 2.0 pour une authentification unique Web fédérée fondée sur SAML 2.0 : http://go.microsoft.com/fwlink/?LinkId=207915 [↑](#footnote-ref-80)
81. Guides Etape-par-Etape AD FS 2.0 : http://technet.microsoft.com/en-us/library/dd727938(WS.10).aspx [↑](#footnote-ref-81)
82. Cf. *Microsoft Makes Strategic Changes in Technology and Business Practices to Expand Interoperability - New interoperability principles and actions will increase openness of key products* : http://www.microsoft.com/presspass/press/2008/feb08/02-21ExpandInteroperabilityPR.mspx [↑](#footnote-ref-82)
83. European Identity Award 2009: http://www.id-conf.com/blog/2009/05/07/awards-for-outstanding-identity-management-projects/ [↑](#footnote-ref-83)
84. European Identity Award 2010: http://www.id-conf.com/blog/2010/05/05/outstanding-projects-and-initiatives-in-im-honored/ [↑](#footnote-ref-84)
85. Centre de ressources Microsoft TechNet AD FS 2.0 : http://technet.microsoft.com/en-us/library/adfs2(WS.10).aspx [↑](#footnote-ref-85)
86. Weblog Groupe produit AD FS 2.0 : http://blogs.msdn.com/b/card/ [↑](#footnote-ref-86)
87. Préparation à la fédération d’identité pour Microsoft Office 365 : http://g.microsoftonline.com/0BD00en-US/72 [↑](#footnote-ref-87)
88. Billet Customizing the AD FS 2.0 Sign-in Web Pages : http://blogs.msdn.com/b/card/archive/2010/01/27/customizing-the-ad-fs-2-0-sign-in-web-pages.aspx [↑](#footnote-ref-88)
89. SDK AD FS 2.0 : http://msdn.microsoft.com/en-us/library/ee914589.aspx [↑](#footnote-ref-89)
90. Service CAS (Client Authentication Service): http://www.yale.edu/tp/auth [↑](#footnote-ref-90)
91. client CAS .NET: https://wiki.jasig.org/display/CASC/.Net+Cas+Client [↑](#footnote-ref-91)
92. ACS 2.0 : http://portal.appfabriclabs.com [↑](#footnote-ref-92)
93. Session PDC 2010 Identity & Access Control in the Cloud : http://bit.ly/8ZnXbT [↑](#footnote-ref-93)
94. Protocole OData : http://www.odata.org/ [↑](#footnote-ref-94)
95. Documentation ACS 2.0 sur CodePlex : http://acs.codeplex.com [↑](#footnote-ref-95)
96. Billet Shaping Windows Azure AppFabric Access Control Service 2.0 Documentation on Codeplex : http://blogs.msdn.com/b/alikl/archive/2010/12/14/shaping-windows-azure-appfabric-access-control-service-2-0-documentation-on-codeplex.aspx [↑](#footnote-ref-96)
97. Livre blanc Guide étape-par-étape Collaboration fédérée avec Shibboleth 2.0 et SharePoint 2010 : http://go.microsoft.com/fwlink/?LinkId=207916 [↑](#footnote-ref-97)
98. Exposing OWA 2010 with AD FS 2.0 to other organizations : http://download.microsoft.com/documents/France/Interop/2011/Exposing\_OWA2010\_ADFS20\_Other\_Organizations.docx [↑](#footnote-ref-98)
99. Livre blanc Single Sign-On from Active Directory to a Windows Azure Application Whitepaper : http://www.microsoft.com/downloads/en/details.aspx?FamilyID=1296e52c-d869-4f73-a112-8a37314a1632 [↑](#footnote-ref-99)
100. Billet Protecting and consuming REST based resources with ACS, WIF, and the OAuth 2.0 protocol : http://blogs.msdn.com/b/card/archive/2010/11/29/protecting-and-consuming-rest-based-resources-with-acs-wif-and-the-oauth-2-0-protocol.aspx [↑](#footnote-ref-100)
101. Bibliothèque OAuth for Java : http://code.google.com/intl/fr-FR/appengine/docs/java/oauth/ [↑](#footnote-ref-101)
102. Billet How to make use of a custom IP-STS with SharePoint 2010? (Part 1) : http://blogs.msdn.com/b/chunliu/archive/2010/04/02/how-to-make-use-of-a-custom-ip-sts-with-sharepoint-2010-part-1.aspx [↑](#footnote-ref-102)
103. Microsoft Technology Center Paris: http://www.microsoft.com/mtc/locations/Paris.mspx [↑](#footnote-ref-103)
104. Anti-Phishing Working Group : http://www.antiphishing.org [↑](#footnote-ref-104)
105. Technologie U-Prove : http://www.microsoft.com/mscorp/twc/endtoendtrust/vision/uprove.aspx [↑](#footnote-ref-105)
106. Livre blanc U-Prove Technology Overview : https://connect.microsoft.com/site642/Downloads/DownloadDetails.aspx?DownloadID=26953 [↑](#footnote-ref-106)
107. Specification U-Prove Cryptographic Specification V1.0 : https://connect.microsoft.com/site642/Downloads/DownloadDetails.aspx?DownloadID=26953 [↑](#footnote-ref-107)
108. Open Specification Promise: http://www.microsoft.com/interop/osp/default.mspx [↑](#footnote-ref-108)
109. SDK U-Prove C# : http://code.msdn.microsoft.com/uprovesdkcsharp [↑](#footnote-ref-109)
110. SDK U-Prove Java : http://code.msdn.microsoft.com/uprovesdkjava [↑](#footnote-ref-110)
111. License libre BSD : http://www.opensource.org/licenses/bsd-license.php [↑](#footnote-ref-111)
112. CTP U-Prove: https://connect.microsoft.com/site642/Downloads/DownloadDetails.aspx?DownloadID=26931 [↑](#footnote-ref-112)
113. Windows Identity Foundation Extension (U-Prove CTP) : https://connect.microsoft.com/Content/#WIFEx [↑](#footnote-ref-113)
114. Microsoft wins awards at the European Identity Conference 2010: http://blogs.technet.com/b/forefront/archive/2010/05/11/microsoft-wins-awards-at-the-european-identity-conference-2010.aspx [↑](#footnote-ref-114)
115. Communiqué de presse International Association of Privacy Professionals Honors Top Privacy Innovators : https://www.privacyassociation.org/about\_iapp/2010\_09\_30\_iapp\_honors\_top\_privacy\_innovators/ [↑](#footnote-ref-115)
116. Projet de recherche européen ABC4Trust (Attribute-Based Credentials for Trust) : http://www.abc4trust.eu/ [↑](#footnote-ref-116)
117. Projet européen STORK (Secure Identity Across Borders Linked) : https://www.eid-stork.eu/ [↑](#footnote-ref-117)
118. Site portail Web Microsoft IDA : http://www.microsoft.com/identity [↑](#footnote-ref-118)
119. Site Microsoft Interopérabilité : http://www.microsoft.com/france/interop [↑](#footnote-ref-119)
120. Communiqué de presse Microsoft Makes Strategic Changes in Technology and Business Practices to Expand Interoperability : [↑](#footnote-ref-120)
121. Site Microsoft Standards : http://www.microsoft.com/france/standards [↑](#footnote-ref-121)
122. Forum des Architectures Applicatives Microsoft: http://linkd.in/archiappms [↑](#footnote-ref-122)