OpenID

Stéphane Bortzmeyer
AFNIC
bortzmeyer@nic.fr

Novembre 2007

Identité

La gestion des identités numériques est un sujet chaud aujourd'hui

Mais que recouvre t-il exactement ?

Annonces diverses, Microsoft Cardspace, OpenID chez Orange, inquiétudes pour la vie privée, problème de tous les mots de passe à gérer, etc.

Ce que fournit un service d'identité

Ce que fournit un service d'identité

1. Attribuer un identificateur à chaque entité, par exemple `bortzmeyer@gmail.com` ou bien « Numéro 6 » (il existe de nombreuses syntaxes), et s'assurer de son unicité, voire de sa stabilité,

Ce que fournit un service d'identité

1. Attribuer un identificateur à chaque entité,
2. Authentifier une entité, par exemple par un mot de passe ou la présentation d'un passeport ou bien par une signature PGP,

Ce que fournit un service d'identité

1. Attribuer un identificateur à chaque entité,
2. Authentifier une entité,
3. Servir des données sur cette entité, par exemple son âge, son nom à afficher, sa langue maternelle, son nombre d'articles publiés sur Slashdot, ...

Ce que fournit un service d'identité

1. Attribuer un identificateur à chaque entité,
2. Authentifier une entité,
3. Servir des données sur cette entité,
4. Donner accès à des données externes, ce qui est très proche du point précédent, à ceci près que les données sont gérées par un autre système,

Ce que fournit un service d'identité

1. Attribuer un identificateur à chaque entité,
2. Authentifier une entité,
3. Servir des données sur cette entité,
4. Donner accès à des données externes,
5. Donner accès à des autorisations ,par exemple `smith` a le droit de committer mais uniquement dans `/usr/ports` ou bien SB126-FRNIC a le droit de modifier le domaine `bortzmeyer.fr`.

Ce que fournit un service d'identité

1. Attribuer un identificateur à chaque entité,
2. Authentifier une entité,
3. Servir des données sur cette entité,
4. Donner accès à des données externes,
5. Donner accès à des autorisations

L'authentification ne garantit rien

Il faut bien distinguer authentification et autorisation

Philosophie et informatique

L'identité n'est pas une caractéristique intrinsèque d'une entité.

Une entité peut se présenter sous plusieurs identités (et c'est souvent recommandé, notamment pour préserver la vie privée).

Cameron et l'identité

Kim Cameron présente l'identité comme une liste d'**assertions** :

- Stéphane Bortzmeyer est orateur à JRES,
- Cette personne a plus de dix-huit ans,
- "CerealesKiller" est un contributeur Wikipédia,

Les sept lois de l'identité

Élaborées par Cameron :

Les sept lois de l'identité

Élaborées par Cameron :

1. Contrôle par l'utilisateur,

Les sept lois de l'identité

Élaborées par Cameron :

1. Contrôle par l'utilisateur,
2. Divulgation minimale, par exemple, on ne devrait pas donner son nom pour boire dans un bar, seulement prouver qu'on est majeur,

Les sept lois de l'identité

Élaborées par Cameron :

1. Contrôle par l'utilisateur,
2. Divulgation minimale,
3. Divulgation uniquement à ceux qui en ont besoin,

Les sept lois de l'identité

1. Contrôle par l'utilisateur,
2. Divulgation minimale,
3. Divulgation uniquement à ceux qui en ont besoin,
4. Identité dirigée,

Les sept lois de l'identité

1. Contrôle par l'utilisateur,
2. Divulgation minimale,
3. Divulgation uniquement à ceux qui en ont besoin,
4. Identité dirigée,
5. Les systèmes d'identité doivent être multiples. Pas de fournisseur d'identité unique !

Les sept lois de l'identité

1. Contrôle par l'utilisateur,
2. Divulgation minimale,
3. Divulgation uniquement à ceux qui en ont besoin,
4. Identité dirigée,
5. Les systèmes d'identité doivent être multiples.
6. Prise en compte des facteurs humains, au contraire de systèmes comme X509,

Les sept lois de l'identité

1. Contrôle par l'utilisateur,
2. Divulgation minimale,
3. Divulgation uniquement à ceux qui en ont besoin,
4. Identité dirigée,
5. Les systèmes d'identité doivent être multiples.
6. Prise en compte des facteurs humains, ,
7. Apparence unique, unifier les différentes identités pour permettre à l'utilisateur une gestion simplifiée.

OpenID

Comment OpenID traite t-il mes cinq services ?

OpenID

Comment OpenID traite t-il mes cinq services ?

1. Attribuer un identificateur à chaque entité, c'est un URL, par exemple `http://www.bortzmeyer.org/`,

OpenID

Comment OpenID traite t-il mes cinq services ?

1. Attribuer un identificateur à chaque entité, c'est un URL,
2. Authentifier une entité, chaque fournisseur OpenID choisit, typiquement un mot de passe avec le fournisseur,

OpenID

Comment OpenID traite t-il mes cinq services ?

1. Attribuer un identificateur à chaque entité, c'est un URL,
2. Authentifier une entité, chaque fournisseur OpenID choisit,
3. Servir des données sur cette entité, ce n'est pas dans le protocole de base, c'est géré par des extensions.

OpenID

Comment OpenID traite t-il mes cinq services ?

1. Attribuer un identificateur à chaque entité, c'est un URL,
2. Authentifier une entité, chaque fournisseur OpenID choisit,
3. Servir des données sur cette entité, ce n'est pas dans le protocole de base.

Le reste est hors-sujet (mais il existe des réflexions). L'identité OpenID peut servir d'entrée dans un registre d'autorisations.

Un scénario avec OpenID

Soit Loïc, un blogueur.

Un scénario avec OpenID

Soit Loïc, un blogueur.

Loïc aime bien laisser des commentaires sur des tas de blogs. Mais les blogs sont envahis de spam ou simplement de c. . . ies.

Un scénario avec OpenID

Soit Loïc, un blogueur.

Loïc aime bien laisser des commentaires sur des tas de blogs. Mais les blogs sont envahis de spam ou simplement de c. . . ies.

Chaque plate-forme de blog crée donc des **identités**. La plate-forme **authentifie** ces identités et note des **réputations**.

Un scénario avec OpenID

Loïc aime bien laisser des commentaires sur des tas de blogs. Mais les blogs sont envahis de spam ou simplement de c. . . ies.

Chaque plate-forme de blog crée donc des **identités**. La plate-forme **authentifie** ces identités et note des **réputations**.

Mais les plate-formes ne communiquent pas ! Non seulement il faut retenir plusieurs mot de passe mais, surtout, on ne pas utiliser sa réputation d'une plate-forme sur une autre. On repart de zéro.

Loïc passe à OpenID

Il ouvre un compte chez MyOpenID, son identité est `http://loic.myopenid.com/`. À chaque plate-forme de blog qui accepte OpenID, il tape cet identificateur.

Il est redirigé vers MyOpenID, il rentre son mot de passe et hop.

Loïc passe à OpenID

Il ouvre un compte chez MyOpenID, son identité est `http://loic.myopenid.com/`. À chaque plate-forme de blog qui accepte OpenID, il tape cet identificateur.

Il est redirigé vers MyOpenID, il rentre son mot de passe et hop.

Loïc est heureux mais il a tort.

Loïc passe à OpenID

Il ouvre un compte chez MyOpenID, son identité est `http://loic.myopenid.com/`. À chaque plate-forme de blog qui accepte OpenID, il tape cet identificateur.

Il est redirigé vers MyOpenID, il rentre son mot de passe et hop.

Loïc est heureux mais il a tort.

Car son identité dépend du fournisseur (l'OP pour *OpenID provider*).

Loïc comprend à quoi sert le DNS

Il achète un nom de domaine pas cher dans un domaine sympa. Il est désormais `http://www.loic.fr/`.

Il met dans la page Web à laquelle on accède avec cet URL :

```
<link rel="openid.server"
href="http://www.myopenid.com/server/"/>
<link rel="openid.delegate"
href="http://loic.myopenid.com/"/>
```

et il a désormais une identité à lui.

Mais comment ça a marché ?

OpenID marche sur HTTP.

Le site Web qui veut authentifier est le RP (*Relying Party*). Le fournisseur d'identité est l'OP (*OpenID Provider*).

Mais comment ça a marché ?

OpenID marche sur HTTP.

Le site Web qui veut authentifier est le RP (*Relying Party*). Le fournisseur d'identité est l'OP (*OpenID Provider*).

1. Le RP regarde le site Web de l'utilisateur et trouve l'OP,

Mais comment ça a marché ?

OpenID marche sur HTTP.

Le site Web qui veut authentifier est le RP (*Relying Party*). Le fournisseur d'identité est l'OP (*OpenID Provider*).

1. Le RP regarde le site Web de l'utilisateur et trouve l'OP,
2. Le RP contacte l'OP, lui demandant d'authentifier l'utilisateur,

Mais comment ça a marché ?

Le site Web qui veut authentifier est le RP (*Relying Party*). Le fournisseur d'identité est l'OP (*OpenID Provider*).

1. Le RP regarde le site Web de l'utilisateur et trouve l'OP,
2. Le RP contacte l'OP, lui demandant d'authentifier l'utilisateur,
3. Le RP redirige l'utilisateur vers son OP,

Mais comment ça a marché ?

Le site Web qui veut authentifier est le RP. Le fournisseur d'identité est l'OP.

1. Le RP regarde le site Web de l'utilisateur et trouve l'OP,
2. Le RP contacte l'OP, lui demandant d'authentifier l'utilisateur,
3. Le RP redirige l'utilisateur vers son OP,
4. L'OP authentifie l'utilisateur (OpenID ne dit pas comment),

Mais comment ça a marché ?

Le site Web qui veut authentifier est le RP. Le fournisseur d'identité est l'OP.

1. Le RP regarde le site Web de l'utilisateur et trouve l'OP,
2. Le RP contacte l'OP, lui demandant d'authentifier l'utilisateur,
3. Le RP redirige l'utilisateur vers son OP,
4. L'OP authentifie l'utilisateur (OpenID ne dit pas comment),
5. L'OP redirige l'utilisateur vers le RP.

Mais comment ça a marché ?

Le site Web qui veut authentifier est le RP. Le fournisseur d'identité est l'OP.

1. Le RP regarde le site Web de l'utilisateur et trouve l'OP,
2. Le RP contacte l'OP, lui demandant d'authentifier l'utilisateur,
3. Le RP redirige l'utilisateur vers son OP,
4. L'OP authentifie l'utilisateur (OpenID ne dit pas comment),
5. L'OP redirige l'utilisateur vers le RP.

Pour les requêtes HTTP exactes, voir l'article.

Support OpenID dans les logiciels

La plupart des moteurs de blog l'ont déjà, parfois via une extension.

Sinon, il existe plusieurs bibliothèques libres, pour plusieurs langages de programmation.

Choisir son identité

Choisir son identité

- Une identité ou plusieurs ? Une seule identité, c'est probablement trop risqué pour la vie privée (risque de jointure). Plutôt trois ou quatre.

Choisir son identité

- Une identité ou plusieurs ? Une seule identité, c'est probablement trop risqué pour la vie privée (risque de jointure). Plutôt trois ou quatre.
- Dépendant de l'OP (`http://me.myprovider.com/`) ou pas (`http://www.me.fr/`). Plutôt pas.

Choisir son identité

- Une identité ou plusieurs ? Une seule identité, c'est probablement trop risqué pour la vie privée (risque de jointure). Plutôt trois ou quatre.
- Dépendant de l'OP (`http://me.myprovider.com/`) ou pas (`http://www.me.fr/`). Plutôt pas.
- Choix du nom de domaine (publicité : le "`fr`" est ouvert aux particuliers).

Choisir son OP

Le choix d'un **fournisseur d'identité** (OP pour *OpenID provider*) demande les mêmes précautions que pour n'importe quel fournisseur (prix, stabilité, etc).

Choisir son OP

Le choix d'un **fournisseur d'identité** (OP pour *OpenID provider*) demande les mêmes précautions que pour n'importe quel fournisseur (prix, stabilité, etc).

En prime :

- Que fait-il de ses journaux ? (Risques pour la vie privée.)
- Offre t-il des services supplémentaires, notamment les extensions d'OpenID ? Et d'autres protocoles ?

Créer un OP

Pour la vie privée, l'indépendance technologique et le plaisir, on peut être son propre OP. C'est relativement facile.

Créer un OP

Pour la vie privée, l'indépendance technologique et le plaisir, on peut être son propre OP. C'est relativement facile.

- Soit un logiciel tout fait qui utilise une base existante (comme Gracie, avec PAM),

Créer un OP

Pour la vie privée, l'indépendance technologique et le plaisir, on peut être son propre OP. C'est relativement facile.

- Soit un logiciel tout fait qui utilise une base existante (comme Gracie, avec PAM),
- Soit en utilisant les bibliothèques libres existantes pour développer sa propre solution.

Sécurité

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

Sécurité

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, ...

Autres systèmes d'identité

La plupart sont très différents d'OpenID donc ne sont pas réellement « concurrents ».

Autres systèmes d'identité

La plupart sont très différents d'OpenID donc ne sont pas réellement « concurrents ».

- Infospace de Microsoft (et son implémentation Cardspace)

Autres systèmes d'identité

La plupart sont très différents d'OpenID donc ne sont pas réellement « concurrents ».

- Infospace de Microsoft (et son implémentation Cardspace)
- LibertyAlliance

Autres systèmes d'identité

La plupart sont très différents d'OpenID donc ne sont pas réellement « concurrents ».

- Infospace de Microsoft (et son implémentation Cardspace)
- LibertyAlliance
- SAML

Autres systèmes d'identité

La plupart sont très différents d'OpenID donc ne sont pas réellement « concurrents ».

- Infospace de Microsoft (et son implémentation Cardspace)
- LibertyAlliance
- SAML
- X509

Autres systèmes d'identité

La plupart sont très différents d'OpenID donc ne sont pas réellement « concurrents ».

- Infospace de Microsoft (et son implémentation Cardspace)
- LibertyAlliance
- SAML
- X509
- Uprove

Autres systèmes d'identité

La plupart sont très différents d'OpenID donc ne sont pas réellement « concurrents ».

- Infospace de Microsoft (et son implémentation Cardspace)
- LibertyAlliance
- SAML
- X509
- Uprove
- Shibboleth

Autres systèmes d'identité

La plupart sont très différents d'OpenID donc ne sont pas réellement « concurrents ».

- Infospace de Microsoft (et son implémentation Cardspace)
- LibertyAlliance
- SAML
- X509
- Uprove
- Shibboleth
- ...

Questions politiques et sociales

Questions politiques et sociales

- Identité contrôlée par l'utilisateur ? Par l'État ? Par une grosse société privée ?

Questions politiques et sociales

- Identité contrôlée par l'utilisateur ? Par l'État ? Par une grosse société privée ?
- Le consentement de l'utilisateur a t-il un sens, si la révélation d'informations privées est une précondition pour accéder à un service ?

Questions politiques et sociales

- Identité contrôlée par l'utilisateur ? Par l'État ? Par une grosse société privée ?
- Le consentement de l'utilisateur a t-il un sens, si la révélation d'informations privées est une précondition pour accéder à un service ?
- Les données privées sont-elles une marchandise dont je suis propriétaire ? Ou bien, comme mon corps, sont-elles inaliénables ?