Architecture technique

Ce document présente les aspects techniques de l'architecture permettant l'identification unique selon les spécifications Liberty [1] ainsi que les spécificités de l'identification par carte à puce.

Sommaire

[1] : http://projectliberty.org

1 Concepts et vocabulaire

Le concept d'**identité réseau** d'une personne physique ou d'une personne morale sur Internet regroupe à la fois :

- Des **attributs** (informations personnelles, préférences, historique des actions passées, etc).
- Les éléments nécessaires à l'**authentification**, c'est à dire garantissant la validité d'une identité avec un niveau de sécurité donné.
- Des **permissions**, c'est à dire les droits d'accès à des informations ou à des services. Ces permissions peuvent dépendre du niveau de sécurité de l'authentification.

Avec le développement d'Internet, cette notion d'identité est aujourd'hui fragmentée, si bien que les usagers doivent, par exemple mémoriser autant d'identifiants et de mots de passe que de services auxquels ils accèdent.

C'est, entre autres, à cette problématique d'identité que le projet Liberty Alliance fournit une réponse appropriée. La phase 1 des spécifications Liberty définit pour cela trois types d'acteurs :

- **Principal** : Personne physique ou morale qui peut acquérir une identité.
- **Fournisseur d'identités** : Crée, et gère l'identité des principaux, et les identifie auprès des fournisseurs de service.
- **Fournisseur de services** : Fournit des services aux principaux une fois qu'ils sont identifiés par un fournisseur d'identités.

Un **cercle de confiance** est une fédération de fournisseurs d'identités et de fournisseurs de services qui se sont mis d'accord pour fédérer l'identité de leurs utilisateurs (principaux).

L'**authentification unique** permet à un principal de s'authentifier sur un fournisseur d'identités, et d'être ensuite automatiquement authentifié sur tous les fournisseurs de service du même cercle de confiance.

On parle donc d'**identité fédérée** car le standard Liberty permet aux principaux de bénéficier de l'authentification unique tout en demeurant potentiellement anonymes pour les fournisseurs de services.

Les fournisseurs de services n'ont aucun moyen de croiser les informations relatives aux principaux, car pour chaque fournisseur de services, le fournisseur d'identités attribue un **pseudonyme** différent au principal.

2 Fonctionnement schématique de l'identification unique

Le flux de données est décrit schématiquement dans la Figure 1.

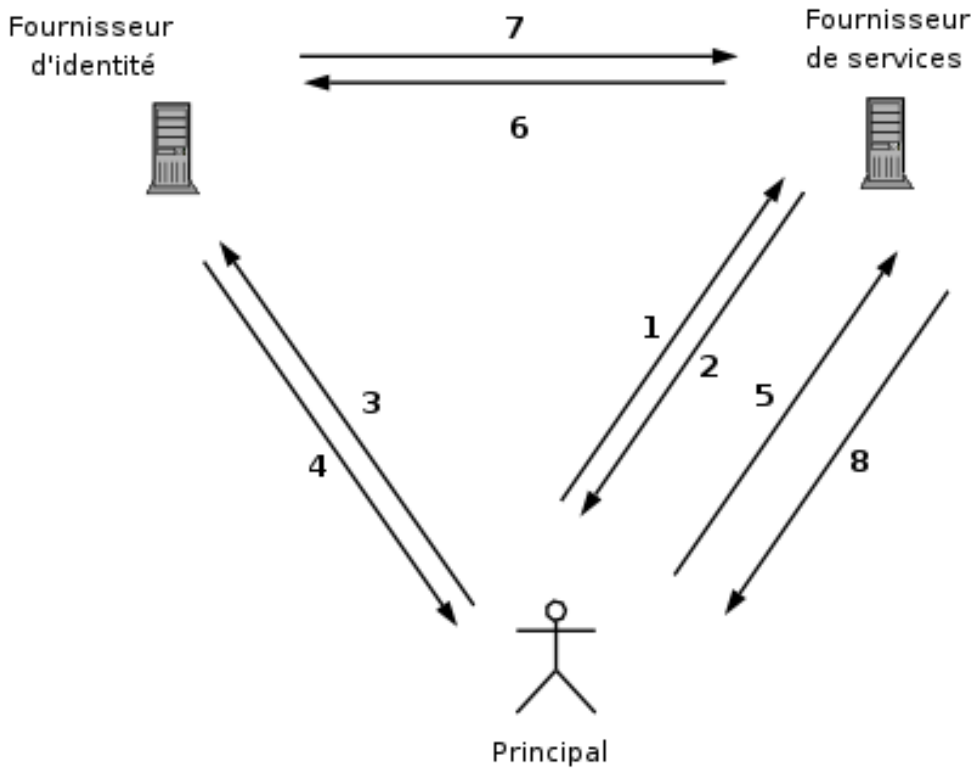

Figure 1: Fonctionnement schématique de l'identification unique.

1. Le principal veut accéder à un service pour lequel il doit s'identifier.
2. Le fournisseur de services redirige le principal sur le fournisseur d'identités.
3. Le principal s'identifie sur le fournisseur d'identités.
4. Le fournisseur d'identités redirige le principal vers le fournisseur de service et lui fournit un « artefact ».
5. Cet artefact est transmis par le principal au fournisseur de services.
6. Le fournisseur de services demande au fournisseur d'identités de valider l'artefact.
7. Le fournisseur d'identités valide l'artefact. Il authentifie ainsi la principal auprès du fournisseur de services.
8. Le fournisseur de services fournit alors au principal le service initialement demandé.

L'opération est transparente pour le principal. Lorsqu'il demande à accéder au service, on lui demande de s'identifier. Il accède ensuite au service.

Il peut ensuite accéder aux services d'autres fournisseurs de services du même cercle de confiance sans avoir besoin de s'identifier à nouveau. Pour cela, le fournisseur d'identités doit pouvoir reconnaître le principal. Le moyen utilisé dépend de la méthode d'identification utilisée :

- Le fournisseur d'identités peut envoyer un cookie au principal.
- Dans le cas d'une identification par certificat stocké dans le navigateur, le certificat est renvoyé au fournisseur d'identités à chaque connexion, et remplace donc avantageusement le cookie.
- De même, si le certificat est stocké sur une carte à puce, il est aussi renvoyé au fournisseur d'identités à chaque connexion tant que la carte reste dans le lecteur.

3 Identification par carte à puce

Une identification par certificat stocké sur une carte à puce permet d'éliminer les problèmes que pose le stockage du certificat du principal dans le navigateur (il faut alors restreindre l'accès à l'ordinateur concerné pour garantir l'identité du principal).

L'usage de cartes à puce respectant la norme PKCS#15 [2] permet de stocker le certificat (la clé publique) dans la carte tout en garantissant que la clé privée ne puisse pas sortir de la carte.

Ce certificat est un identifiant unique. Il ne doit donc être communiqué qu'au fournisseur d'identités. S'il était communiqué aux fournisseurs de services, ceux-ci pourraient croiser les informations personnelles des principaux dont ils disposent.

Aucune information personnelle en dehors du certificat n'est stockée sur la carte, à l'exception du nom et du prénom de l'usager car :

- cela lui permet de signer ses courriers électroniques.
- cela lui permet de reconnaître le certificat au cas où le navigateur lui en proposerait plusieurs.

Nom et prénom ne sont pas utilisés pour l'identification, et ne sont pas stockés sur le fournisseur d'identités.

Dans le cadre d'une identification par carte à puce multi-services avec une architecture différente qui impliquerait une identification directement auprès des fournisseurs de services, le stockage d'informations personnelles sur la carte n'est pas une bonne solution :

- L'usage de la carte nécessite un code PIN, et le seul moyen de limiter l'envoi des informations qu'elle contient (à l'exception de la clé privée, qui elle ne peut pas être extraite) est d'utiliser plusieurs codes PIN différents, ce qui n'est pas envisageable pour l'usager.
- Les fournisseurs de services conservent de toute manière une partie des informations personnelles de leurs usagers.

[2] : http://www.rsasecurity.com/rsalabs/pkcs/

4 Autorités de certification

Les certificats des fournisseurs de services ne sont pas signés par une autorité de certification rattachée (directement ou indirectement) à l'autorité de certification racine des certificats stockés sur les cartes.

Cette disposition permet de s'assurer que les serveurs des fournisseurs de service ne pourront pas avoir accès au certificat des citoyens (et donc à la clé unique les identifiant).