

Présentation OpenId

Par KENFACK Patrick
MIF30

19 Mai 2009

Sommaire

- I. Introduction
- II. Qu'est ce qu'un OpenId?
- III. Acteurs
- IV. Principe
- V. Implémentation
- VI. Sécurité
- VII. conclusion

Introduction

- Vue le nombre croissant de sites web nous demandant de nous identifier, la maîtrise de l'identité numérique est devenue un enjeu important.
- Cette maîtrise est devenue possible grâce aux systèmes d'authentification comme OpenID qui facilite l'authentification unique et le partage des attributs.
- Ces systèmes d'authentification nous permettent d'obtenir rapidement auprès des fournisseurs d'identité ou OP une identité numérique, de changer ou de révoquer cette identité tout aussi rapidement.

Introduction (suite & fin)

- Grace à cette identité on pourra s'authentifier sur n'importe quel site web supportant cette technologie.
- C'est dans ce contexte qu'il est important de s'arrêter sur l'aspect sécurité qu'il a autour de cette technologie OpenId, en dégagant les différents protocoles de cryptages qui entrent en jeu dans ce mécanisme d'authentification unique.

Qu'est ce qu'un OpenId?

- système d'authentification décentralisé qui permet l'authentification unique, ainsi que le partage d'attributs. Il permet à un utilisateur de s'authentifier auprès de plusieurs sites (devant supporter la technologie) sans avoir à retenir un identifiant pour chacun d'eux mais en utilisant à chaque fois un unique identifiant OpenID.
- Le modèle OpenID se base sur des liens de confiance préalablement établis entre les fournisseurs de services (sites web utilisant OpenID par exemple) et les fournisseurs d'identité (OpenID providers). Il permet aussi d'éviter de renseigner à chaque fois un nouveau formulaire en réutilisant les informations déjà disponibles.

Acteurs

On distingue :

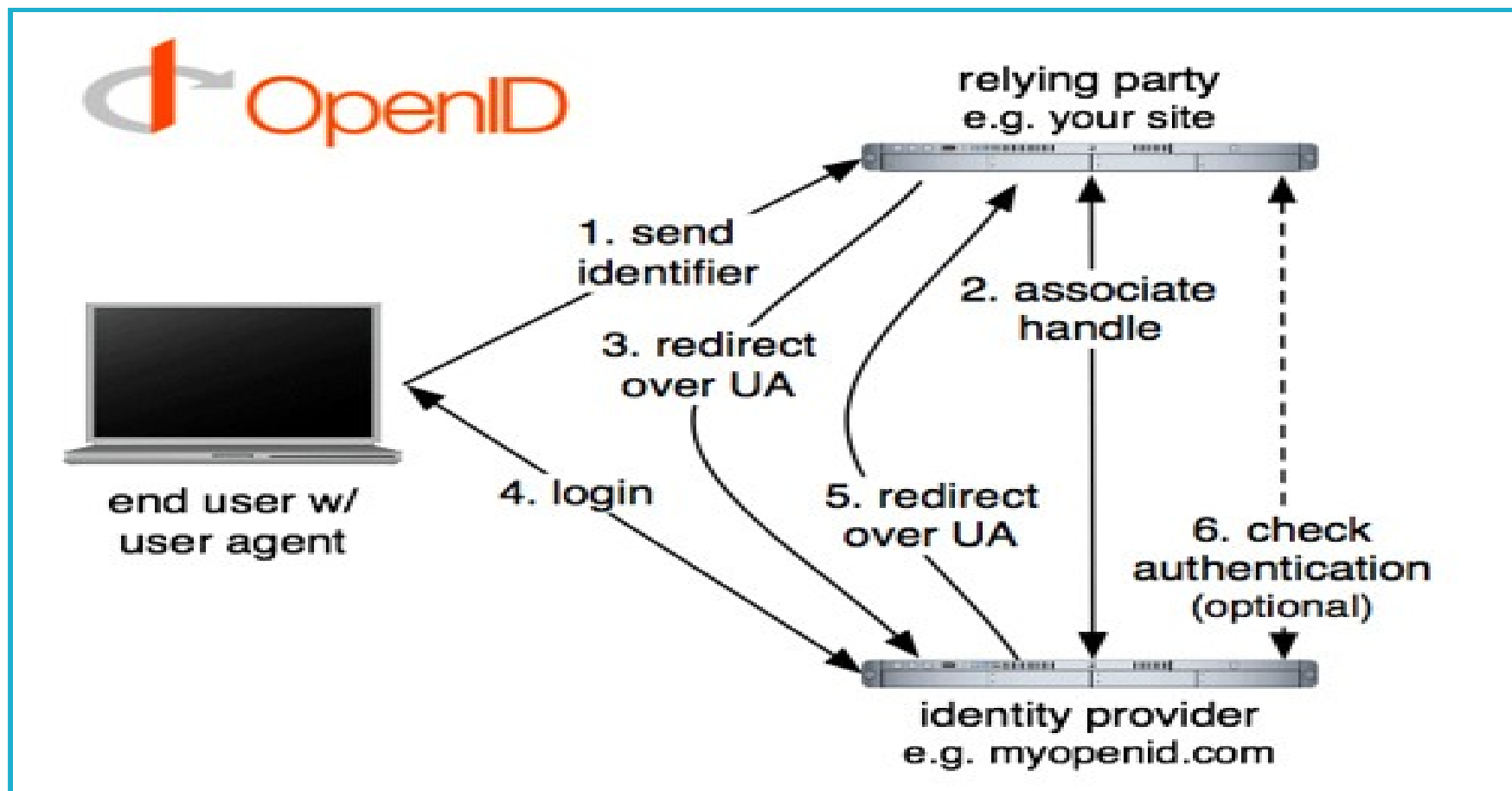
- l'utilisateur
- le consommateur (en abrégé RP, pour Relaying Party) : il désire avoir une preuve de l'identité de l'utilisateur. C'est un site web, un service web
- le fournisseur d'identité (OpenID Provider, ou OP, ou IdP, ou IP ou juste Provider) : c'est un serveur d'authentification OpenID qui est contacté par le consommateur pour obtenir Une preuve de l'identité de l'utilisateur ;
- le client, par exemple le navigateur internet de l'utilisateur.

Principes

Lors d'une authentification unique, et donc lors d'une authentification via OpenID, on trouve trois entités:

- l'utilisateur qui souhaite s'authentifier (en fait, le navigateur utilisé, EU ou End User)
- le site sur lequel l'utilisateur souhaite s'authentifier (RP ou Relaying Party)
- le serveur d'authentification (OP ou OpenID Provider, ici le serveur OpenID).

Principes (suite & fin)



Implémentation

❖ Point de vue utilisateur:

- il faut choisir un fournisseur de service OpenID et s'inscrire auprès de ce fournisseur afin d'obtenir une identité numérique OpenID, matérialisée par une URL

<http://www.OpenIDfrance.fr/sirpatrick>).

- **redirection vers une URL de votre choix?**

Vous avez un site internet ou un blog, vous souhaitez l'utiliser comme identifiant OPENID ?

C'est très simple, il vous suffit de recopier le code ci-dessous entre les balises <head> <\head> :

```
<html>
<head>
<link rel="OpenID.server" href="http://www.OpenIDfrance.fr/index.php" />
< link rel="OpenID.delegate" href="http://www.OpenIDfrance.fr/sirpatrick" />
</head>
<body>
</body>
</html>
```

Implémentation (suite)

- ▶ Mise en place de votre propre serveur d'identité

```
<html>
<head>
<link rel="OpenID.server" href="http://nom_serveur/MyID.config.php" />
<link rel="OpenID.delegate" href=http://nom\_serveur/MyID.config.php/>
</head>
<body>
</body>
</html>
```

Implémentation (suite & fin)

❖ Point de vue Administrateur

► Drupal:

C'est un CMS, une application Web de gestion de contenu.

➤ Mise en place de son propre site web

`common.php` : ce fichier contient les définitions de fonctions globales nécessaires au dialogue avec le serveur OpenID.

`index.php` : il s'agit du fichier principal, qui sert à saisir l'URL OpenID et à gérer l'affichage des informations par inclusion dans les autres fichiers.

`authentification.php` : ce fichier contient la première partie du processus d'authentification

- création d'un consommateur (qui va servir à dialoguer avec le serveur) ;
- construction de la requête qui sera envoyée au serveur OpenID sous forme d'URL
- redirection vers le serveur OpenID pour que l'utilisateur s'authentifie auprès de lui.

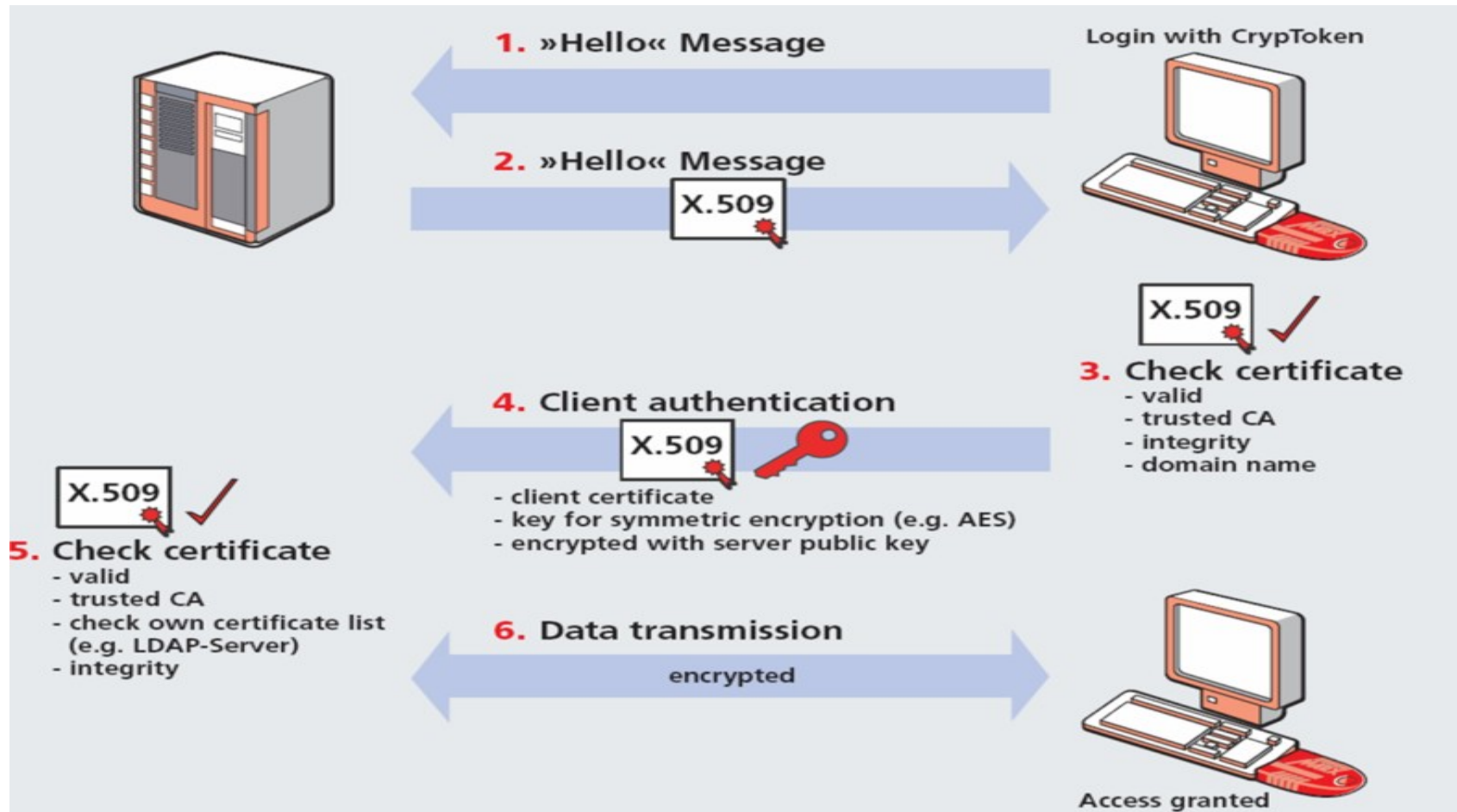
`recuperation.php` : ce fichier contient la dernière partie du processus d'authentification :

- création d'un consommateur (qui va servir à dialoguer avec le serveur) ;
- récupération de la réponse envoyée par le serveur OpenID
- analyse de la réponse ;
- affichage des données fournies

Sécurité

- ▶ Cryptographie : par des opérations mathématiques, on peut prouver que tel message a été signé par le possesseur d'une clé numérique. A la base de techniques comme TLS, X.509, PGP,
- ▶ X.509 : norme de certificats cryptographiques. C'est ce qu'utilise votre navigateur Web pour afficher le petit cadenas.
- ▶ TLS (ex-SSL) : le protocole d'échange de données chiffrées entre votre navigateur et le site Web.

Aperçu du fonctionnement de l'authentification client SSL



Sécurité (suite)

Risque pour la vie privée : l'OP est informé de nos visites. Solutions : bien choisir son OP, être son propre OP, avoir plusieurs identités.

➤ Risque de hameçonnage : le RP nous redirige vers l'OP. Un méchant RP peut donc nous rediriger vers un vilain OP qui gardera notre mot de passe.

Solutions : mécanismes anti-hameçonnage classiques (secret partagé), ne pas utiliser de choses réutilisables comme les mots de passe, . . .

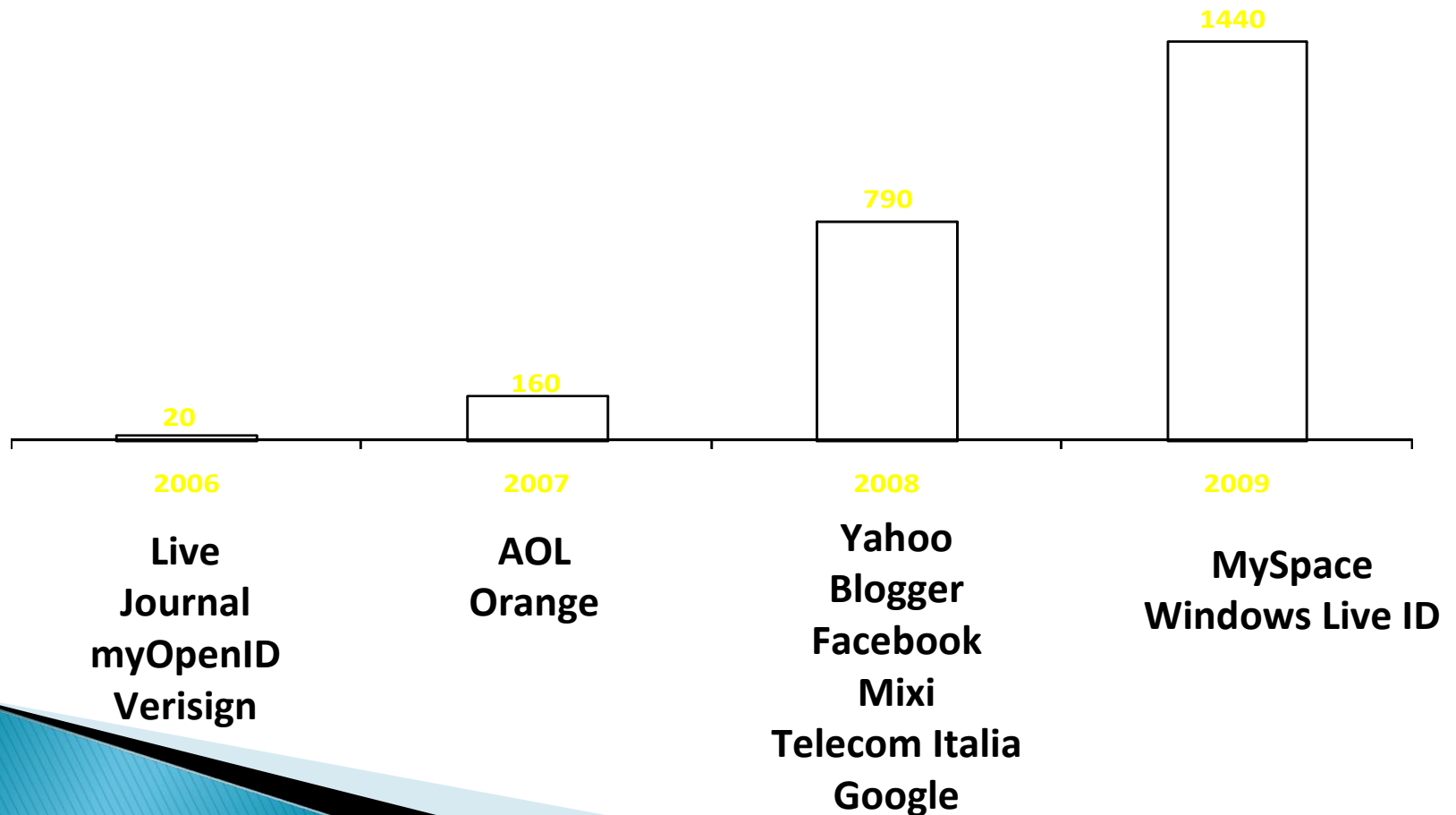
➤ Risque liée aux certificats des serveurs de TLS (Transport Layer Security) ex: les clé faibles

Sécurité (suite & fin)

- ▶ De telles clés sont bien sûr à bannir mais leur présence ne rend pas DES moins robuste en théorie. DES a un espace de clés qui contient 2^{56} possibilités. La probabilité de trouver une clé faible avec un tirage aléatoire parfait est de $4/2^{56}$.

Conclusion

OpenID est aujourd'hui un standard stable pour l'identification numérique dans un système décentralisé, largement mise en œuvre dans beaucoup de logiciels (ce qui est un tribut à sa simplicité), mais encore relativement peu déployé.



Plus de 40000 sites web Accepte l'authentification par Openid

San Francisco Chronicle



Citysearch



CNN

MAPQUEST.



JAL
JAPAN AIRLINES

TechCrunch

stackoverflow

uservoice
What do users really want?

plaxo

Google
Friend Connect BETA

radio POP
Prototype from BBC Radio Labs

GET
SATISFACTION

SB★NATION

Dailymotion

MoveOn.ORG
Democracy In Action.

Joost

SOURCEFORCE®

Microsoft
HealthVault
Microsoft

Oxfam
International



OKLAHOMA
STATE
UNIVERSITY

sulit.com.ph
Free Ads ba? Sulit na!

ITHACA

StumbleAudio

Questions

Merci....