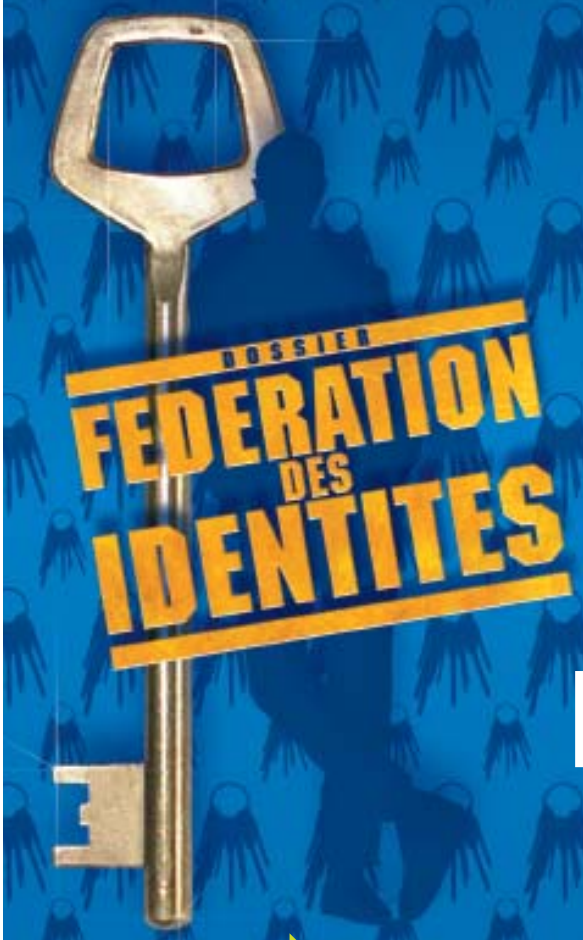


Paroles de CONSULTANTS

LES PROJETS DE FEDERATION DES IDENTITES ENTRE TECHNIQUE ET PEDAGOGIE

La mise en œuvre d'une solution de Fédération d'Identités n'échappe pas à la règle de tout projet de sécurité : elle nécessite de bonnes connaissances techniques, une excellente organisation et une véritable stratégie de communication. Mais dans ce genre de projet, le RSSI a un rôle moins central que lors de la mise en œuvre d'outils de sécurité plus classiques. Il agit en amont en tant que conseil, puis comme garant de la politique de sécurité. Dans le même temps, il a une tâche de pédagogue auprès des salariés de l'entreprise en mettant en avant le confort d'utilisation par la suppression des mots de passe multiples, tout en préservant dans certains cas l'anonymat et la confidentialité de certaines opérations réalisées par les utilisateurs.

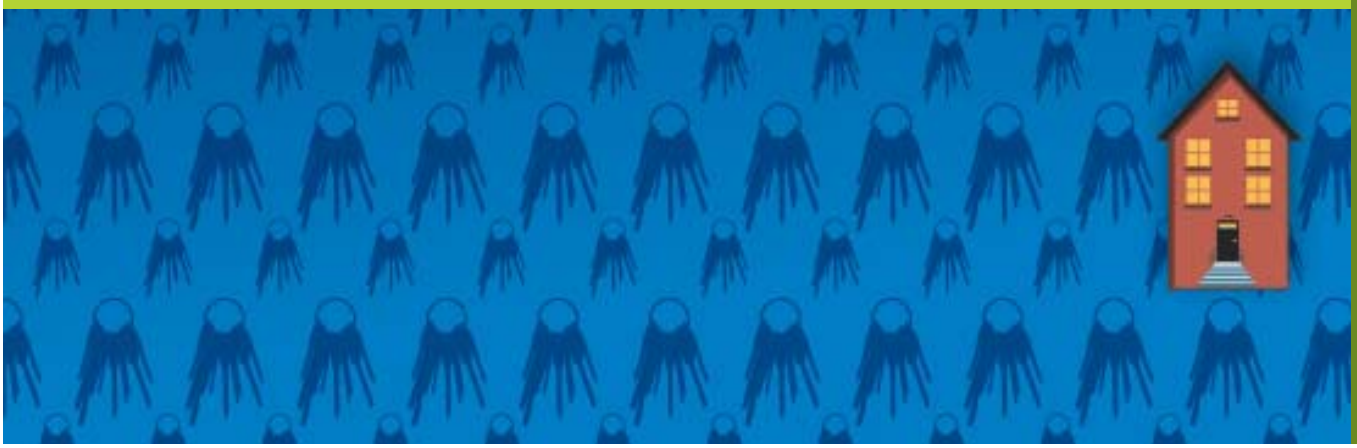
Nos quatre experts, Sylvain Barbier, Consultant Senior Identity & Access Management chez Cyber Networks, Philippe Dajean, Consultant chez SoluCom, Igor Herrmann, Directeur des opérations et Directeur général de Vipawan et François Vergez, Senior Manager chez Deloitte, expert en sécurité des systèmes d'informations estiment que cette technologie est vouée à un bel avenir. Pour le moment, les réalisations sont toutefois peu nombreuses.

Sylvain Barbier, Cyber Networks

Pour Igor Herrmann, la gestion de la Fédération d'Identité (FIM, Federated Identity Management en anglais) est une appellation qui regroupe à la fois des concepts, des protocoles et des outils et qui est, encore aujourd'hui, en phase d'évolution. Peu de solutions FIM sont déployées, notamment en France. Ces projets ont pour objet de donner une identité numérique unique à un individu (physique), avec une liste de propriétés et d'attributs, gérée et sécurisée en un point unique, mais accessible. Cette identité numérique est reconnue et partagée par des entités administratives différentes. L'objectif est double : faciliter l'activité des utilisateurs et unifier la gestion des droits au travers de systèmes d'informations techniquement différents, et gérés par des entités différentes.

Fédérer les identités ne signifie pas les authentifier

Selon Igor Herrmann, il est donc



CONCEPTS ET PRINCIPES DE FONCTIONNEMENT PAR PHILIPPE DAJEAN SOLUCOM

Le service de fédération se base sur la définition d'un domaine de confiance, rassemblant des fournisseurs d'identités et des fournisseurs de services :

- Le fournisseur d'identités (IdP : Identities Provider) réalise les tâches d'identification et d'authentification des utilisateurs du domaine de confiance. Il cherche les attributs utilisateurs dans les annuaires ou les bases de données, applique la politique de sécurité du domaine pour réaliser l'authentification, et transmet les attributs nécessaires à la ressource demandée par l'utilisateur, pour que celle-ci accorde l'autorisation.
- Le fournisseur de services (SP : Services Provider) réalise le contrôle des autorisations d'accès aux ressources. Il lit les attributs transmis par le fournisseur d'identités du domaine. Ce dernier les a reçus du fournisseur d'identités du domaine de référencement de l'utilisateur (auquel il fait confiance). Le SP applique alors sa propre politique de sécurité pour autoriser l'accès.

Les fournisseurs d'identités et de services s'échangent des assertions de sécurité. Ce sont des requêtes et des réponses servant à l'authentification, à l'autorisation ou encore à véhiculer des attributs.

L'authentification se base sur l'échange de preuves d'authentification : mots de passe, certificats…

Le principe de fonctionnement de la fédération des identités est illustré sur la Figure 1 et est décrit ci-dessous :

1. L'utilisateur est référencé dans le domaine de confiance 1. Il souhaite se connecter à une ressource appartenant au même domaine de confiance (SP2 sur le schéma).
2. La ressource s'adresse à l'IdP du domaine auquel elle appartient (IdP1) pour demander des informations d'identification sur l'utilisateur : s'est-il authentifié ? La ressource demande éventuellement des attributs concernant l'utilisateur pour autoriser l'accès.
3. L'utilisateur ne s'est pas encore authentifié dans la fédération, donc l'IdP1 lui demande des preuves d'authentification.
4. L'utilisateur fournit des preuves d'authentification.
5. Si l'authentification est réalisée, l'IdP1 transmet les informations d'identité de l'utilisateur nécessaires à son autorisation auprès du SP2, qui l'accepte.
6. L'utilisateur accède à la ressource demandée, le SP2.
7. L'utilisateur décide ensuite d'accéder à un service de la fédération, mais appartenant à un autre domaine.
8. Le SP de la ressource distante (SP5) se tourne vers l'IdP de son domaine (IdP2) pour demander des informations d'identification. L'IdP2 ne connaît pas l'utilisateur, mais a reçu les informations d'identité le concernant au moment de son identification auprès de l'IdP1 (ou bien il les demande à l'IdP1 à ce moment). C'est la relation de confiance entre les domaines de confiance 1 et 2 qui autorise le transfert d'informations d'identité entre les deux IdP.
9. L'IdP2 renvoie les informations d'authentification au SP5.
10. Le SP5 autorise l'accès à l'utilisateur avec les droits appropriés.

nécessaire de bien distinguer la notion de Fédération des Identités (FIM) de la notion d'authentification et surtout de celle de gestion des accès et des identités (IAM, Identity Access Management). Effectivement, reprend François Vergez, dans ce cadre, elle doit permettre la communication et l'interaction de solutions de Gestion des Identités d'entités différentes, comme par exemple une entreprise et ses fournisseurs, une entreprise et ses partenaires, deux entreprises d'un même

François Vergez, Deloitte

IDENTITY FEDERATION
CONSULTANT VIEWPOINT
IDENTITY FEDERATION PROJECTS: A BLEND OF TECHNOLOGY AND EDUCATION

The implementation of an identity federation solution is subject to the same rules as any other security project: it requires good technical know-how, excellent organisation and a good communication strategy. But with this type of project, the information system security manager plays a less central role than in the implementation of the more traditional security tools. He acts as a consultant in the initial stages and subsequently ensures that everything fits in with the overall security policy. He also has an educative role to play, ensuring that employees understand that the elimination of multiple passwords improves usability and that anonymity and confidentiality, when needed, are not compromised.

Our four experts, Sylvain Barbier, senior Identity & Access Management consultant with Cyber Networks, Philippe Dajean, consultant with SoluCom, Igor Herrmann, operations director and general manager of Vipawan and François Vergez, senior manager with Deloitte, experts in information system security, consider that the technology has a bright future. For the moment though, few projects have actually been implemented.

groupe… Pour une entreprise, la Fédération des Identités n'a de sens que si les solutions de Gestion des Identités sont fonctionnelles. Mais, rappelle Sylvain Barbier, il ne faut pas oublier que son objectif est la simplification des échanges entre partenaires. Elle permet aux utilisateurs d'un des partenaires d'accéder aux ressources d'un autre partenaire, de façon sécurisée et digne de confiance. Ces accès ne nécessitent aucune authentification supplémentaire, car ils sont intégrés dans l'authentification unique Web de l'entreprise (Web Single Sign-On). La Fédération d'Identités étend le périmètre de la Gestion des Identités de l'entreprise à ses partenaires. Techniquement, conclut Philippe Dajean, son principal objectif est de rendre interopérables des systèmes de gestion des identités et des accès, et de déterminer un domaine de confiance.

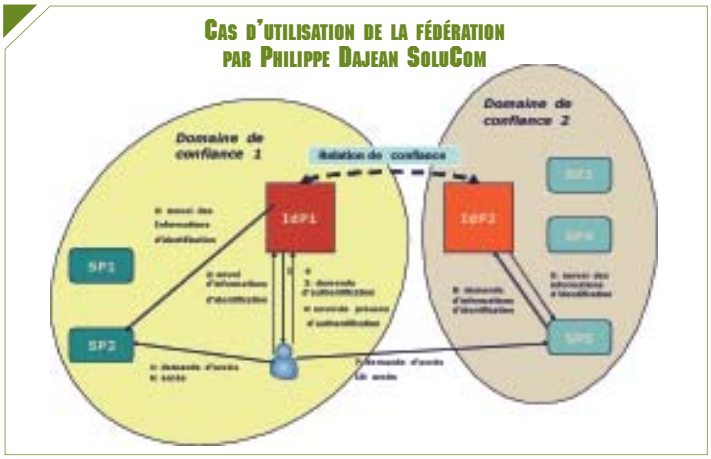
Dans les grandes lignes, lorsqu'un utilisateur souhaite accéder à une ressource proposée par un tiers, il peut présenter une nouvelle identité et des informations le caractérisant. Celles-ci permettent au tiers de l'identifier et de lui autoriser l'accès à la ressource demandée. L'utilisateur peut contrôler les informations transmises et en particulier :

- Choisir l'identité qu'il présente et par exemple accéder aux ressources de manière anonyme.
- Présenter une preuve d'authentification (couple identifiant / mot de passe, certificat…) qualifiée par un niveau d'authentification.

De plus, la fédération peut fournir à l'utilisateur un Single Sign-On (authentification unique) sur l'ensemble des ressources de la fédération.

Globalement, dans un environnement distribué, où chaque partenaire dispose de son propre SI, la fédération permet l'accès croisé aux ressources logiques. Elle peut, par exemple, être proposée à des clients d'une société de transport aérien qui a passé des accords commerciaux avec une chaîne hôtelière. Avec la fédération, le client pourra bénéficier d'une offre préférentielle de séjour dans un hôtel partenaire, correspondant aux dates du voyage, tout en étant un parfait inconnu pour cette chaîne hôtelière.

Cas d'utilisation de la fédération par Philippe Dajean SoluCom



L'ouverture des SI est l'élément déclencheur de tout projet de fédération

Pour nos quatre experts, le principal élément déclencheur d'un projet de fédération d'identités dans une entreprise est l'ouverture de son Système d'Information à des tiers. Ainsi, Sylvain Barbier voit deux motivations : la multiplicité des applications externes auxquelles les utilisateurs de l'entreprise doivent accéder (applications hébergées, applications de partenaires, etc) et l'ouverture du SI de l'entreprise aux partenaires, comme la création d'un service auquel les utilisateurs de multiples entreprises pourront accéder. La mise en œuvre de telles solutions permet d'améliorer l'expérience utilisateur au-delà du SI de son entreprise (authentification unique étendue), de simplifier la Gestion des Identités entre partenaires et de réduire les coûts de Gestion des Identités des applications inter-partenaires.

Philippe Dajean, SoluCom

Igor Herrmann, Vipawan

Igor Herrmann estime que le critère numéro un est le fait qu'une entité se définisse comme appartenant à une communauté de confiance (de type économique ou stratégique) et que cette entité veuille faciliter l'accès aux ressources pour les utilisateurs ou clients de la communauté. Il faut que cette volonté soit partagée par tous et qu'ils acceptent le principe de créer un anneau de confiance, à savoir accepter que la phase d'authentification de l'utilisateur soit réalisée par une autre entité qu'eux-mêmes. Cela peut également impliquer, à terme,

AVANTAGES D'UN PROJET DE FÉDÉRATION D'IDENTITÉS PAR FRANÇOIS VERGEZ, DELOITTE

La maîtrise et la réduction des risques

- Protéger son patrimoine informationnel,
- Gérer de manière globale et cohérente les utilisateurs et leurs habilitations,
- Identifier les tentatives d'accès malveillants,
- Répondre aux contraintes légales et réglementaires (SOX, loi sur la sécurité financière, protection de données personnelles…).

La création de valeur

- Réduire les coûts d'administration,
- Supporter au meilleur coût les enjeux métiers de l'entreprise, qui se traduisent principalement par l'ouverture de son système d'information à l'ensemble de ses partenaires et par les nouveaux modes de communication (mobilité),
- Accélérer la disponibilité des nouvelles applications en s'appuyant sur des services communs de gestion des utilisateurs et de leurs habilitations.

d'étendre sa confiance à l'externalisation complète des bases d'authentification et de gestion des droits, ce qui reste culturellement peu développé aujourd'hui. De manière plus modeste, la volonté de partager les informations utilisateurs d'annuaires différents et d'établir des relations transitives de confiance est, en soi, déjà un projet de FIM. C'est par exemple ce qui se passe dans des relations d'approbations entre domaines Windows, entre services d'une même entreprise ou entre filiales d'un même groupe. Les avantages sont liés à l'existence d'une architecture de SSO permettant une transparence des fonctions d'authentification pour l'utilisateur. Fini les "pop up" de demande de saisie du login mot de passe.

La Fédération pour soutenir la gouvernance institutionnelle et créer de la valeur

François Vergez remarque que, comme pour la Gestion de l'Identité, les projets de Fédération des Identités, qui ont pour objet l'ouverture des SI vers des utilisateurs externes, soutiennent d'une part la gouvernance institutionnelle des entreprises en permettant de maîtriser et de réduire les risques d'accès non autorisé à l'information sensible. D'autre part, ils aident aussi la gouvernance d'activité en créant de la valeur et en améliorant la performance. Philippe Dajean voit dans ces déploiements deux moteurs : les enjeux métiers et les logiques de consolidation.
Dans le premier cas, les stratégies de sourcing de plus en plus développées (travail collaboratif avec de nombreux partenaires : sous-traitants, voire concurrents) induisent une nécessité d'ouvrir les SI, tout en protégeant savoir-faire et propriété intellectuelle. Ceci est encore plus vrai dans un contexte de mondialisation. Il devient fondamental de collaborer et de fluidifier les échanges tout en garantissant sa sécurité.

Pour le second cas, l'organisation des entreprises en entités autonomes et en filiales implique une plus grande complexité avec le plus souvent une gouvernance déléguée. Il s'agit de permettre des accès croisés aux ressources de l'entreprise tout en préservant l'existant et l'indépendance de chacun.
Sans fédération, les entreprises ont deux possibilités : chaque partenaire de la fédération gère l'ensemble des populations accédant à ses ressources, ou bien il récupère les informations par consolidation des bases utilisateurs (annuaires ou bases de données). Dans le premier cas, outre des modes d'accès différents pour les utilisateurs, les entreprises ne pourront que difficilement tracer les mouvements des personnes : il sera compliqué d'identifier ceux qui accèdent aux ressources. De plus, le système sera moins réactif, il ne permettra pas de tenir à jour les entrées et les sorties dans le SI. Ces deux facteurs entraînent un affaiblissement du niveau de sécurité.
Dans le second cas, les flux de consolidation sont complexes à mettre en œuvre et coûteux.
A l'inverse, la fédération permet de lever ces différentes contraintes car elle met en place une relation de confiance entre partenaires. Cette relation s'appuie sur deux principes régis par des conventions partagées : chaque partenaire a la responsabilité de ses utilisateurs, et celle de protéger l'accès à ses ressour-

ces. Ce mode décentralisé est évolutif. Il permet d'intégrer au fur et à mesure de nouveaux partenaires de fédération, à coût marginal, et en maintenant la sécurité des échanges.

En France, les organisations mettant en œuvre ces projets sont les pouvoirs publics et les opérateurs

Ainsi, les principales organisations qui ont aujourd'hui déployé des solutions de Fédération des Identités sont de très grandes entreprises dont l'organisation est décentralisée ou des entreprises qui doivent gérer de nombreux partenaires externes, des universités, et les services publics. En France, il n'y a que très peu de déploiement. Sylvain Barbier a recensé les cas suivants de fournisseurs d'identités souhaitant proposer un nombre important de services :

- Les administrations, l'éducation : Portail Mon Service Public (scénario 3 page https://mon.servicepublic.fr/portail/img/visite_index.swf)
- Les opérateurs : Microsoft Passport (https://accountservices.passport.net/ppnetworkhome.srf?vv=410&lc=1033), Orange

Les fournisseurs de services souhaitant simplifier leur intégration avec leurs clients fournisseurs d'identités :

- Les assurances

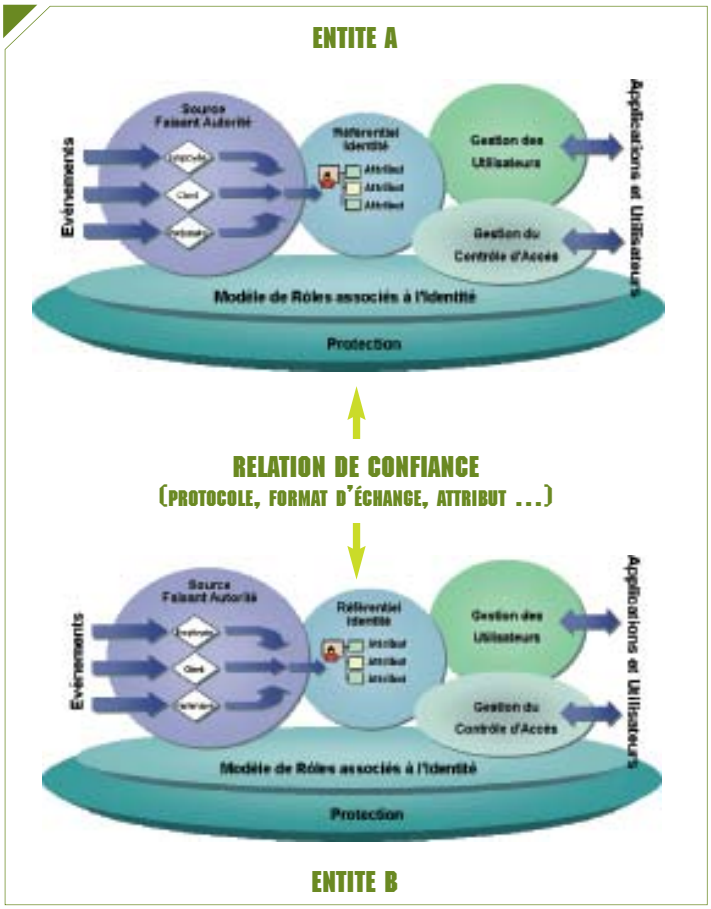
Philippe Dajean complète cette énumération par les domaines de l'industrie automobile et de l'énergie du fait de la taille des entreprises, de la généralisation de la sous-traitance, de l'ouverture internationale et des alliances commerciales. Il constate que dans le reste du monde, et en particulier aux Etats-Unis, les projets sont bien plus nombreux.

La dimension organisationnelle est la base de tout déploiement

François Vergez, faisant un parallèle avec les projets de Gestion des Identités, est convaincu que le facteur clé de réussite d'un projet de Fédération des Identités est l'organisation. Avant tout déploiement de solutions techniques, les processus de gestion des utilisateurs et de leurs habilitations doivent être définis, formalisés et documentés :

- Quels sont les utilisateurs ? (salariés, stagiaires, prestataires de services, partenaires, clients …)
- Qui est à l'origine de l'identité des utilisateurs (Ressources Humaines, Direction Métiers, Services Généraux, DSI,…) ?
- Comment le cycle de vie de l'identité des utilisateurs est-il géré (création, modification, suppression, …) ?
- Comment sont gérées les habilitations des utilisateurs ?
- Quelles sont les identités strictement Internes et Externes ?

Ainsi, les solutions de Fédération des Identités définissent des



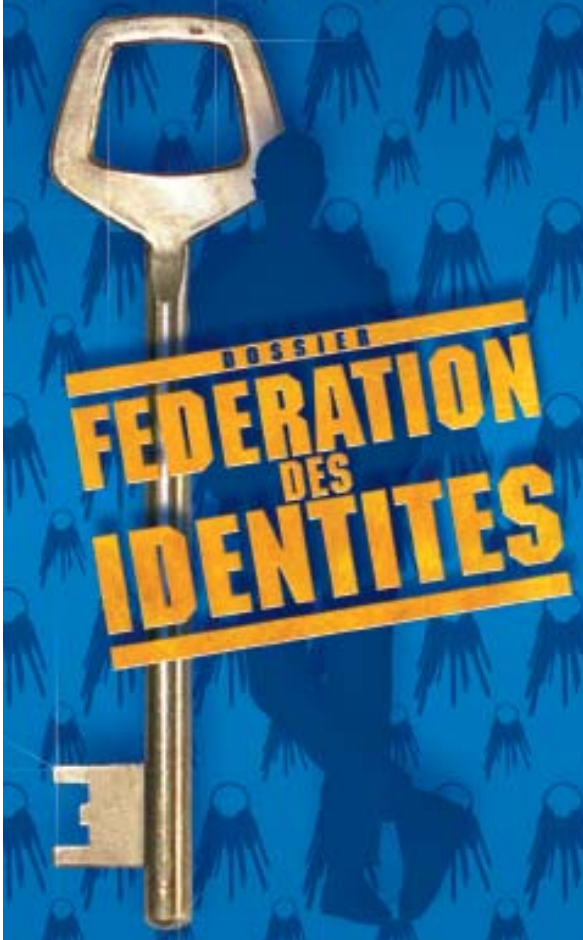
relations de confiance entre les solutions de Gestion de l'Identité :

1. Source faisant Autorité : une source faisant autorité est un élément du système d'information à l'origine d'une partie de l'identité de l'utilisateur,
2. Référentiel d'Identité : les identités, provenant d'applications et de systèmes différents, sont gérées et consolidées afin d'assurer une identité globale,
3. Gestion des utilisateurs : La gestion des utilisateurs est assurée depuis un point central de contrôle,
4. Gestion du contrôle d'accès : Le contrôle d'accès s'appuie sur des rôles et permet une approche flexible de l'authentification et de l'autorisation à partir d'un point central de contrôle,
5. Modèle de rôle associé à l'Identité : Les rôles des utilisateurs sont décrits, formalisés et documentés en fonction de profils « métiers »,
6. Protection : La définition globale des moyens nécessaires afin de sécuriser la solution de gestion de l'identité.

Sur le plan technique, Sylvain Barbier retient uniquement deux éléments :

- Le ou les fournisseurs d'identités nommés IdP (Identity Provider)
- Le ou les fournisseurs de services nommés SP (Service Provider), qui sont également les consommateurs d'identités.

Pour conclure, le fournisseur d'identités gère l'authentification des utilisateurs ainsi que la relation avec les fournisseurs de services SP ou d'autres fournisseurs d'identité. C'est également lui qui permet une authentification unique des utilisateurs.



Paroles de CONSULTANTS

LA FEDERATION DES IDENTITES REPOSE SUR UNE TECHNOLOGIE MATURE, MAIS LE CHOIX D'UN STANDARD RESTE CORNELIEN

Les composants logiques de la fédération, fournisseurs d'identités et de services, doivent s'appuyer sur les systèmes d'IAM existants : serveurs de contrôle d'accès, serveurs web, modules d'authentification et de SSO. Viennent se greffer à ces systèmes des modules spécifiques qui mettent en œuvre la génération et l'échange des assertions de sécurité. Des agents et des proxies peuvent également compléter l'architecture, et ceci sans impact majeur sur l'existant. Mais le point crucial de tout déploiement reste le choix du standard.

Pour Igor Herrmann, une solution de FIM repose, en effet, sur divers éléments : annuaire hiérarchisé, mots de passe, SSO, authentification, interopérabilité entre applications, organisation. Conceptuellement, il distingue trois entités : l'utilisateur (ou plutôt l'application sur le poste de travail), les applications sécurisées qui doivent rendre le service demandé, et surtout le serveur d'identité chargé de la partie validation / gestion des crédits et sessions utilisateurs. Cela a un impact majeur : pour être compatibles avec une solution de FIM, les applications (côtés clients et serveurs) doivent nécessairement être enrichies des fonctions compatibles avec l'un des standards de fait, l'interopérabilité entre normes n'étant pas encore faite.

Le cercle de confiance doit reposer sur les standards Shibboleth, Liberty Alliance, WS-Fédération, SAML 2.0…

Il faut rappeler, rebondi Philippe Dajean, qu'à la marge, la gestion

de l'annuaire des acteurs de la fédération peut entraîner une modification des schémas d'annuaire ou encore la mise en œuvre d'un service de découverte (composant supplémentaire décrit par certaines spécifications comme Shibboleth ou Liberty Alliance). Un projet de fédération intervient donc nécessairement après un projet d'IAM. Il réunit, en effet, et met en cohérence plusieurs de ces systèmes. Effectivement, reprend Igor Herrmann, sans vouloir réduire les fonctions de FIM, on peut dire qu'elles s'appuient sur les concepts de SSO et d'IAM. Le tout sera centralisé en un point unique, interrogeable de manière sécurisée et limitée, par toutes les ressources que l'utilisateur sollicite. La dimension n'est donc pas la même. C'est dire l'ambition qui a prévalu à la définition de ce concept !
En l'absence de fédération, reprend Philippe Dajean, les possibilités de gestion des informations d'identité utilisateurs entre les différents domaines se limiteraient à la synchronisation de login/mot de passe. La fédération permet en plus de véhiculer des informations contenues dans les attributs utilisateurs, qui permettent de la personnalisation et du contrôle d'accès, et ceci même si la personne se présente sous un pseudonyme. La fédération apporte également des avantages significatifs pour le SSO inter-domaines. Le cookie de fédération délivré par le premier fournisseur d'identités est valide dans les autres domaines DNS, sur la base des règles de confiance qui existent entre les fournisseurs d'identités.

D'une façon pratique, Sylvain Barbier remarque que les solutions de Fédération d'Identités sont basées la plupart du temps sur des protocoles d'échange normalisés tel que SAML, Liberty Alliance, etc. Un cercle de confiance commercial et technique est alors établi entre les partenaires. L'utilisateur peut ensuite lier (fédérer) 2 identités existantes afin d'accéder aux services des 2 partenaires de façon transparente (sans réauthentification). Lorsque l'utilisateur n'a pas encore accédé aux services du second partenaire, un processus de provisioning peut automatiser la création de son identité ainsi que sa fédération. Une fois la fédération effectuée au niveau de l'utilisateur, celui-ci peut accéder aux services des 2 partenaires avec une authentification unique.

Dans cette configuration, il est évident que chaque composant est essentiel. Toute défaillance, dysfonctionnement ou inefficacité de l'un des composants remet en cause la solution dans son ensemble, conclut François Vergez.

Les standards sur la sellette

Avant même de parler d'architecture idéale, Philippe Dajean est convaincu que le premier sujet à traiter est le choix du standard. En effet, une architecture de fédération s'inspire d'un modèle de sécurité défini dans un standard de fédération : SAML (Security assertion markup language), Liberty Alliance, Shibboleth, ou encore WS-Federation. Les fournisseurs d'identités et les fournisseurs de services s'échangent des messages dans le format, suivant les protocoles définis par le standard. L'agrégation de nouveaux domaines à la fédération nécessite que ces domaines implémentent des standards interopérables avec l'existant. La solution qui offre le plus de possibilités d'interopérabilité est le choix de SAML 2.0. Si les domaines de confiance implémentent des produits de Microsoft, le choix de WS-Federation est à considérer : WS-Federation n'est pas interopérable avec les autres standards, mais associé à d'autres spécifications de sécurité (la suite WS-*), il présente des fonctionnalités riches, comparables avec celles de SAML 2.0.
Si le même standard ne peut être utilisé par tous les membres de la fédération à cause de l'existant ou de choix technologiques divergents, le problème d'interopérabilité peut être en partie résolu à l'aide de passerelles de fédération. Une passerelle de fédération permet ainsi de

Identity federation
Consultant viewpoint
Although identity federation is based on mature technology, the choice of a standard is not so easy

The logical components of identity federation, i.e. those which supply IDs and services, must be based on existing IAM systems: access control servers, web servers, authentication modules and SSO functions. In addition, specific modules need to be added for generating and exchanging security assertions. Agents and proxies can also be part of the overall architecture. These additional components should be designed so as not to have any significant impact on existing systems. However, the critical part of any implementation is the choice of standard.

traduire les messages de sécurité d'un standard vers un autre. Toutefois, une passerelle traduit rarement toutes les spécifications du marché et son utilisation génère une augmentation de la charge sur les serveurs. Cette solution doit donc être considérée uniquement dans le cas où aucun accord ne peut être trouvé.

La problématique de l'architecture n'est pas que technique....

Pour mettre en place une « bonne » architecture Igor Herrmann affirme que le niveau d'hétérogénéité de l'environnement et de la culture du client ont beaucoup d'importance. Il est parfois délicat de proposer des solutions Open-source, même très efficaces dans des environnements Windows et inversement. La présence dans le système d'information de briques d'un éditeur plutôt qu'un autre est encore, aujourd'hui, le principal facteur de choix. Bien sûr, rajoute Philippe Dajean, l'architecture mise en œuvre dépend directement des usages de la fédération d'identités. Dans un usage classique, elle est très distribuée (de nombreux fournisseurs d'identités et d'accès). Un usage très orienté « grand public » (chaîne hôtelière, voyages…) aura tendance à restreindre le nombre de fournisseurs d'identités par rapport au nombre de fournisseurs de services. Il est même possible que l'utilisateur soit maître de la création de son identité, ce qui revient à ne plus avoir de fournisseur d'identités. C'est ce que propose la technologie Windows CardSpace/InfoCard de Microsoft. Dans tous les cas, Sylvain Barbier conseille d'utiliser des architectures basées sur des standards ouverts tel que Liberty Alliance.

L'architecture recommandée par François Vergez est celle qui saura répondre :

- aux exigences des Métiers,
- aux exigences fonctionnelles des processus de gestion des utilisateurs et de leurs habilitations,
- au modèle de gouvernance des systèmes d'information de l'entreprise,
- à la culture d'entreprise.

Une offre pléthorique, mais encore peu de projets

Si, en France, les réalisations ne sont pas encore très répandues, l'offre de produits de fédération est déjà bien avancée.
Parmi les leaders Philippe Dajean cite spontanément Microsoft qui propose le produit ADFS (Active Directory Federation Services pour Windows Server 2003), basé sur les spécifications WS-Federation. Celles-ci s'intègrent dans la suite WS-* (spécifications de Microsoft sur les Web Services) et l'ensemble fournit une solution de fédération riche et sécurisée. Ce produit est généralement réservé aux environnements Microsoft. Les principaux acteurs de l'IAM tels que BMC, CA, HP, IBM, Oracle, RSA, Sun ou bientôt Novell, ont choisi d'implémenter 2 ou 3 des standards dans leurs produits, laissant un plus large choix aux entreprises. Notons que la plupart des éditeurs intègrent SAML 2.0 dans leur plan de route (même si peu d'entre eux le supportent à l'heure actuelle). Ce standard proposera ainsi une plus grande interopérabilité entre les produits. Enfin, Oracle, HP ou PingIdentity proposent des passerelles de fédération (produits récents, usages peu répandus, mises en œuvre encore rares aujourd'hui et techniquement viables qu'en présence d'un nombre réduit de domaines de confiance). Pour François Vergez comme pour Sylvain Barbier, les premiers acteurs viennent du projet Liberty Alliance : Sun, Novell, Oracle, CA,

HP, RSA… Microsoft a lancé son propre protocole : WS-Federation. Il l'a développé avec l'aide notamment d'IBM, membre par ailleurs de Liberty Alliance…

Un déploiement freiné par l'organisation, la technologie et le manque d'interopérabilité

François Vergez souligne que les limites, mises à part celles inhérentes à toute solution en fonction du contexte technique, sont avant tout liées à l'inefficacité, à la défaillance voire à l'absence de processus organisationnels de gestions des utilisateurs et de leurs habilitations. Sur le plan technique, Philippe Dajean voit des limites inhérentes à la fédération : tout d'abord, la nature et le fonctionnement des composants mis en œuvre dans le cadre d'une fédération ne permettent d'offrir des services qu'en environnement Web. De plus, il existe des limites sur la finesse des autorisations qui peuvent, voire qui doivent, être gérées : seul un premier niveau de contrôle d'accès (applications, principaux modules des applications…) est pris en compte.
Par ailleurs, il recense aussi celles dues au manque d'interopérabilité. Celles-ci dépendent de deux facteurs : le standard de fédération supporté et l'implémentation technique qui en est faite par l'éditeur. Comme évoqué précédemment, SAML 2.0 est la réponse attendue. Il devra néanmoins faire ses preuves en conditions opérationnelles. Enfin, les produits n'offrent bien souvent le maximum de fonctionnalités que s'ils viennent compléter la suite de gestion des identités et des accès du même éditeur. Toutefois, constate Sylvain Barbier, « l'interopérabilité des protocoles d'échange tend à s'améliorer avec la convergence des standards Liberty Alliance / SAML / WS-Federation.
Cependant, l'interopérabilité entre les solutions de Fédération d'Identités et la Gestion des Identités de différents éditeurs manque également. Enfin, les solutions actuelles ne sont pas encore intégrées nativement avec les solutions de Gestion des Identités des éditeurs. » Si le projet de FIM a, originellement, une vocation planétaire, nous en sommes encore loin, résume Igor Herrmann.

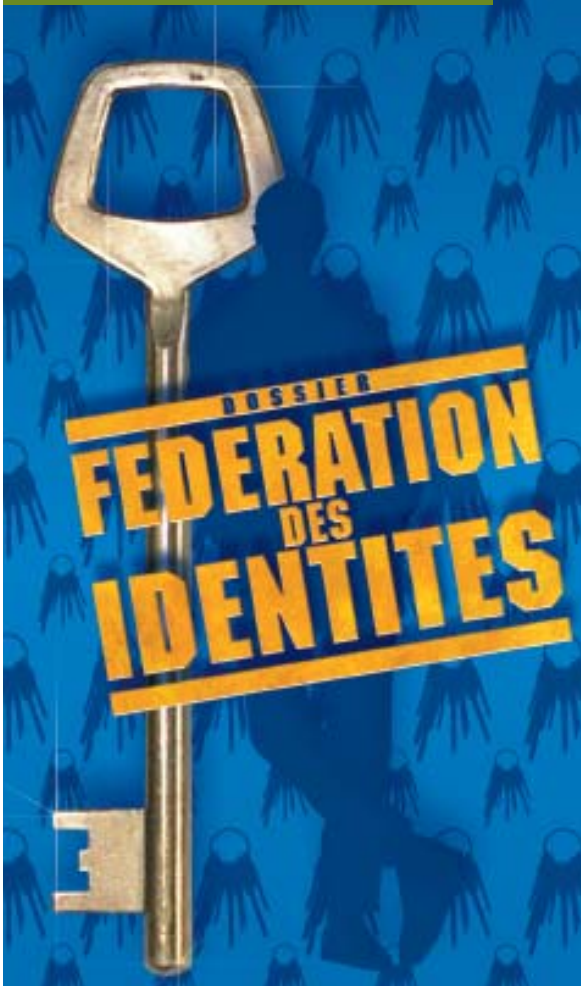
La sécurité repose tout d'abord sur les standards et la technique…

La sécurité de ces solutions repose à la fois sur des standards techniques et sur le principe de confiance entre tous les acteurs.
Au niveau technique, selon Philippe Dajean, « le standard SAML permet d'inclure certaines mesures de sécurité. Pour garantir la confidentialité des messages, les assertions SAML peuvent être chiffrées, avec les protocoles SSL ou TLS. L'authentification des parties communicantes (fournisseurs d'identités et de services) peut se faire par échange de certificats. Pour éviter le rejeu des assertions par un tiers non digne de confiance, elles peuvent contenir une limite de durée de validité. Enfin l'intégrité des données peut être garantie par signature numérique des assertions. Toutes ces mesures sont conseillées dans les spécifications SAML, mais n'en font pas partie.
Parmi les spécifications de fédération existantes, c'est celle de Microsoft qui accorde le plus d'importance à la sécurité. En effet, WS-Federation s'associe à WS-Trust et WS-Security afin de sécuriser les échanges. Microsoft définit d'autres composants logiques, en plus du fournisseur d'identités et du fournisseur de services, qui assurent également des fonctions de sécurité : le service d'attributs qui gère la confidentialité, et le service de pseudonymes.
Les spécifications WS-Security adressent notamment les problèmes suivants : altération, divulgation de message, intégrité de la clé, authentification et authenticité, disponibilité des services, rejeu de requête. Les solutions décrites par WS-Security reposent en particulier sur du chiffrement, des signatures, de l'authentification forte par PKI, la sécurisation des cookies de fédération. »
Igor Herrmann distingue la qualité de la conception, de l'implémentation d'un code source à l'intégration d'une solution dans un système d'information.
L'implémentation d'un protocole dans un code, afin d'en faire une application, a, historiquement, toujours fini par poser un problème – dire que c'est presque une question de temps pour voir survenir un problème n'est pas être pessi-

miste. En ce qui concerne le modèle théorique de gestion de la sécurité et du SSO, il est éprouvé. Il est directement dérivé des travaux du MIT et du projet Kerberos, dont les implémentations et les dérivées sécurisent nos réseaux modernes, notamment Windows.
Par contre, des réserves ont été formulées en ce qui concerne les risques liés à des mécanismes de SSO utilisant les cookies de navigateurs : les techniques classiques de Cross Site Scripting, de détournement de navigateur, ou de détournement de réponse DNS, peuvent permettre d'abuser les services utilisant le SSO.Une mauvaise sécurité de l'environnement peut également être la cause de problèmes de sécurité graves : avec une fonction de SSO, le poste utilisateur devra être, par principe, irréprochable en terme de sécurité. Les solutions ne sont donc pas différentes que pour les autres applications du système d'information : transparence et réactivité des éditeurs, veille technologique et réactivité des équipes clients, mais surtout, recherches indépendantes et critiques de la part de la communauté sécurité.
Tous doivent jouer le jeu des bonnes pratiques en terme d'amélioration de la sécurité, sans autre arrière pensée ou entrave artificielle, sous peine de jeter de manière radicale la suspicion sur les mécanismes de SSO et les applications de FIM.

...mais aussi sur la confiance entre les acteurs

Sylvain Barbier concentre son attention sur les problèmes de confiance. En effet, la Fédération d'Identités instaure une confiance mutuelle entre partenaires. Si l'un des partenaires laisse des failles de sécurité apparaître (comptes non-conformes, comptes orphelins), l'autre partenaire peut en subir les conséquences. Ce type de risque implique une garantie de la qualité de Gestion des Identités et des Accès des partenaires, garantie qui pourrait être apportée par des lois et règlements de type SOX, LSF. Une fois de plus François Vergez se positionne sous l'aspect des processus organisationnels (enregistrement d'un utilisateur, suppression d'un utilisateur, modification des rôles d'un utilisateur …). Donc à la base, la sécurité des solutions de Gestion de l'Identité doit être assurée. Ensuite, dès lors que des relations de confiance sont à établir entre les différents systèmes de Gestion des Identités, ces niveaux de sécurité doivent être cohérents ; on perçoit facilement le risque à établir une relation de confiance entre deux systèmes dont le niveau de sécurité serait trop différent… Par analogie avec les Autorités de Certification, les risques sont moins sur la possibilité de craquer une clé de chiffrement que sur la possibilité de contourner la procédure d'enregistrement et d'obtenir ainsi un vrai-faux certificat !
Effectivement, déplore Philippe Dajean, dans le cadre d'une fédération d'identités, une entreprise met en place une relation de confiance avec un tiers et délègue une part des responsabilités, dans la gestion des utilisateurs notamment. Les limites actuelles de ce mode de fonctionnement portent essentiellement sur les moyens de contrôle de l'engagement pris par chaque membre dans cette relation de confiance. Il n'existe pas, en effet, de méthodologie, de règle ou d'outil pour contrôler les engagements, pas plus que de certification de la relation de confiance. Deux facteurs expliquent cela : d'une part la relative jeunesse du sujet, et d'autre part la complexité du contrôle en lui-même. En réalité, très peu de contrôles sont aujourd'hui réalisés. Ils peuvent quelques fois prendre la forme d'audits ponctuels sur une partie, voire sur la totalité, des moyens mis en œuvre.



Paroles de **CONSULTANTS**

FEDERATION DES IDENTITES : LE CONFORT, MAIS PAS SANS L'EFFORT

Malgré un potentiel certain, la France connaît un important retard dans le déploiement de solutions de Fédération des Identités. Il est vrai que la mise en œuvre de tels projets est loin d'être chose facile. Trop souvent, en effet, la définition du projet, des rôles de chacun, de leurs habilitations, etc. reste imprécise et en devient incompréhensible pour les utilisateurs. De plus, le « processus business » de l'entreprise évolue constamment et le système de gestion des identités doit le suivre en permanence.
Cependant, si le projet est suffisamment bien préparé, la Fédération d'identités apporte plus de confort aux utilisateurs ; elle nécessite des efforts de communication intenses en amont de tout déploiement. Pour faire face à ces réticences, nos quatre experts nous font part de leurs conseils pour mettre en œuvre un projet de Fédération d'Identités fiable et efficace, ainsi que des avantages qui, à leurs yeux, rendent cette solution intéressante et accessible.

Réussir un projet de fédération d'identités : de la technique et de l'organisation

Réussir un projet de fédération d'identités nécessite une fois de plus de bonnes connaissances techniques et une organisation « quasi-militaire ».

Côté technique, Igor Herrmann recommande d'analyser, en amont du contexte, les applications à inclure et le choix de la solution et des moyens technologiques. Enfin, il ne faut pas qu'un projet de FIM mette en péril l'ensemble du système d'information. L'analyse des risques et leur traitement doit impérativement faire partie de l'étude en amont.

Sylvain Barbier rappelle que comme dans tout projet IAM, il faut :
- Commencer par un périmètre restreint d'applications, de fonctionnalités et d'utilisateurs.
- Ne pas implémenter des Fédérations propriétaires, utiliser les standards.
- Se baser sur une solution clé en mains, reconnue et opérationnelle. Les solutions Toolkit

sont complexes à mettre en œuvre et leur pérennité face aux évolutions des standards n'est pas garantie.
- Bien dimensionner la solution et prévoir de pouvoir la redimensionner en fonction de la croissance des requêtes et du nombre d'utilisateurs.

Côté organisation, Igor Herrmann explique qu'il est très important d'intégrer l'aspect culturel et de communiquer avec les utilisateurs sur les bons comportements. François Vergez, pour sa part, propose une démarche en six parties :

- Une vision claire de l'impact organisationnel et technique d'un tel projet sur l'entreprise,
- Un sponsor « non technique » et l'adhésion de l'ensemble des parties prenantes (Directions Métiers, DRH, DSI, etc.),
- Des processus fiables de gestion des utilisateurs et de leurs habilitations,
- Une conduite du changement,
- Un déploiement par phase,
- Un suivi régulier afin de s'assurer de l'alignement de la solution avec les enjeux de l'entreprise et ses processus.

Devant l'authentification, « à l'insu de son plein gré », la CNIL reste vigilante et très conservatrice

« Dès lors que des informations d'identités sont stockées dans une entreprise, une déclaration du contenu et des usages qui seront faits de ces informations doit être entreprise auprès de la CNIL. Lorsque les usages viennent à changer comme dans le cas d'une fédération (diffusion des informations à l'extérieur de l'entreprise, accès aux informations par des tiers…) une nouvelle déclaration simplifiée appelée modification de traitement

RÉUSSIR UN PROJET DE FÉDÉRATION D'IDENTITÉS : LES CONSEILS DE PHILIPPE DAJEAN, SOLUCOM

Pour le bon fonctionnement de la fédération, il est nécessaire de définir un cadre d'interopérabilité qui, non seulement, corresponde aux attentes actuelles, mais qui puisse également suivre les évolutions « business » de l'entreprise.
En conséquence, la mise en œuvre d'un projet de fédération nécessite de mener notamment les actions suivantes :

- Établir la politique et les règles de la fédération :
- Conditions d'inscription/retrait, usages de la fédération.
- Responsabilité, engagement des membres (processus de gestion des identités, sécurisation…) et moyens de contrôle de cet engagement.
- Organisation de la fédération (contacts, listes des fournisseurs d'identités et de services…).
- Informations de référence et nomenclatures partagées (nommage et sémantique).
- Garantir l'interopérabilité par le choix d'un standard partagé qui offre le plus de possibilités d'interopérabilité et d'une solution qui s'intègre avec l'existant.
- S'assurer du respect des exigences juridiques et réglementaires relatives à la protection des informations transmises et aux destinataires de ces informations.

D'autre part, la réussite d'un tel projet passe très fréquemment en amont par l'amélioration de la gestion des identités et des accès au sein de chaque entreprise, et en particulier par :

- La révision des processus et de l'organisation de la gestion des identités.
- La mise en place ou le renforcement du contrôle d'accès, de règles d'habilitation.
- La mise en place ou le renforcement des traces et des audits des accès.

IDENTITY FEDERATION
CONSULTANT VIEWPOINT
IDENTITY FEDERATION: EASE OF USE, BUT NOT WITHOUT EFFORT

Despite having real potential, France is significantly behind in the deployment of identity federation solutions. It is true that the implementation of this sort of project is far from easy. Indeed, too often, the project definition, individual roles and authorisations etc., remain unclear and are incomprehensible as far as the users are concerned. In addition, the company's business processes are constantly changing and the identity management system must also follow suit.
However, if the project is sufficiently well prepared, identity federation brings improved ease of use to users. This requires significant up-front communication in all cases. To overcome this reticence, our four experts advise on how to implement a reliable and efficient identity federation project and outline the advantages, which in their view, makes this solution worth while and accessible.

doit être adressée à la CNIL. La CNIL doit donner un « feu vert » pour la mise en œuvre de fichier ou de traitement de données personnelles. En complément, des règlements peuvent s'appliquer en propre pour chaque entreprise, que ce soit par exemple vis-à-vis des représentants du personnel ou des syndicats, » analyse Philippe Dajean. Bien sûr, mais ces contraintes légales et réglementaires à prendre en compte sont les mêmes que celles rencontrées, par exemple, dans des projets de SIRH (système d'information de ressources humaines) ou de CRM (customer relationship management) rajoute François Vergez. Cependant, Igor Herrmann remarque que « l'une des caractéristiques d'une solution de SSO est que l'utilisateur n'a plus le pouvoir de décider s'il veut ou non laisser une trace de son identité (refus de se connecter) et ne contrôle pas non plus (simplement) les données de son profil qu'il transmet puisqu'il ne les saisit plus explicitement. L'authentification se fait finalement, à son insu avec un identifiant unique quelque soit le lieu. Les possibilités de tracer sont plus précises et plus importantes. Des contraintes sont également liées à la notion d'hébergement des données nominatives, donc liées à un individu, sur un serveur centralisé ; elles sont en fait les mêmes que pour les solutions d'IAM. La CNIL est extrêmement vigilante sur ces points et se révèle très conservatrice en la matière. Cependant, rappelle Sylvain Barbier selon les spécificités des besoins, la fonctionnalité d'Aliasing (Aliasing permet d'attribuer plusieurs adresses IP différentes sur une même interface Ethernet) peut être utilisée afin d'empêcher toute fuite et tout croisement d'informations.

La Fédération d'identités apporte plus de confort pour les utilisateurs, mais nécessite des efforts de communication en amont de tout déploiement

Selon Philippe Dajean, les principaux apports de la fédération aux utilisateurs sont la facilité et la rapidité d'accès aux ressources informatiques, à la fois internes et externes à l'entreprise. Le nombre de ces ressources mises à disposition des utilisateurs, et donc les services qui leurs sont rendus, peut ainsi augmenter. Effectivement reprend Sylvain Barbier, les projets de Fédération des Identités apportent des bénéfices aux utilisateurs comme pour un projet de SSO (authentification unique). Il est, par contre, important de les impliquer en amont afin de lever toute question notamment par rapport aux confidentialités des informations personnelles transmises ou non.

Pour Igor Herrmann, aucun doute : « La Fédération d'Identité est un bénéfice ! Le SSO est réellement une demande de la part de toutes les divisions fonctionnelles et même, dans certains cas, des administrateurs techniques. Il existe un véritable consensus sur ce point.

En même temps, il représente un foyer d'inquiétude sur les renseignements stockés et plus particulièrement, sur les moyens de contrôler leur diffusion.

Tout le monde sait aujourd'hui qu'une des menaces en plein développement est le vol d'identité sur Internet. Cela n'incite pas à la confiance, pré requis absolu pour un dossier FIM de grande ampleur.

La solution, pour associer les utilisateurs à un tel projet, passe par plusieurs points :

- Une volonté de communiquer sur les enjeux, les bénéfices et les risques
- Etablir des relations de confiance entre individus en pré requis à l'établissement de

liens de confiance techniques
- Montrer que les outils technologiques s'accompagnent de processus utilisés comme des gardes fous, établis en commun. »

Comment peut-on déterminer un RoI lors du déploiement d'une solution de fédération d'identités ?

La détermination d'un RoI pour un projet de fédération d'identités est un exercice toujours périlleux. François Vergez considère qu'à l'instar des projets de Gestion des Identités, les projets de Fédération des Identités permettent de maîtriser et réduire les risques et de créer de la valeur en améliorant la performance. Le chiffrage d'une réduction de risques ou d'une amélioration de performance est toujours délicat à mener… Cela impliquerait d'ailleurs que l'entreprise dispose d'une comptabilité analytique appropriée. L'adoption progressive de chaque solution apporte un bénéfice concret. Cependant l'implémentation de tous les aspects du modèle de sécurité sera le gage d'un bénéfice maximum. Pour Igor Herrmann, il est un peu à l'image du RoI des fonctions IAM : réduction des coûts indirects liés à la gestion des mots de passe locaux aux applications et aux opérations de gestion des habilitations. On peut imaginer qu'à terme, le FIM étant mutualisé entre plusieurs entités, il permette de limiter les coûts directs et indirects de gestion des bases d'authentification et d'habilitation en les externalisant. Philippe Dajean, pour sa part, estime que les implémentations sont encore peu nombreuses et il est trop tôt pour disposer de références significatives en termes de RoI. La question de l'investissement ne se pose donc pas en ces

termes, et les projets sont déclenchés en raison des moteurs que nous avons précédemment évoqués.
Néanmoins, les postes de gains suivants peuvent être considérés dans une analyse économique :

- Facilité d'accès aux services et donc augmentation de la fréquence ou du nombre d'utilisateurs d'un service.
- Réactivité dans l'attribution et le retrait des accès à des ressources, permettant d'augmenter la productivité associée à l'utilisation de ces ressources.
- Diminution du temps d'administration de la gestion des accès croisés dans la fédération.

Sylvain Barbier propose une méthode de calcul légèrement différente à partir :

- De l'automatisation des tâches manuelles récurrentes de Gestion des Identités sur les applications partenaires.
- De la réduction des coûts d'intégration des applications partenaires suivantes, voire des applications internes dans de grands groupes.
- De la capacité d'ouverture du SI aux partenaires même si elle est difficilement chiffrable

La fédération est un projet transverse qui implique toutes les directions

Nos quatre consultants sont unanimes, à l'instar de François Vergez : « Les projets de Fédérations des Identités sont des projets transverses à l'entreprise ou à un ensemble d'entreprises. Toutes les directions de l'entreprise, qu'elles soient Métiers ou Support (RH, DSI, Services Généraux …), sont des parties prenantes. La DSI ou le RSSI ne sont pas nécessairement les mieux placés pour initier ou soutenir ce genre de projet. Ainsi, leur rôle, comme dans tout projet lié au Système d'Information, est d'être garant de la sécurité du patrimoine informationnel. Nous n'identifions pas de rôle spécifique dans un projet de Fédération des Identités et nous ne pensons pas qu'il doive avoir un rôle d'exploitation de la solution. »
Plus spécifiquement, Philippe Dajean pense que le RSSI peut faire partie des administrateurs de la fédération. À ce titre, il doit contrôler que les engagements pris vis-à-vis de la fédération sont bien tenus par l'entreprise : il doit ainsi veiller à la gestion des identités et des accès au sein de son domaine de confiance (processus, règles d'habilitation, traces et audits…). Plus généralement, il doit s'assurer de la cohérence de sa propre politique de sécurité avec les règles de confiance de la fédération, et de son application. Il peut également être responsable du contrôle du respect des engagements de la fédération par les autres membres, dans les conditions prévues par la politique de la fédération. Enfin, il peut participer à l'évolution de cette politique dans le cadre du cycle de vie de la fédération.

Enfin Igor Herrmann considère deux cas :

1er cas : le RSSI dont l'entité fait partie d'une communauté.

Il est le client des ressources d'authentification et d'autorisation mutualisées.

Le problème reste donc de protéger son système d'information et ceux de la communauté contre :

- les comportements abusifs des utilisateurs légitimes,
- l'usurpation d'identité,
- le contournement des systèmes d'authentification ou des crédits utilisateurs,

- l'escalade de privilège,
- le détournement du poste, voire simplement du navigateur d'un utilisateur,

La conséquence de l'existence d'un SSO et de la délégation de la gestion des droits a de forts impacts.

En cas de problème sur un accès utilisateur, ce sont toutes les applications liées au SSO qui deviennent accessibles, et dans une plus ou moins grande mesure, les données qu'elles renferment.

C'est donc le cas en interne, mais les ressources externes par l'intermédiaire de la Fédération d'Identités deviennent également accessibles. Dans ce second cas, un problème de sécurité prendra une tournure légale complètement différente puisqu' impliquant deux entités juridiques différentes.

2ème cas : le RSSI dont l'entité gère les services d'authentification et d'autorisation de la communauté.

En plus des contraintes du premier cas, il a la responsabilité de la confidentialité de données nominatives et économiques (par exemple numéros de cartes de crédit, renseignements personnels) liées aux identités gérées. Les implications juridiques et légales sont donc d'une toute autre dimension !

Pour être très francs, nous pensons que les projets de FIM accentuent la pression sur le RSSI pour ce qui est de l'organisation, de la sécurité et de la réactivité globale nécessaire aux entités d'une même communauté.

Un incident de sécurité sur l'un des membres d'une communauté fédérée peut donc impacter tous les autres, notamment en ce qui concerne l'accès à des informations confidentielles.

Faire confiance à un tiers - et c'est l'un des principes de tout projet de fédération - ne doit pas signifier absence de contrôle et d'application de mesures de sécurité strictes, et ceci pour le bien de tous.

Notre recommandation aux RSSI est donc, pour l'intérêt même de la structure qui l'emploie :

- de procéder régulièrement à une analyse de risques liés à la mise en place ou à l'extension d'un projet de Fédération d'Identités, notamment sur les implications juridiques et légales ;
- d'obtenir, de déployer les outils et les processus adéquats sous peine d'exiger la suspension du projet de FIM ;
- de préparer, comme pour un plan de « disaster recovery », un plan de réaction et de communication en cas de compromission des accès et de mise en danger de la communauté ;
- d'appliquer avec rigueur les processus et de tenir bon face aux pressions … tout en expliquant avec pédagogie les risques encourus.

Dans la pratique, Sylvain Barbier attribue aux RSSI les tâches d'audit de sécurité régulier des applications ouvertes à l'extérieur (attaques possibles, tests d'intrusion, etc.). Le DSI, quant à lui, devra superviser la solution (évolution du nombre d'identités, performances et croissance, etc).

Chez Cyber Networks, la taille du projet le plus important mené totalise environ 200 millions d'identités techniques, qui concerne 70 millions d'utilisateurs en Europe. Chaque utilisateur dispose de plusieurs identités techniques correspondant à différents fournisseurs d'identités correspondant à plusieurs services. Ce projet regroupe 20 fournisseurs d'identités et 300 fournisseurs de services.
Chez SoluCom, les projets concernent des entreprises possédant un grand nombre de sous-traitants, soit de plusieurs dizaines à plusieurs centaines de milliers d'utilisateurs à gérer (secteur industriel), des entreprises dont l'activité porte sur des métiers soumis à des contraintes réglementaires différentes, imposant une certaine autonomie dans la gestion des utilisateurs (secteur de l'énergie, 30.000 utilisateurs) et des administrations et des collectivités locales (plusieurs millions d'utilisateurs).

Evolution d'un projet de Fédération d'identités
par François Vergez, Deloitte

Une fédération d'identités doit être capable de suivre l'évolution des standards

François Vergez considère que « la Fédération des Identités représente la dernière étape d'une Gestion des Identités réussie, en permettant d'obtenir une Identité Globale. Si aujourd'hui chaque projet de Fédération des Identités ne concerne que quelques partenaires, leur évolution naturelle sera une interopérabilité globale avec l'ensemble des systèmes d'informations qu'ils soient dans la sphère publique, économique, sociale, éducative, privée… » Sans compter qu'elle doit principalement être capable de suivre l'évolution des standards, rajoute Sylvain Barbier.

Bien entendu, elle doit pouvoir intégrer de nouveaux domaines de confiance, rajoute Philippe Dajean. Pour cela, la politique de la fédération doit être mise à jour à chaque nouvelle entrée. Elle doit également supporter de plus en plus de standards et suivre leurs évolutions (en appliquant notamment les mises à jour des produits). Enfin, une solution de fédération peut également évoluer de services simples de fédération (autorisations d'accès croisé, SSO, pseudonymes) vers des services plus avancés (anonymat, niveaux d'authentification…).

L'histoire va vers la fédération, mais l'Homme est-il prêt à se voir « traquer » sur le web ?

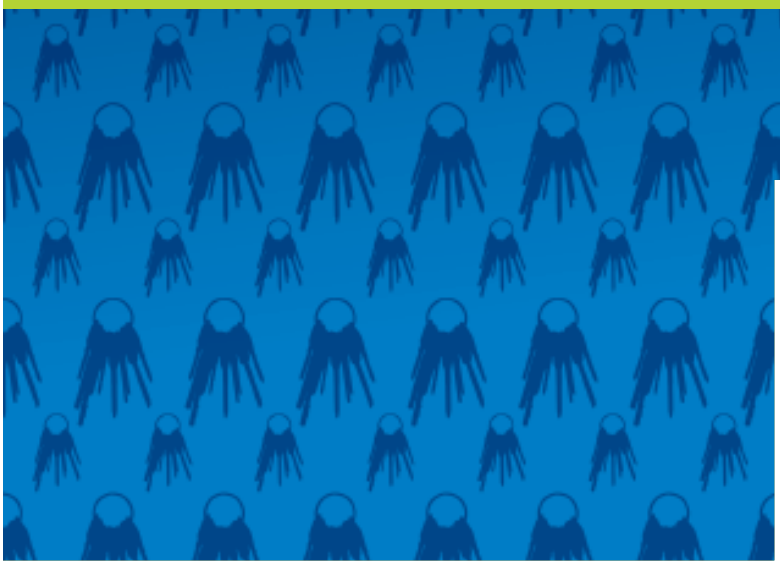
« Tout le monde vous le dira : entre une expérience sans ou avec SSO, la différence est vraiment impressionnante. Cette tendance va dans le sens de l'histoire et d'ailleurs, c'est un peu ce que réalisent nos navigateurs Web en mémorisant nos mots de passe. Eu égard aux dangers d'une fonction de SSO et de l'hébergement des renseignements personnels sensibles, nous recommandons la prudence et la méthode des petits pas. La pression de la simplification pour les utilisateurs et l'idée de centralisation de toutes les données ne doivent pas permettre l'irréparable. Les technologies et les normes sont déjà présentes et réalisent des performances tout à fait étonnantes. Mais l'aspect sécurité et relation avec l'IAM doit être renforcé et devenir plus interopérable. Je ne suis pas certain que culturellement, nous soyons tous prêts. Le FIM repose sur des concepts d'anneau de confiance, d'omniscience et de détention par un tiers et certains de nos attributs. Cela fait tout simplement peur, surtout dans le cas d'une utilisation personnelle ! Pour l'instant seuls des FIM « ponctuels », pour des besoins précis et notamment professionnels, sont envisageables. L'évolution devra surtout marquer positivement les « être humains - identités » que le FIM ambitionne de fédérer. » conclut Igor Herrmann.

Paroles de Consultants
Vue sur l'Open-source

L'OPEN-SOURCE SERA-T-IL LE STANDARD UNIVERSEL DE LA FEDERATION DES IDENTITES ?

La promotion des solutions open-source est particulièrement active en France au sein des projets de fédération des identités. Les standards open-source Shibboleth et Liberty Alliance ont ainsi reçu le soutien de bon nombre d'entreprises. Les Universités avec le standard Shibboleth, et la Gendarmerie Nationale qui utilise Lemon LDAP, sont des exemples reconnus.

Mais il est vrai que les déploiements sont peu nombreux et concernent plutôt les opérateurs télécoms et quelques institutions financières. La mise en œuvre de ces solutions est le plus souvent portée par les DSI avec le support des RSSI. Anne Lupfer, consultant HSC, Nat Makarévitch, co-fondateur d'Idealx et Xavier Fasola, consultant Upperto Groupe Devoteam, soutiennent le développement de ces techniques, car elles sont sources d'économie, améliorent le confort des utilisateurs et la sécurité des SI. Elles nécessitent toutefois un travail important d'étude et d'audit préalable et ne peuvent réussir sans le soutien de l'ensemble des acteurs du cercle de confiance.



Pour nos trois experts des solutions open-source, la fédération d'identités a pour objectif de faciliter l'accès des utilisateurs aux applications par une authentification forte. Nat Makarévitch a retenu, dans sa définition, les concepts d'interopérabilité avec des solutions, libres ou non, d'annuaire, et d'outils de configuration (provisionning) compatibles avec l'existant et ses contraintes. Pour Xavier Fasola, ces solutions doivent permettre un travail collaboratif entre des personnes issues de sociétés différentes en utilisant des applications communes et en partageant les ressources. Anne Lupfer s'est intéressée à la signification de chaque mot : « Composée du mot fédération venant du verbe fédérer, qui signifie dans le cas présent « gérer de façon coordonnée », et du mot « identités » au pluriel qui désigne l'ensemble des identifiants (c'est-à-dire les logins utilisés pour s'identifier), l'expression « fédération d'identités » représente, à son sens, un socle fédérateur pour la gestion d'identités et le contrôle d'accès. En pratique, le concept de fédération d'identités est beaucoup utilisé au sein des portails proposant des services personnalisés, dépendant de l'abonnement souscrit ou des préférences du client. Les opérateurs téléphoniques, les sites marchands et les programmes de fidélité sur Internet sont de bons exemples d'utilisation. »

La liberty Alliance est incontournable pour les solutions open-source ou propriétaires

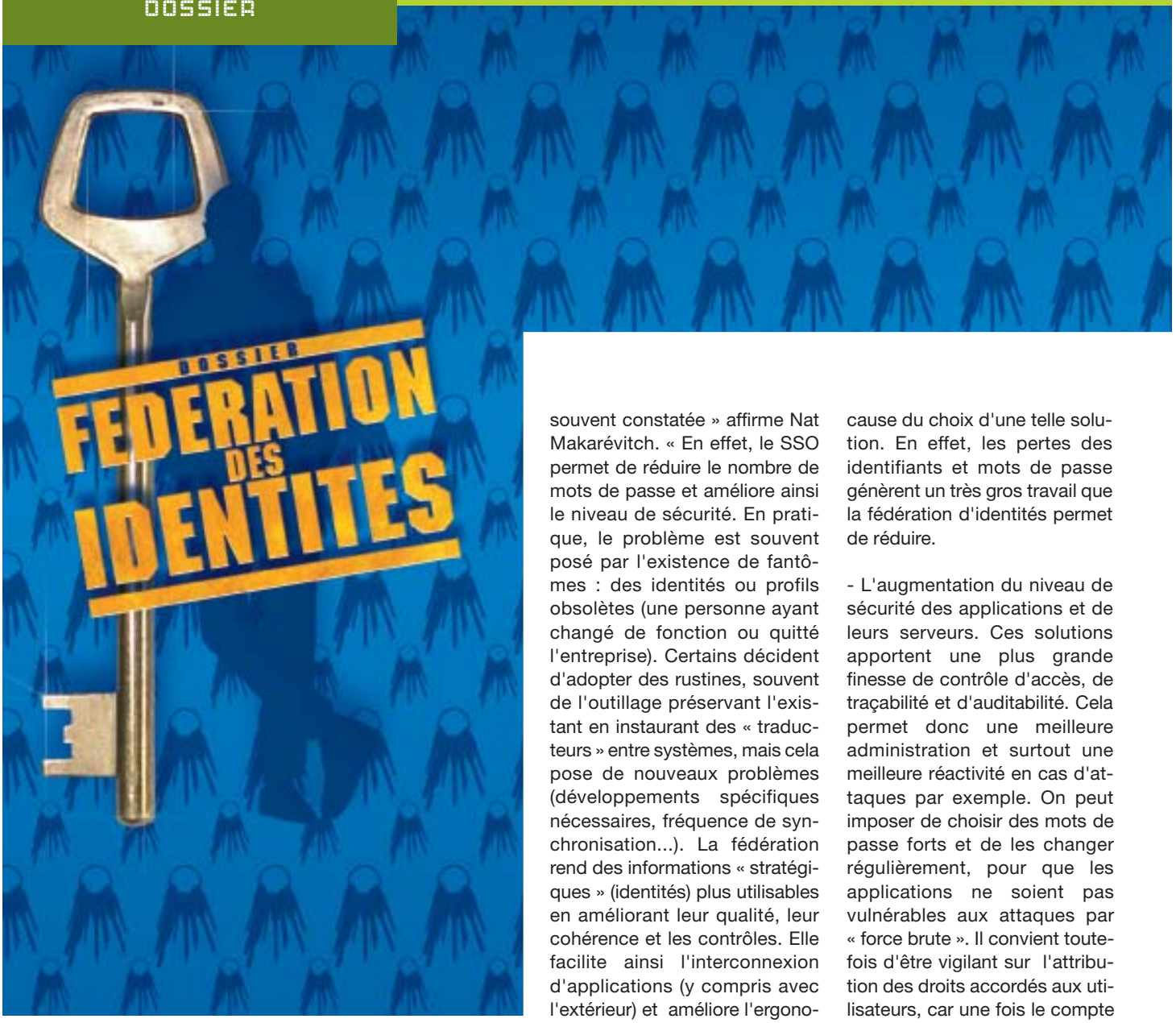
En matière de fédération d'identités la solution du projet Liberty Alliance est incontournable (cf. http://www.projectliberty.org/) et s'impose tant dans le monde open-source et que dans le monde propriétaire. « Même si les solutions propriétaires apportent certains savoir-faire, bon nombre d'éditeurs se sont regroupés au sein de projets comme Liberty Alliance ou Shibboleth (standard utilisé dans les Universités) » remarque Xavier Fasola. Effectivement, reprend Anne Lupfer : « de nombreuses solutions commerciales incluent des éléments de ce projet dans leur solution de gestion d'identités. Elles s'orientent donc vers une approche beaucoup plus complète qui inclut à la fois la gestion des identités et des accès et la gestion de l'authentification unique. Ces solutions basées sur des briques open-source n'apportent pas forcément une clarté aux projets, mais se présentent comme des solutions très complètes et souvent lourdes à mettre en place. Elles proposent aux clients des réponses à des problèmes qu'ils n'ont pas soulevé en compliquant ainsi les tâches de déploiement et d'administration. Avant de choisir sa solution, il convient d'étudier les besoins réels en tenant compte des évolutions futures et de la modularité du produit afin de ne pas s'orienter sur un projet et une solution démesurés. » Nat Makarévitch a une position plus tranchée en faveur de l'open-source : « les solutions open-source sont économiques car elles ne dépendent pas directement des effectifs concernés. De plus, elles sont auditables : des experts peuvent en évaluer l'adéquation (par exemple de s'assurer de l'absence de porte dérobée). Elles réduisent les coûts d'intégration et améliorent la gestion du mode dégradé comme des projets d'extension. La stricte conformité aux normes ouvertes ou, à défaut, la transparence (fourniture du code source), en matière de protocoles comme de formats de données, supprime de nombreux efforts inutiles. Un ensemble technique capable de bloquer tous les accès au SI ne devrait

Anne Lupfer,
Consultant HSC

Identity federation
Consultant viewpoint a look at open source solutions
Will open source be the universal standard for identity federation?

Promotion of open source solutions for identity-federation projects is particularly active in France, and a number of companies have endorsed the open standards Shibboleth and Liberty Alliance. Some well-known examples are the use of Shibboleth by the Universities and Lemon LDAP by the National Gendarmerie.

However, it is true that deployment is not widespread and is more or less confined to telecom operators and a few financial institutions. The implementation of these solutions is often undertaken by IT managers with the support of the information system security managers. Anne Lupfer, consultant with HSC, Nat Makarévitch, co-founder of Idealx and Xavier Fasola consultant with Upperto Groupe Devoteam support the development of these techniques because they provide cost savings and improve system usability and security. However, a significant planning and audit effort is required and success can only be achieved if there is buy-in from all concerned.



pas être opaque car, tôt ou tard, le fait de pouvoir décider librement du niveau de compétence des équipes internes (de l'ignorance totale à la maîtrise complète) rendra plus facile la connexion de nouveaux programmes ou les diagnostiques. »

Confort d'utilisation, attrait du SSO, amélioration de la sécurité et réduction des appels au Help Desk sont les éléments décisifs pour un projet

« L'attrait du SSO est une cause souvent constatée » affirme Nat Makarévitch. « En effet, le SSO permet de réduire le nombre de mots de passe et améliore ainsi le niveau de sécurité. En pratique, le problème est souvent posé par l'existence de fantômes : des identités ou profils obsolètes (une personne ayant changé de fonction ou quitté l'entreprise). Certains décident d'adopter des rustines, souvent de l'outillage préservant l'existant en instaurant des « traducteurs » entre systèmes, mais cela pose de nouveaux problèmes (développements spécifiques nécessaires, fréquence de synchronisation...). La fédération rend des informations « stratégiques » (identités) plus utilisables en améliorant leur qualité, leur cohérence et les contrôles. Elle facilite ainsi l'interconnexion d'applications (y compris avec l'extérieur) et améliore l'ergonomie du SI ainsi que l'exactitude des informations (grâce aux tâches de configuration partiellement effectuées par l'utilisateur et aux délégations), les tableaux de bord et la traçabilité. Elle déso-lidarise, par ailleurs, certaines couches applicatives des services d'authentification de la plate-forme sous-jacente. Dans de nombreux cas, elle améliore la disponibilité et la capacité de montée en charge, car un ensemble central hautement disponible l'emporte à ces titres sur des éléments disparates. »

Anne Lupfer propose une analyse en quatre points :
- La réduction des coûts du Help Desk. C'est souvent la première cause du choix d'une telle solution. En effet, les pertes des identifiants et mots de passe génèrent un très gros travail que la fédération d'identités permet de réduire.

- L'augmentation du niveau de sécurité des applications et de leurs serveurs. Ces solutions apportent une plus grande finesse de contrôle d'accès, de traçabilité et d'auditabilité. Cela permet donc une meilleure administration et surtout une meilleure réactivité en cas d'attaques par exemple. On peut imposer de choisir des mots de passe forts et de les changer régulièrement, pour que les applications ne soient pas vulnérables aux attaques par « force brute ». Il convient toutefois d'être vigilant sur l'attribution des droits accordés aux utilisateurs, car une fois le compte disposant de nombreux droits compromis, il devient facile de corrompre les applications.

- La transparence fonctionnelle pour les utilisateurs. En effet, nombre d'entreprises offrent à leurs clients des services qu'elles ne font que revendre. C'est le cas des MVNO (Mobile Virtual Network Operator) qui revendent des minutes SFR, Orange ou Bouygues Telecom, comme des grands opérateurs qui proposent des services (téléchargement de sonneries, de logos, etc.). Tout est transparent pour le client grâce à la fédération d'identités.

- Les possibilités de configuration par l'utilisateur lui-même. Le

traitement des données personnelles est facilité. Les portails d'accès sont personnalisés et offrent un confort d'utilisation accru grâce à une meilleure ergonomie. L'utilisateur se sent en confiance dans son espace personnel. Cela permet aux entreprises de présenter une image de marque positive et de la renforcer.

Une solution solide de fédération d'identités doit reposer sur un annuaire centralisant les informations et garantissant une authentification forte

« Chez Idealx, les éléments techniques essentiels d'une solution solide sont un annuaire centralisant les informations ainsi que des certificats, garants de l'authentification forte. L'annuaire peut-être constitué d'une couche présentant de façon unifiée et enrichie des informations obtenues dans des annuaires existants (« meta-annuaire ») ou par des passerelles logicielles capables de puiser des descriptions d'identités (« profils ») maintenues par des logiciels déployés (applicatifs et plate-formes). L'utilisation de certificats rend l'authentification sûre, et confère toute sa valeur à une identité numérique (confiance dématérialisée) d'agent ou de ressource et rend souhaitable de déployer une IGC.

Nat Makarévitch, Idealx

LES PRINCIPAUX ÉLÉMENTS DÉCLENCHEURS D'UN PROJET DE FÉDÉRATION D'IDENTITÉS PAR XAVIER FASOLA UPPERTO, GROUPE DEVOTEAM :

- Répondre à un besoin d'interconnexion des systèmes d'authentification pour permettre le partage des ressources entre les utilisateurs de différentes sociétés,
- Ne pas avoir à gérer les utilisateurs des autres entreprises,
- Mettre en place un système d'authentification plus ergonomique pour les utilisateurs.

La mise en place de ce type de projet va donner aux entreprises :

- Une meilleure sécurité : pas de diffusion du mot de passe à l'extérieur,
- Une meilleure ergonomie pour les utilisateurs avec le SSO et la propagation des attributs,
- Une mise en place des statistiques de connexions,
- Une meilleure gestion des droits d'accès.
- Et leur éviter de dupliquer le référentiel utilisateurs des prestataires.,

FÉDÉRATION D'IDENTITÉS : TOUTES LES ENTITÉS PRÉSENTES SUR LE WEB SONT CONCERNÉES PAR ANNE LUPFER – HSC.

Toutes les entités présentes sur le Web ont potentiellement un besoin de fédération d'identités à partir du moment où elles échangent des informations avec des partenaires ou communiquent avec des sites bancaires. La fédération d'identités est toutefois incontournable pour certaines organisations. C'est le cas par exemple des universités dont le besoin est induit par leur structure. En effet, un étudiant d'une Université pourra accéder aux ressources d'une autre (applications, ressources documentaires...) de manière transparente.

Un autre exemple concret d'application est le portail Internet du gouvernement "mon.service-public.fr" qui permet aux citoyens de réaliser de nombreuses démarches administratives en ligne. Après une identification unique, l'utilisateur se déplace donc virtuellement d'un guichet à un autre et non plus physiquement. Ce portail fédère l'ensemble des sites du gouvernement qui sont indépendants et utilisent leur propre référentiel.

Les opérateurs mobiles ont un réel besoin de fédération d'identités souvent couplé avec des solutions d'authentification unique afin de souscrire à des services sans abonnement tels que l'achat de logos ou de sonneries.

Les sites dit de "programme de fidélité sur Internet" dont le principe est pour l'utilisateur de cumuler des points de fidélité en achetant chez différents partenaires des produits sont un autre exemple d'application de la fédération d'identités. Chaque achat rapporte des points qui sont crédités sur le compte de l'utilisateur pour lui proposer ensuite divers avantages. L'utilisateur peut à partir du portail du programme de fidélité se rendre sur le site partenaire, faire ses achats et avoir son compte crédité en toute transparence.

Xavier Fasola, Upperto Groupe Devoteam

Le SSO et l'IA&M sont, respectivement, des effets et des moyens de la fédération. L'IA&M renforce des aspects de l'authentification sans lesquels l'intérêt même de gérer des identités diminue. La meilleure approche consiste d'abord à construire un socle de confiance fiable et central, puis à décliner progressivement les services. À ce titre, la carte à puce offre un vecteur acceptable car simple, peu coûteux, efficace et de plus en plus répandu et bien géré par les chaînes logicielles adéquates, » expose Nat Makarévitch.

« Effectivement, cette base est un élément particulièrement sensible de la solution. Il convient d'en assurer une sécurité optimale en trois phases : sécuriser la machine, sécuriser les données, sécuriser l'accès. Le SSO permet de regrouper toutes les demandes d'authentification en une procédure unique. En d'autres termes, appliqué dans le cas de la fédération d'identités, le SSO web permet de gérer les accès. Il est cependant nécessaire d'être particulièrement vigilant sur le transit des informations d'authentification sur le réseau (chiffrement du flux) et la sensibilité des applications. Dans le cas d'applications sensibles, le SSO permet d'évoluer vers une solution d'authentification OTP (One Time Password), plutôt qu'à un mot de passe, » complète Anne Lupfer. Ainsi, HSC recommande de créer des architectures faciles à administrer avec cloisonnement des services selon leur sensibilité. Le projet de fédération des identités ne doit pas impacter l'architecture réseau, mais s'y intégrer.

Techniquement, pour Xavier Fasola, une solution de fédération des identités permet à une application d'interagir avec le système d'authentification d'un partenaire : c'est pour cela que l'on parle de relation de confiance. En effet, l'application que l'on nomme « fournisseur de services » va déléguer tout le processus d'authentification d'un utilisateur à l'entreprise à laquelle il appartient, c'est le « fournisseur d'identités ». L'avantage de cette solution est donc que le fournisseur de services garde la gestion des droits d'accès (pour cela il va utiliser des attributs de l'utilisateur fournit par le fournisseur de services) sans pour autant gérer l'utilisateur directement (notam-

RAPPEL DES PRINCIPAUX ÉLÉMENTS TECHNIQUES COMPOSANT UNE SOLUTION DE FÉDÉRATION D'IDENTITÉS PAR XAVIER FASOLA UPPERTO, GROUPE DEVOTEAM

- Annuaire fournisseurs d'identités : c'est l'annuaire fédérateur (il regroupe l'ensemble des utilisateurs de la société, il peut être réalisé grâce aux outils de gestions d'utilisateurs comme le méta annuaire) qui va contenir les utilisateurs et leurs attributs permettant de répondre aux requêtes des fournisseurs de services,
- Fournisseur de services : applications d'un organisme qui, pour des besoins d'authentification, va faire appel à un fournisseur d'identités. Il utilisera des attributs prédéfinis pour autoriser les connexions des utilisateurs. Il convient donc de définir les attributs qui doivent lui être envoyés pour l'authentification.
- SSO : le SSO va permettre de sécuriser les connexions de l'utilisateur. En effet, l'utilisateur ne possède plus qu'un identifiant avec un mot de passe et en se connectant une fois, il accède à l'ensemble de ces applications. Ce type de service est souvent mis en place en dernier (certains logiciels d'identités permettant la synchronisation du mot de passe).
- Certificats : la relation de confiance entre les différents systèmes s'appuie sur des certificats.

ment dans la gestion du mot de passe des utilisateurs : initialisation, perte, …). Bien sûr, dans ce type de solution, un « fournisseur de services » peut être utilisé par des utilisateurs de différents « fournisseurs d'identités » et les utilisateurs d'un « fournisseur d'identités » peuvent accéder à différents « fournisseurs de services ». Ainsi, une solution de fédération va plus loin qu'un simple projet SSO ou qu'un projet IA&M, car il regroupe les deux précédents projets dans un projet global.

En effet, un projet de fédération d'identités permet d'étendre le périmètre du SSO au-delà d'une entreprise. « Je dirais que c'est même la base d'une solution de

PRINCIPES DE FONCTIONNEMENT DES SOLUTIONS DE FÉDÉRATION D'IDENTITÉS PAR ANNE LUPFER HSC

Les solutions de fédération d'identités font transiter les informations d'identification sur le réseau. Le fonctionnement de ces solutions est très complexe du fait de la différence des applications et des protocoles utilisés. Les solutions libres telles que Liberty Alliance et Shibboleth ont un fonctionnement similaire qui consiste à définir :

- Un fournisseur de services qui interagit avec les autres services. Pour Liberty Alliance, un fournisseur de services peut être n'importe quelle organisation offrant des services sur l'Internet. En fonction des solutions, le protocole de communication diffère. Il convient d'être vigilant concernant la confiance accordée au fournisseur de services, car l'authentification et la propagation des informations sont réalisées par ce dernier. De fait, le fournisseur de services doit s'assurer de la disponibilité de ses services, du niveau de sécurité du système d'authentification et des serveurs.

- Un fournisseur d'identités qui gère les informations d'identité et qui transmet les informations d'authentification au service d'authentification, ou au service de single sign on.
- Un cercle de confiance réunissant les fournisseurs de services et les fournisseurs d'identités en réseau ayant des accords opérationnels afin de permettre notamment les transactions commerciales. Pour réutiliser les termes de la Liberty Alliance, le cercle de confiance est une fédération de services web qui ont des relations entre eux.
- Lors du premier accès au service, l'utilisateur est redirigé vers un service de découverte des identités qui facilite l'enregistrement et rattache l'utilisateur à sa provenance. L'utilisateur possède alors une clé de fédération d'identités unique.
- L'authentification est gérée par l'application. Il est ainsi plus facile d'ajouter une brique de Single Sign On web sur la solution de fédération d'identités.
- Nombreuses solutions se basent sur SAML, structuré sur le langage XML et développé par OASIS. SAML2.0 est vu comme un standard en terme de fédération d'identités pour Liberty Alliance et contribue à l'échange d'informations entre les différents systèmes.

Les spécifications de la Liberty Alliance en termes de connexions permettent plusieurs moyens d'authentification :

- Authentification par carte à puce contenant un certificat de sécurité (au format X.509v3).
- Authentification par certificat de sécurité (au format X.509v3) stocké dans le navigateur;
- Authentification par identifiant et mot de passe (système moins sécurisé mais plus souple).

http://www.projectliberty.org/liberty/specifications__1 pour le fonctionnement détaillé de la solution Liberty Alliance)

gestion des identifiants et des accès. C'est le socle qui permet et facilite la mise en place des solutions de gestion d'identités. C'est la première brique d'un projet de gestion d'identités et d'accès. Cette phase du projet permet de mettre en place des éléments essentiels tels que la politique de sécurité à appliquer, les niveaux de sensibilité des applications, la matrice d'habilitations..., » conclut Anne Lupfer.

La liberty Alliance et Shibboleth sont les véritables leaders de la fédération des identités

Pour Anne Lupfer, les principaux leaders dans le monde du libre sont Liberty Alliance et Shibboleth :

- Liberty Alliance est un consortium d'entreprises, fondé en 2001, qui a produit plusieurs spécifications sur la gestion d'identités et dont l'objectif premier était d'établir un standard libre de fédération d'identités. Aujourd'hui, au vu des besoins qui se font ressentir, Liberty Alliance a élargi son spectre à la gestion des identités et des accès. **(Voir** http://www.projectliberty.org/**)**
- Shibboleth est une solution orientée vers les universités, et reprise par plusieurs éditeurs. Son objectif premier est de faciliter le partage des ressources en ligne entre les différents établissements. **(Voir** http://federation.cru.fr/**)**

On peut également citer FederID qui est une solution libre de fédération et de gestion des

identités. Cette solution intègre InterLDAP, OpenLDAP et LASSO (Liberty Alliance SSO) pour l'authentification unique.

Plusieurs éditeurs proposent des solutions de gestion des identités interopérables avec SAML2.0, et conformes à la spécification Liberty ID-FF, dont voici une liste non exhaustive :

- IBM Tivoli Federated Identity Manager
- RSA Security Federated Identity Manager
- NTT I-dLive
- ...

Liberty Alliances tient à jour une liste des produits compatibles qui est disponible à l'adresse http://projectliberty.org/liberty/liberty_interoperable/interoperable_products.

Microsoft a abandonné sa solution Passport pour la solution InfoCard qui est plus une solution de gestion d'identités que de fédération d'identités.

Effectivement, confirme Nat Makarévitch, dans le monde Open-Source, les leaders sont bien Shibboleth et Liberty Alliance. Mais Higgins trust framework (Eclipse) progresse, et des approches plus innovantes, par exemple Yadis, apportent divers concepts et réalisations potentiellement pertinents. Shibboleth est opérationnel et déployé. Sa modularité simplifie les efforts nécessaires, pour les fournisseurs de solutions comme pour les utilisateurs. Liberty Alliance est aujourd'hui encore neuf et ses implémentations restent rares. La principale limite de la fédération tient au manque d'applications directement compatibles et, l'habituel « catch 22 » jouant, cela ne contraint guère les éditeurs à respecter les normes sous-jacentes (aujourd'hui, en particulier, SAML 2.0), donc les applications directement compatibles manquent...
Pour Xavier Fasola, CA, Sun, Oracle, HP ont pour avantage de posséder, d'ores et déjà, des outils de gestion d'identités (donc d'un annuaire qui peut faire office de fournisseur d'identités) et n'ont donc que la brique de fédération d'identités à rajouter.

Des risques en terme de sécurité qui reposent sur le navigateur web et sur la confiance

Anne Lupfer considère que les risques de sécurité sont identiques pour toutes les applications. Ici, il convient tout de même d'ajouter que de la sécurité repose sur celle du navigateur qui est le point d'entrée dans le système. Selon Xavier Fasola, la mise en place de ce type de solutions peut effectivement engendrer une faille de sécurité au sein de la société (notamment avec la diffusion d'informations concernant les utilisateurs), c'est pourquoi une étude poussée est nécessaire. Il doit exister une notion forte de confiance entre les partenaires, or ce type de relation n'est pas toujours évident.

Habilité, méthodes, vigilance et communication sont les 4 facteurs de réussite d'un projet

« Des aspects organisationnels et politiques entrent également en jeu dans ce type de projet. Il

Note : Le gouvernement français ayant opté pour une solution basée sur Liberty Alliance et les universités pour une solution basée sur Shibboleth, des efforts de convergence de ces produits sont réalisés afin qu'ils soient parfaitement homogènes pour répondre à un besoin futur.

convient donc d'être très habile et très méthodique, notamment dans la définition de la sensibilité des applications et des droits utilisateurs.
A la différence de certains projets informatiques, dans le cas d'un projet de fédération d'identités, les utilisateurs sont les premiers impactés par une solution de fédération d'identités, car ils sont au cœur de la solution. Il faudra donc être vigilant concernant les changements dans l'utilisation. Il est essentiel de former les utilisateurs et de leur expliquer les bénéfices d'une telle solution. Lorsque le client est directement impacté, il est évident que les équipes marketing doivent être inclues dans la boucle projet. Et surtout, il ne faut penser à gérer les exceptions, » explique Anne Lupfer.

Tout à fait d'accord, reprend Nat Makarévitch, les acteurs doivent saisir que le projet de fédération consiste à délaisser l'ordre dispersé où chaque élément d'identification est peu sûr et relatif (à un applicatif, à un sous-ensemble organisationnel...) afin d'établir des descriptions d'identités correspondant à celles du monde réel, donc à des entités et individus pour lesquels on peut exprimer le degré de confiance investi. L'ordre dispersé est un instantané, souvent trop statique, de la confiance accordée à un agent (« oui, Dumond peut accéder à la comptabilité ») tandis que la fédération offre le moyen de toujours décrire afin d'appliquer systématiquement et partout les règles associées (« telle catégorie d'utilisateurs ne peut plus accéder à la comptabilité »). Il s'agit de gérer en fonction de la confiance, au lieu de la décrire de façon ad hoc. On commencera par déterminer l'utilité d'une identité : les usages, les degrés de confiance, les ressources concernées (à quoi peut prétendre tel niveau de confiance)... L'authentification forte est, en cela, tout à la fois : d'emblée nécessaire et l'apport majeur du projet.

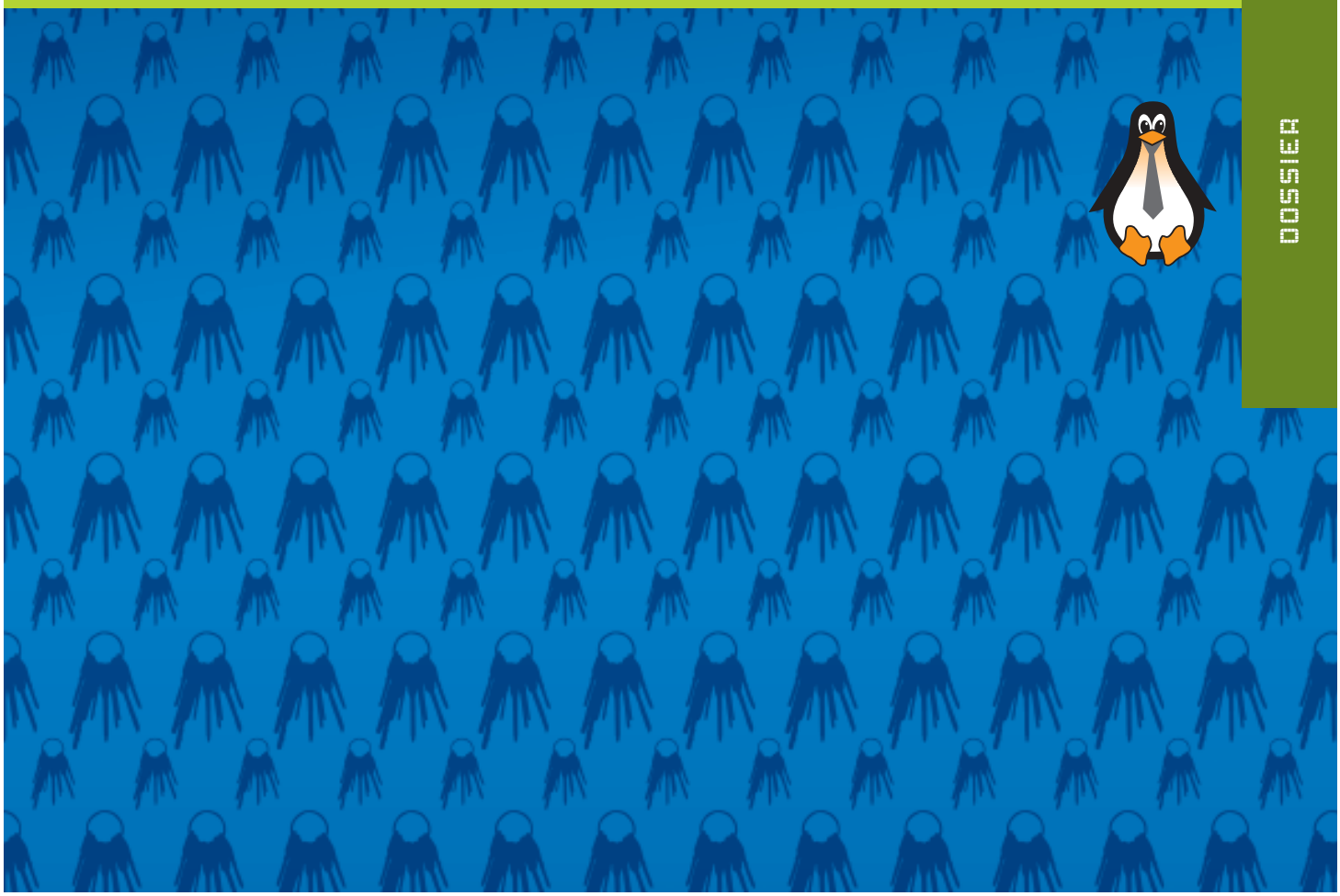
Il faut également désolidariser ce projet de tout aménagement du mode de fonctionnement de l'entreprise. La fédération est un outil, non une nouvelle méthode. Elle facilite en éclairant et mécanisant mais ne contraint pas à adopter de nouvelles conventions, auxquelles elle sera toutefois adaptable.

Un parallèle avec la programmation objet se dessine puisque la fédération oriente la réflexion vers la réalité des éléments en ménageant des possibilités d'amélioration de leur description, plutôt qu'en fournissant des moyens de représentation partielle d'une idée que l'on s'en fait sur le moment. Cela améliore la souplesse, la réutilisation... la rentabilité. Cette prise de conscience nous semble profitable, voire nécessaire, au projet. Je rajouterai qu'il faut une relation de confiance et une bonne communication entre les différents acteurs, conclut Xavier Fasola.
L'évolution naturelle de tout projet est la migration progressive vers une gestion des accès centralisée, voire automatisée. Déployer le SSO devient alors naturel, explique Anne Lupfer. Elle pourra aussi conduire à une intégration des applications hors du contexte web, estime Xavier Fasola.

Un RoI relativement facile à mesurer

Plusieurs éléments entrent dans le calcul du retour d'investissement, plus ou moins facile à évaluer, que Xavier Fasola et Anne Lupfer résument :

- L'ouverture de services partenaires par exemple peut être facilement évaluée,
- La diminution des coûts de Help Desk et d'administration pourra être évaluée en termes de jour/homme et confirmée sur le long terme,
- D'une manière générale les utilisateurs des services fédérés devraient voir leur productivité s'accroître, l'attribution de ressource étant plus rapide.
- Le gestionnaire de ressources n'a pas de système d'authentification à mettre en place,
- Le fournisseur d'identités peut s'appuyer sur ses systèmes internes,



- L'image de marque est un élément plus complexe à évaluer mais les équipes marketing devraient être en mesure de le faire.

Un projet de DSI, mais où le RSSI joue un rôle de facilitateur et contrôle la politique de sécurité

Nos trois experts considèrent que ce type de projet est généralement porté par la DSI, même si pour Anne Lupfer, il est possible que le projet soit initié par le marketing qui souhaite accroître la souplesse d'utilisation de son portail. Dans ce cas, le marketing sera accompagné par des équipes informatiques qui pourront apporter les solutions et les réponses aux problèmes posés. C'est un cas classique de coopération entre la maîtrise d'ouvrage et la maîtrise d'œuvre. Dans tous les cas, le RSSI joue un rôle important. Pour Xavier Fasola, il devra veiller à ce que les autorisations d'accès soient pertinentes et contrôlées. De même, si il y a un échange d'informations concernant les utilisateurs vers une société extérieure, il vérifiera que ces informations ne sont pas confidentielles. Si elles le sont, il contrôlera leur bonne utilisation et leur exploitation dans le strict cadre du projet. Il validera aussi que l'ensemble du système soit bien sécurisé et, enfin, prendra en compte les outils de reporting (remontées d'alertes, systèmes de logs, …). En amont et durant tout le projet, il éclairera les réflexions menant à décrire la confiance (qui la délivre, quand et comment...), à s'assurer que la réalisation respecte la politique de sécurité, puis à améliorer les tableaux de bord. C'est pour cela qu'il doit connaître les processus et décideurs en place, complète Nat Makarévitch. Il pourra même, dans certains cas, être l'initiateur du projet, mais ce n'est pas une règle absolue, conclut Anne Lupfer : « dans tous les cas, il devrait avoir un rôle d'accompagnement et de surveillance. Il doit aider les équipes à réaliser le projet notamment concernant les points d'organisation (matrice des habilitations, classement de la sensibilité des applications), et aider dans le choix des solutions techniques (chiffrement, authentification...). Il interviendra de manière transverse sur le projet et s'assurera que les principes fondamentaux de la sécurité sont appliqués (confidentialité, intégrité, authenticité et non répudiation des données). Les projets ayant souvent des impacts sur les clients de l'entreprise, l'avis des équipes marketing ne doit pas être mis à l'écart. »