Microsoft

Gestion de l'identité en environnement Web 2.0

Pierre Couzy
Architecte en Systèmes d'information
Microsoft France
plerre.couzy@microsoft.com

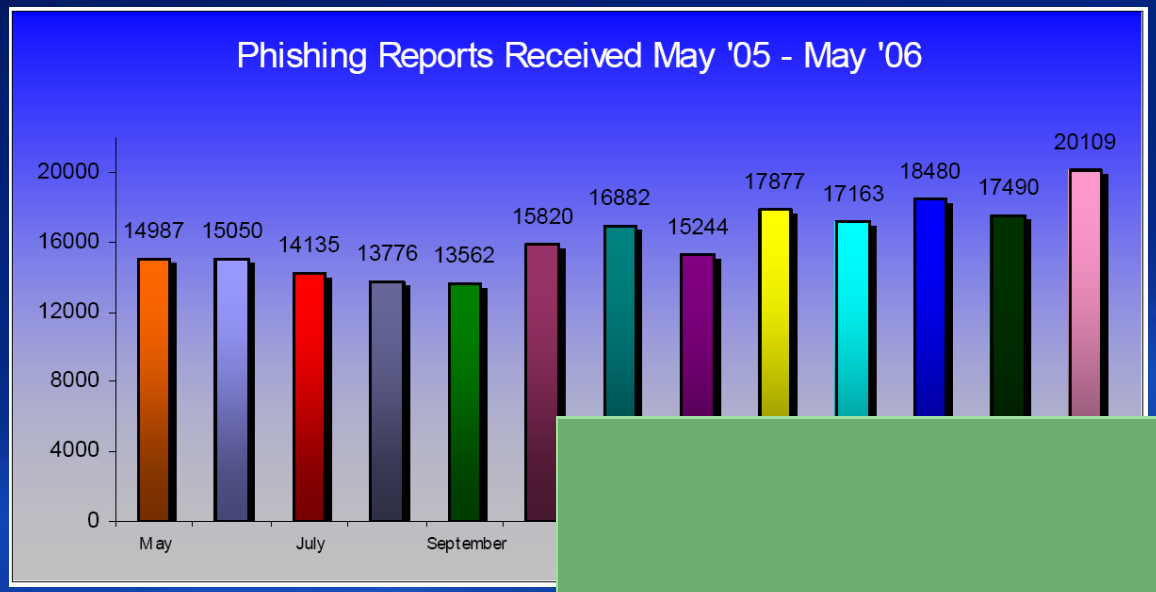
Sommaire

- Internet vu de l'utilisateur
- Qu'est-ce que l'identité ?
  - Définition
  - Principes fondateurs d'un système d'identité
- Que propose CardSpace ?
  - Le sélecteur d'identité
  - Les protocoles de communication
- Pourquoi investir dans CardSpace ?

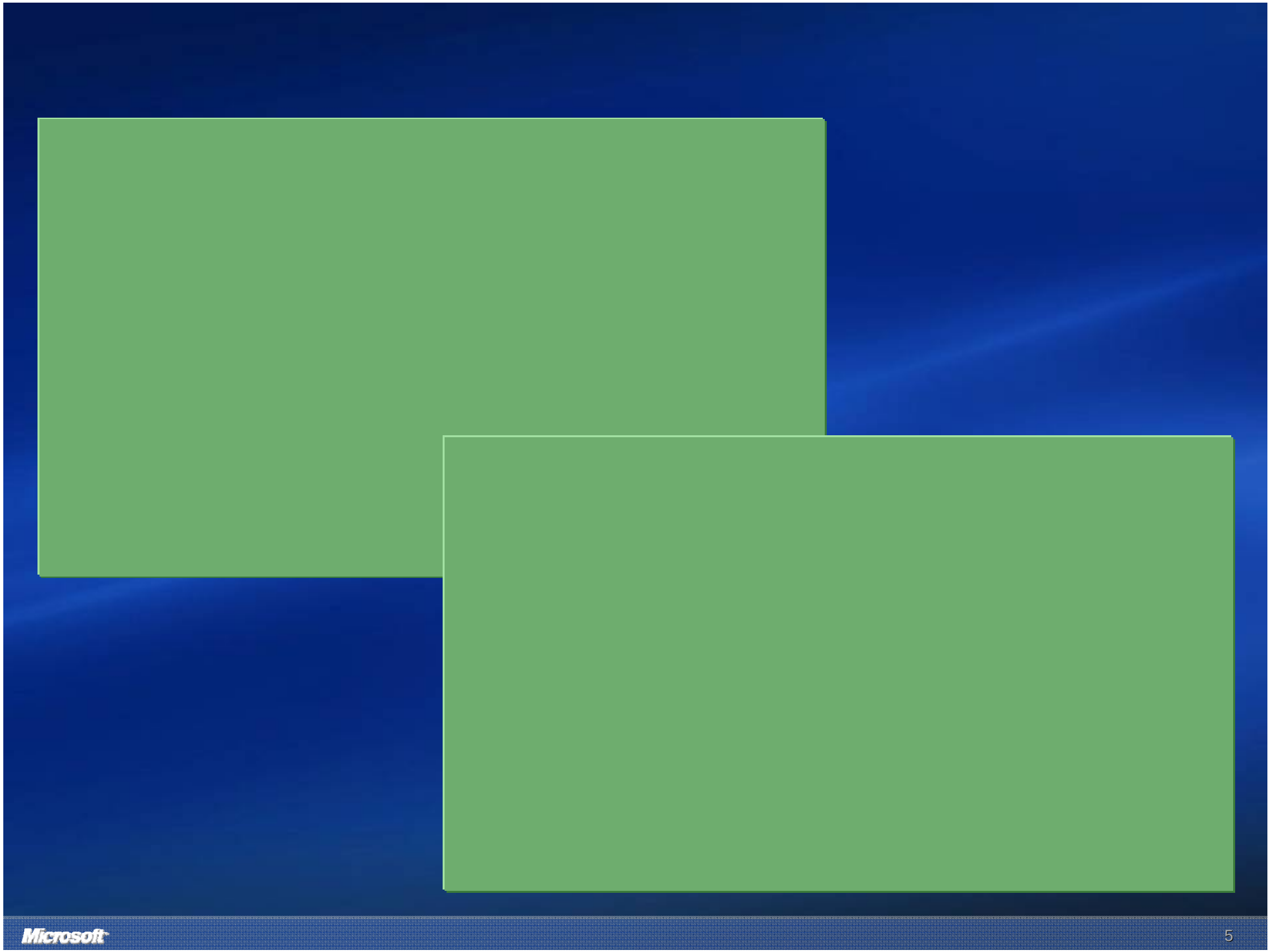
Pas de Web 2.0 sans utilisateurs

Oui, mais …

Ca ressemble au site de ma banque …



Source: http://www.antiphishing.org



Cliquez ici pour vous inscrire…

Un problème prévisible

- La sécurité n'a pas été un but de conception de l'Internet
  - ftp, rsh, smtp, etc.
- Une première brique a été construite autour de l'identité des serveurs
- L'identité des utilisateurs n'est pas aujourd'hui normalisée
  - Repose sur des certificats, des comptes système, des bases locales aux applications, etc.
- Ce manque de normalisation est bloquant pour de nombreuses architectures
  - Pas de pattern standard pour l'utilisateur ou l'application cliente
  - Pas de fédération d'identité entre différents consommateurs d'identité
- Et pour l'utilisateur
  - Perte de confiance

Sommaire

- Internet vu de l'utilisateur
- Qu'est-ce que l'identité ?
  - Définition
  - Principes fondateurs d'un système d'identité
- Que propose CardSpace ?
  - Le sélecteur d'identité
  - Les protocoles de communication
- Pourquoi investir dans CardSpace ?

Qui suis-je ?

Le_testeur@hotmail.com

Cycliste

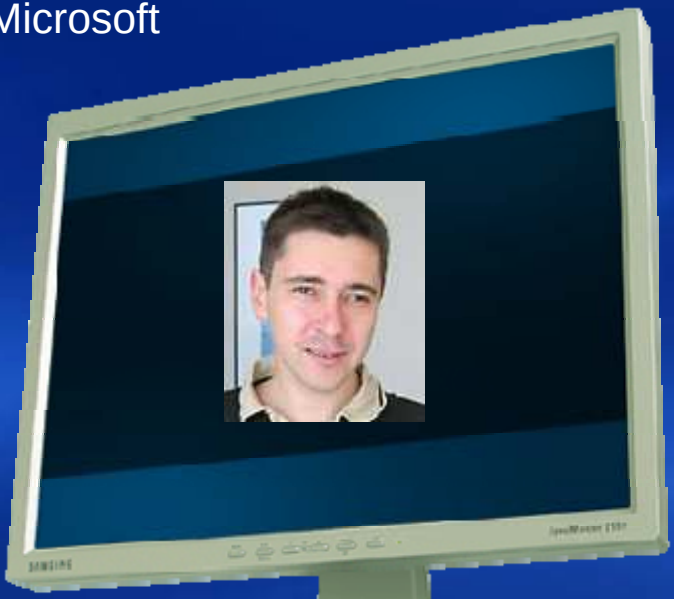
01 45 08 XX XX

Architecte chez Microsoft

Membre 13083xx de la FFB

Speaker ce matin

Ex employé de MTV Telecom



Pierre Couzy

Amateur de films indiens

Fils de, frère de, père de, …

N° de sécurité sociale : 169XXXXXXXXX

Pointure : 43

piercou@nospam.microsoft.com

Collaborateur de Steve Sfartz

01 69 86 xx xx

Ancien élève de, membre actif de, ex enseignant de, …

Apprécié à 90,4% sur ebay

6 points sur mon permis

Ancien élève du lycée Montaigne

Client régulier chez mon coiffeur

Qu’est-ce que l’identité ?

- Mon identité
  - Dépend de qui me la demande
    - Pointure pour un marchand de chaussettes
    - Bancaire pour un paiement
    - Civile pour un vote
    - Médicale pour un hôpital
    - …
  - Peut être auto-proclamée
    - Personne ne garantit ma pointure
  - ou garantie et maintenue par une tierce partie
    - Date de mon dernier rappel anti-tétanique
    - Plafond de retrait hebdomadaire
    - Mon classement au bridge

Confusion identité / identifiant

- Un site web utilise mon email comme identifiant.
  - Cet email sert à deux choses
    - Clé primaire d'un certain nombre de relations en base
    - Adresse email pour communiquer avec moi
  - Si je change d'adresse email
    - La première fonction demande que le site conserve le champ email
    - La deuxième qu'il le change
- Fondamentalement, un identifiant est une donnée technique
  - Symbolise la relation entre un sujet et un consommateur d'identité
  - Ne porte ni l'identité ni l'authentification
  - Si l'identifiant porte une connotation métier, il fragilise le système
- L'identifiant ne doit pas être partagé entre consommateurs d'identité
  - Donneriez-vous votre No de Sécurité Sociale à Amazon ?

Confusion identité / profil

- Mon identité : ce qui peut être proclamé
  - Par le sujet : jeu d'infos utile pour N services
  - Par un fournisseur d'identité : jeu d'infos de son domaine
- Mon profil : ce dont le service a besoin pour fonctionner
  - Infos complémentaires
  - Historique
  - …
- Un système réparti doit faire la distinction entre les deux
  - L'identité est sous la responsabilité du fournisseur d'identité
  - Le profil est sous la responsabilité du consommateur d'identité

En résumé

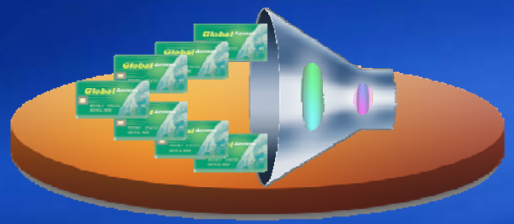
- Identité
  - Corrélé à (moi dans un domaine)
  - Ensemble de données proclamé ou auto-proclamé
- Identifiant
  - Décorrélé de l'identité
  - Propre à ma **relation** avec un service
  - C'est un artefact technique
- Profil
  - Corrélé à (moi dans un domaine pour le service auquel j'accède)
  - Contient au moins un sous-ensemble de l'identité et un identifiant

Sommaire

- Internet vu de l'utilisateur
- Qu'est-ce que l'identité ?
  - Définition
  - Principes fondateurs d'un système d'identité
- Que propose CardSpace ?
  - Le sélecteur d'identité
  - Les protocoles de communication
- Pourquoi investir dans CardSpace ?

Quels acteurs ?

Consommateur d'identité



Fournisseur d'identité

Sujet

Individu et/ou application

Une première approche : le SSO

- Tous les consommateurs d'identité
  - S'adressent à un fournisseur centralisé (éventuellement répliqué)
  - Récupèrent un jeu d'informations normalisé
- Fonctionne bien dans un périmètre donné (entreprise élargie)
  - Un seul fournisseur d'identité, ou
  - Les informations d'identité se rapportent toutes au même domaine métier, et
  - L'identité est propageable entre fournisseurs (ADFS)
- Echoue dès qu'on sort de ce périmètre
  - Collaboration ad hoc entre entreprises
  - La plupart des scénarios Internet
  - Un exemple : Passport
    - Excellent système de gestion des utilisateurs sur le périmètre des sites grand public Microsoft
    - N'a pas fonctionné hors de ce périmètre

  … Pourquoi ?

Les lois de l'identité

- Etablies au travers d'un dialogue avec l'industrie

1. Contrôle et consentement de l'utilisateur
2. Divulgation minimale pour un usage défini
3. Présence justifiée des parties en présence
4. Support d'identités publiques et privées
5. Pluralisme des opérateurs et des technologies
6. Prise en compte de l'humain
7. Expérience cohérente entre les contextes

Rejoignez les discussions sur http://www.identityblog.com

Sommaire

- Internet vu de l'utilisateur
- Qu'est-ce que l'identité ?
  - Définition
  - Principes fondateurs d'un système d'identité
- Que propose CardSpace ?
  - Le sélecteur d'identité
  - Les protocoles de communication
- Pourquoi investir dans CardSpace ?

CardSpace : buts de conception

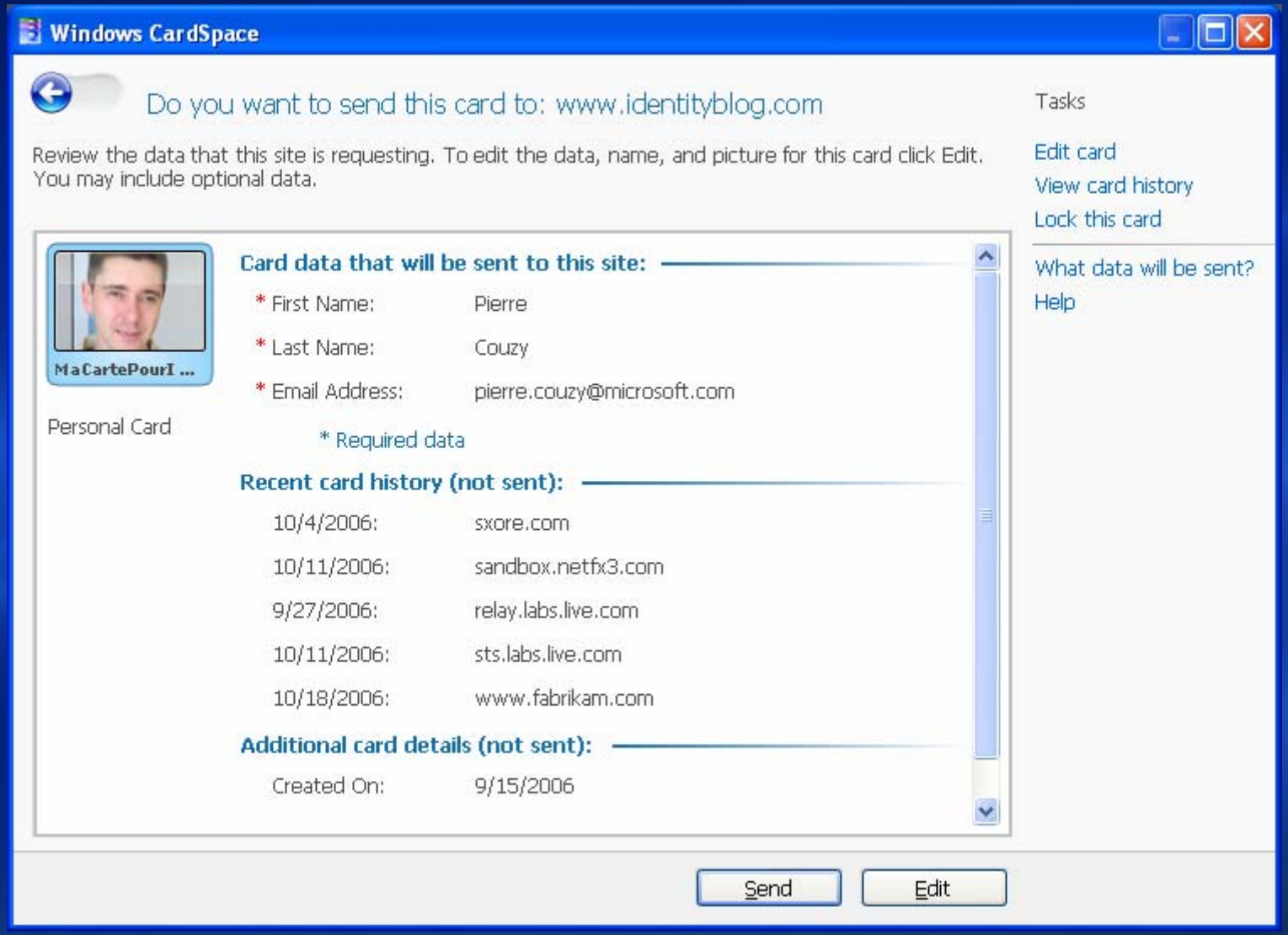
Suivre les lois de l'identité :

- Sortir du SSO pour aller vers un mécanisme de fédération
- Donner au sujet le contrôle
  - De la transmission de son identité
  - De l'identité de son interlocuteur
- Donner aux consommateurs d'identité
  - Une implémentation simple
  - L'autonomie dont ils ont besoin vis-à-vis des fournisseurs d'identité

Les acteurs d'une communication

- Un fournisseur d'identité
- Un consommateur d'identité
- Un sujet (moi, mon programme)
- Que propose CardSpace ?
  - La mise en relation des 3 acteurs
    - Un ensemble de protocoles standards réutilisables et interopérables.
  - Un sélecteur d'identité pour le sujet
    - Une implémentation cliente sous XP et Vista

Le sélecteur d'identité



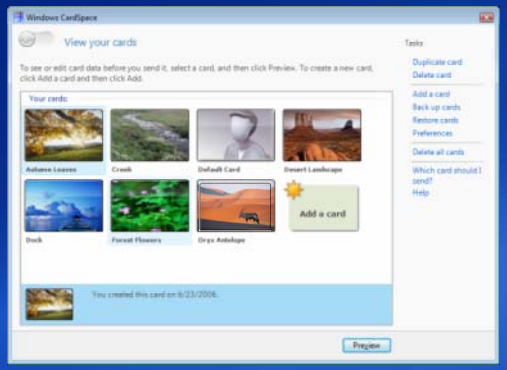
Les acteurs et protocoles

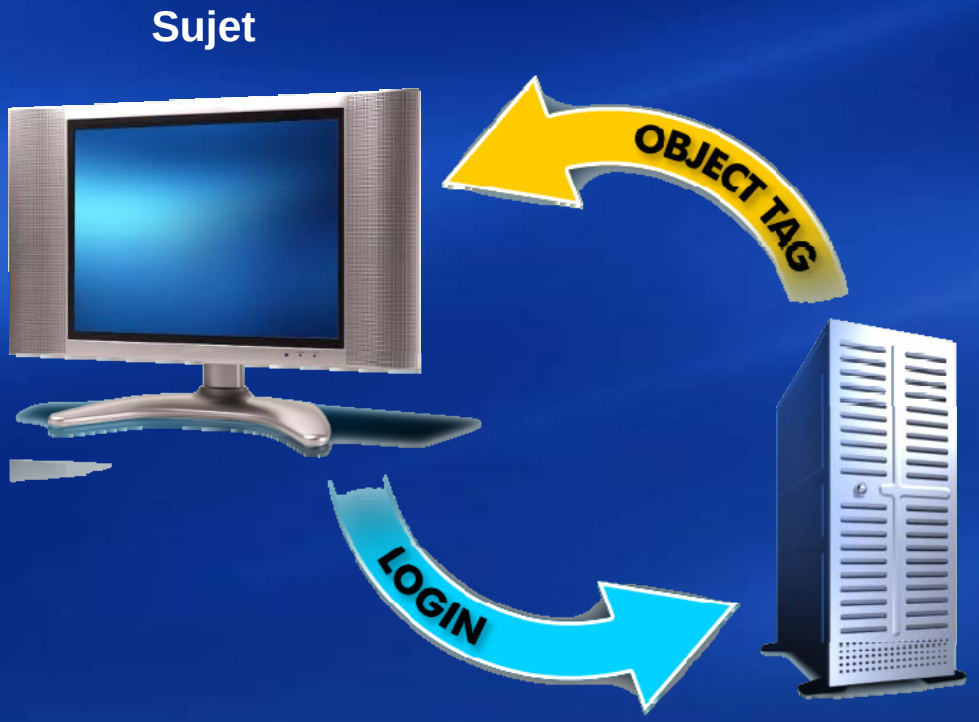
Sujet

Fournisseur d’identité

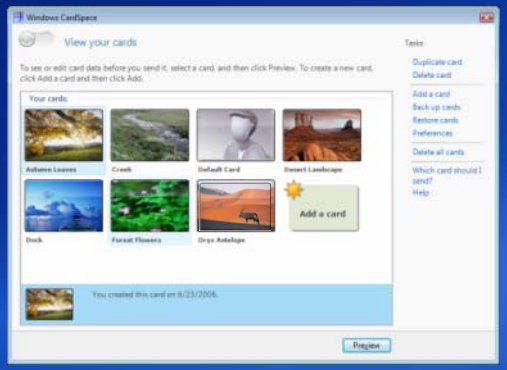
Consommateur d’identité

Login avec carte personnelle





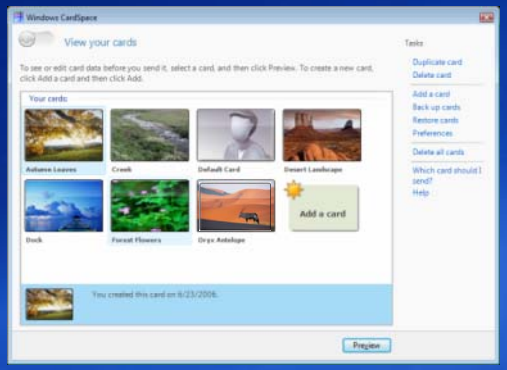
Sélection de la carte



Sujet

Consommateur d'identité

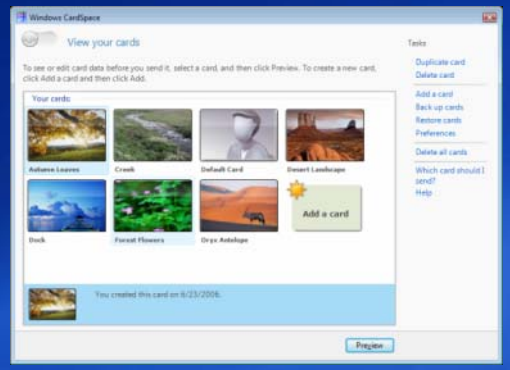
Création du jeton



Sujet

Consommateur d'identité

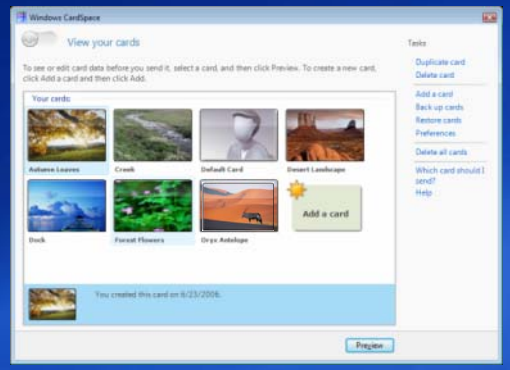
Chiffrement, signature, transmission

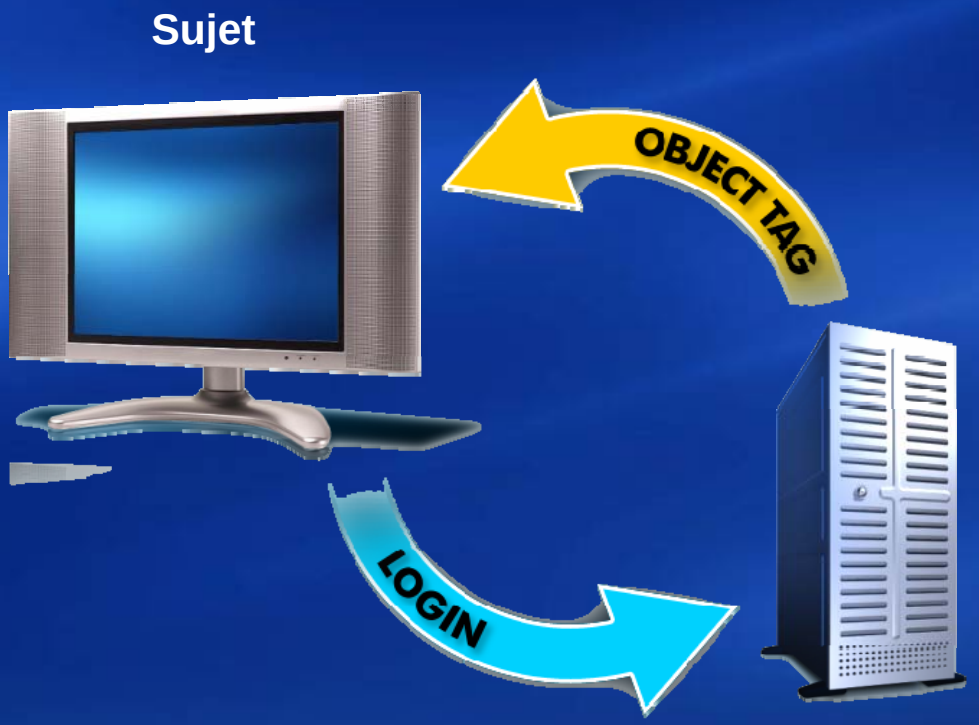


Sujet

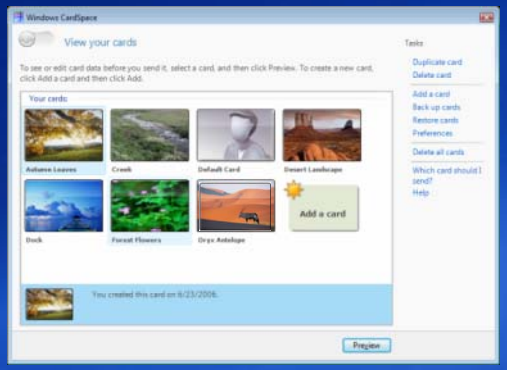
Consommateur d'identité

Login avec carte managée





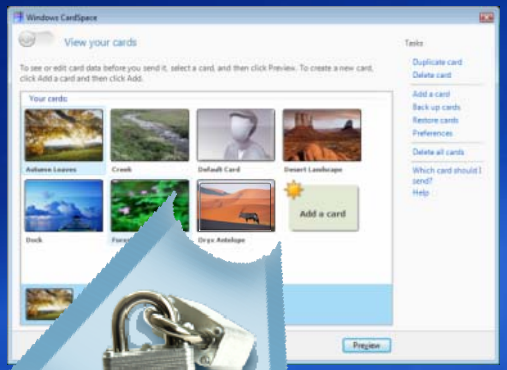
Sélection d'une carte



Sujet

Consommateur d'identité

Sélection d’une carte



Sujet

Auth’:
X509, Kerb, SIC, U/PWD
…

Fournisseur d’identité

Consommateur d’identité

Demande d’un jeton

Transmission du jeton

Sujet

Fournisseur d’identité

Consommateur d’identité

Login via CardSpace

Sommaire

- Internet vu de l'utilisateur
- Qu'est-ce que l'identité ?
  - Définition
  - Principes fondateurs d'un système d'identité
- Que propose CardSpace ?
  - Le sélecteur d'identité
  - Les protocoles de communication
- Pourquoi investir dans CardSpace ?

Quelles garanties pour l'utilisateur ?

- Seul le site cible peut avoir accès à mes informations
  - Le jeton est chiffré,
  - Non modifiable,
  - Non rejouable,
  - Non interceptable
- Le site cible est identifié de façon non ambigüe
  - Certificat + logotype
  - Historique d'utilisation de la carte
  - Avertissement en cas de première utilisation
- Vol de carte ?
  - La carte ne contient pas les infos
  - Point de révocation : le fournisseur d'identité
  - Pour les identités auto-proclamées, la révocation doit se faire auprès du consommateur d'identité

Quelles garanties pour l'entreprise ?

- L'entreprise ou le site web (consommateur d'identité)
  - Peut imposer un partenaire (fournisseur d'identité) précis
    - Intégration dans un sign on d'entreprise (AD)
    - Intégration à un organisme bancaire (e-commerce)
  - Peut supprimer la dépendance avec un partenaire
    - Demande d'une donnée sans préciser son garant
    - Je veux avoir l'âge, quel que soit le garant de cette donnée
    - Réutilisation d'un ou N systèmes existants
  - Doit s'identifier (anti phishing)
    - => certificat, donc SSL pour les sites
- L'utilisateur ne détient pas son identité
  - Il demande un jeton au partenaire (fournisseur d'identité)
  - Ce jeton est non modifiable
  - L'entreprise sait que les données sont miennes, à jour, et non corrompues

CardSpace, propriétaire ?

- L'architecture de CardSpace et les protocoles sur lesquels il repose sont intégrés à l'OSP (Open Specification Promise)
  - http://www.microsoft.com/interop/osp
  - http://identityblog.burtongroup.com/
- Le sélecteur d'identité se répand rapidement
  - Pour Windows

    intégré à IE7 et à .Net 3
  - Pour Macintosh

    http://www.hccp.org/safari-plug-in.html

    (cartes auto-proclamées uniquement)
  - Pour le reste du monde

    http://xmldap.org/ (sélecteur pour Firefox)

CardSpace, propriétaire ?

- Pour les consommateurs d'identité
  - Le code de manipulation d'un jeton est disponible aujourd'hui en .Net, php et Java
  - Pour écrire le vôtre : xmldap.org
- Pour les fournisseurs d'identité
  - Active Directory comporte un STS (ADFS V2)
  - Oracle, IBM, Novell,
  - Ecrire le vôtre : netfx3.com ou xmldap.org

L’intégration avec Livo

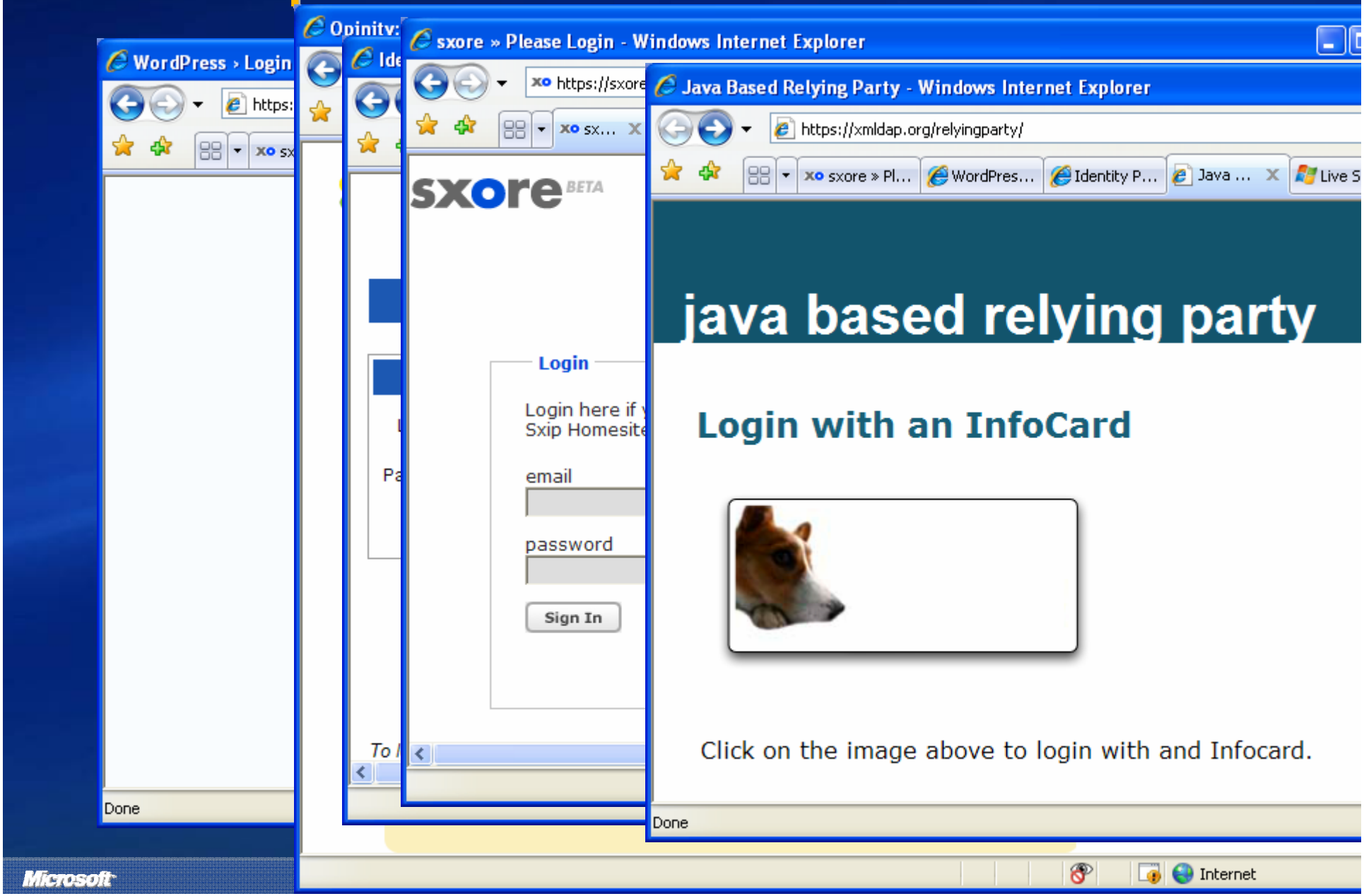
- Lorsque l’utilisateur de Cardspace demande un jeton XML à un fournisseur, il doit montrer patte blanche
  - Possession d’un certificat
  - Kerberos
  - Username/password
  - Présentation d’un jeton (fédération)
- Nous explorons deux pistes avec Livo
  - Création d’un Fournisseur d’identité local sur clé USB
  - Utilisation de WS-Federation pour un scénario centralisé

L’intégration avec Livo

- L’intérêt de l’intégration Livo/CardSpace
  - Une authentification Livo dans un scénario CardSpace
    - => Authentification forte plus conviviale et à un coût moindre que les solutions OTP/SmartCard
  - L’utilisation de CardSpace comme agent d’authentification pour le système Livo
    - => Interopérabilité avec les grands standards de gestion d’identité numérique
    - => Solutions mixtes Livo/Autre facteur d’authentification

Utilisation d’un fournisseur d’identité local

Exemples de sites



Où trouver de l'information ?

Un point d'entrée : http://cardspace.netfx3.com

Des blogs :

- Kim Cameron — http://www.identityblog.com/
- Andy Harjanto — http://blogs.msdn.com/andyhar/
- Garrett Serack — http://blogs.msdn.com/garretts/
- Vittorio Bertocci — http://blogs.msdn.com/vbertocci/

Interop : http://wiki.eclipse.org/CardSpace_Interop

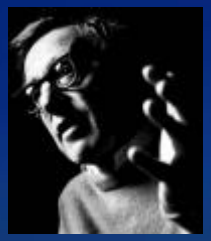
Un site de test : www.cardspacedemos.com

Un bon résumé technique :
http://channel9.msdn.com/ShowPost.aspx?PostID=241455

OSP : http://www.microsoft.com/interop/osp

Dick Hardt : http://identity20.com/media/OSCON2005/

discussion



La réponse est oui.
Mais quelle était la question ?

Microsoft®

Your potential. Our passion.™