

12 mars 2009
Baker & McKenzie,
Paris

Paris
Baker & McKenzie
12 mars 2009

Les technologies de gestion de l'identité

ATELIER 1

Paul TREVITHICK, CEO de Parity – Responsable projet Higgins – Président
Fondation Infocard (en anglais)

InfoCard / Higgins

Fulup AR FOLL, Sun – Master Architect

Liberty Alliance

Christophe BOUTET, Entr'ouvert – PDG

Point de vue d'un intégrateur de solution Liberty Alliance

Sébastien BRAULT, **Karim SBATA**, Orange

OpenID et solutions Orange

Pierre COUZY, Microsoft France - Architecte en système d'informations

Philippe BERAUD, Microsoft France

Cardspace et autres solutions Microsoft

Commission Identité Numérique

Groupe de travail Gestion des identités

ATELIER

Les technologies de gestion de l'identité

Philippe BERAUD, CISSP

Consultant Architecte

Direction Technique

Microsoft France

philippe.beraud@microsoft.com

Pierre COUZY

Architecte en système d'informations

Division Plateforme et Ecosystème

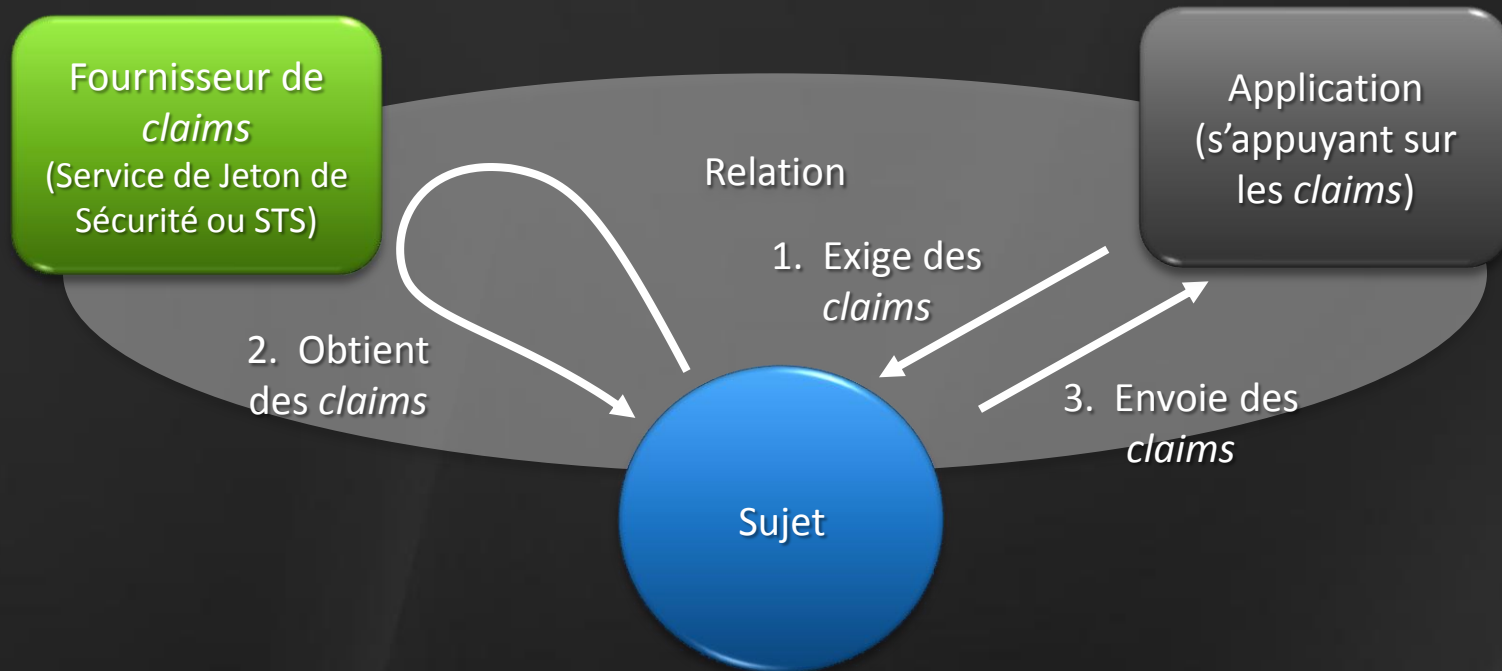
Microsoft France

pierre.couzy@microsoft.com

Le périmètre

- ▶ Microsoft a historiquement investi dans
 - ▶ La gestion centralisée d'une base de SSO (Passport, Live ID)
 - ▶ Les ponts entre l'entreprise et l'Internet (AD Federation Services)
 - ▶ Les protocoles et formats d'une gestion d'identité fédérée (tournée vers des scénarios actifs - Cardspace)
 - ▶ L'interopérabilité avec les autres acteurs du marché et les scénarios Cloud
- ▶ Tous ces investissements se font dans le respect et la protection des données personnelles (divulgaration minimale et directionnelle, etc.)

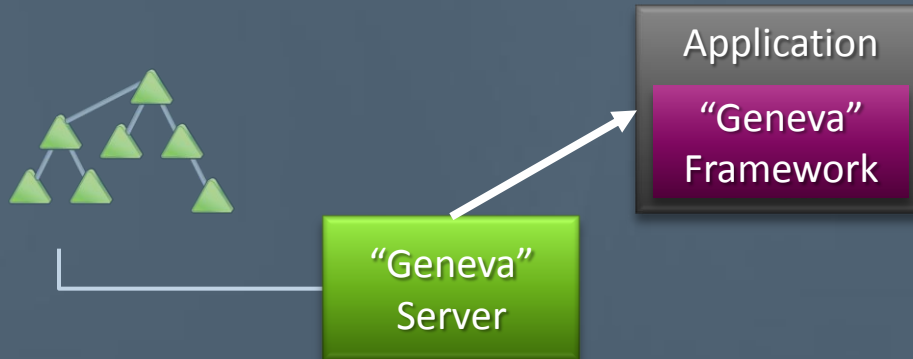
Un modèle basé sur les *claims*



- Application : exige, et utilise la notion de *claims* pour définir les utilisateurs et les contrôles d'accès
- Fournisseur de *claims* : supporte les protocoles pour l'émission de *claims*
- Relationship : contexte dans lequel la signification/sémantique des *claims* est définie

“Backbone” Identité B2B

“Backbone” Identité d’Entreprise



Claims



“Geneva” Server

- STS intégré avec les services d’annuaires Active Directory
- Supporte Windows CardSpace

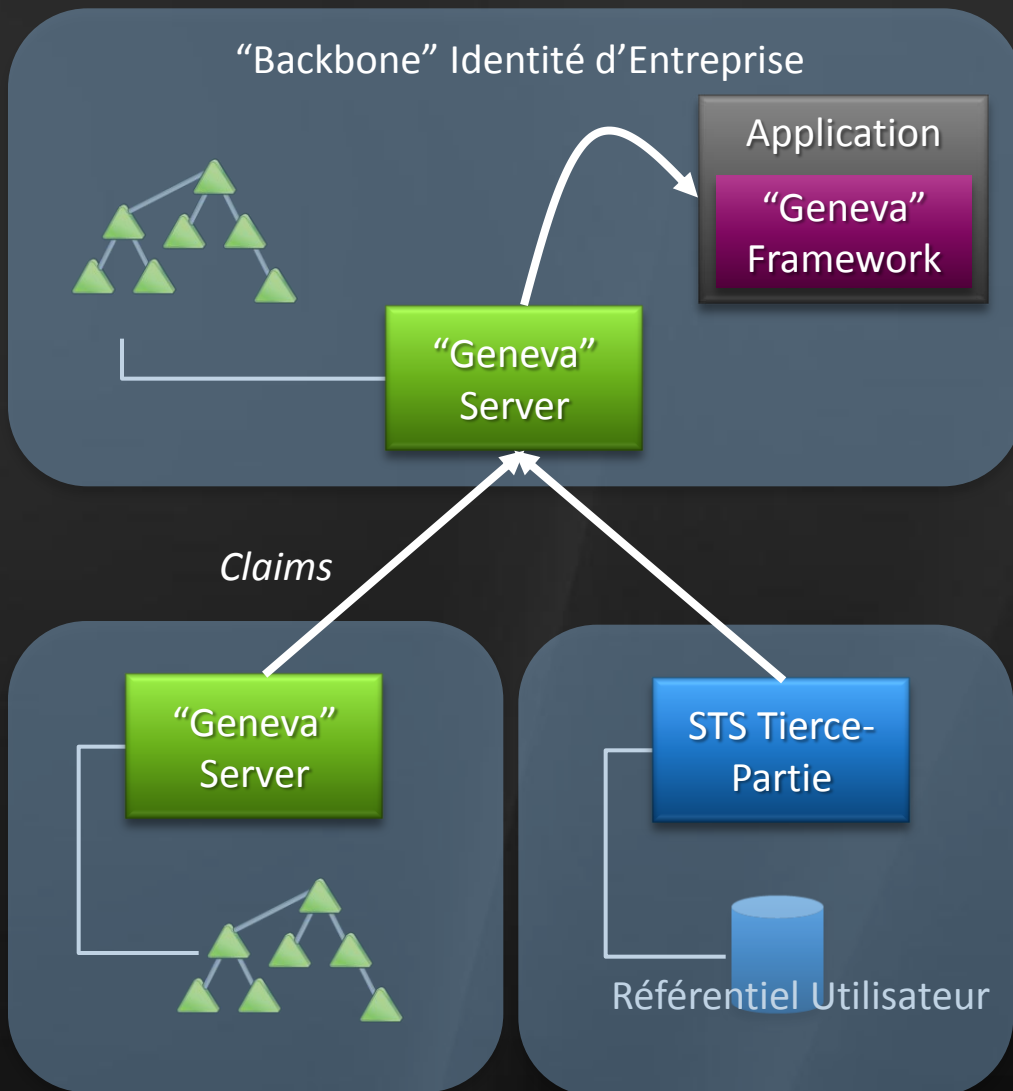
“Geneva” Framework

- Framework .NET pour la conception d’applications “claims-aware”

Windows CardSpace “Geneva”

- Sélecteur d’identité sous le contrôle explicite des utilisateurs
- Plus compact et rapide

Pile d'identité interoperable



Supporte

- ▶ WS-Federation,
- ▶ WS-Trust,
- ▶ SAML 2.0



Interopère avec les logiciels et les services qui supporte ces standards

Pour mémoire : interopérabilité AD FS 1

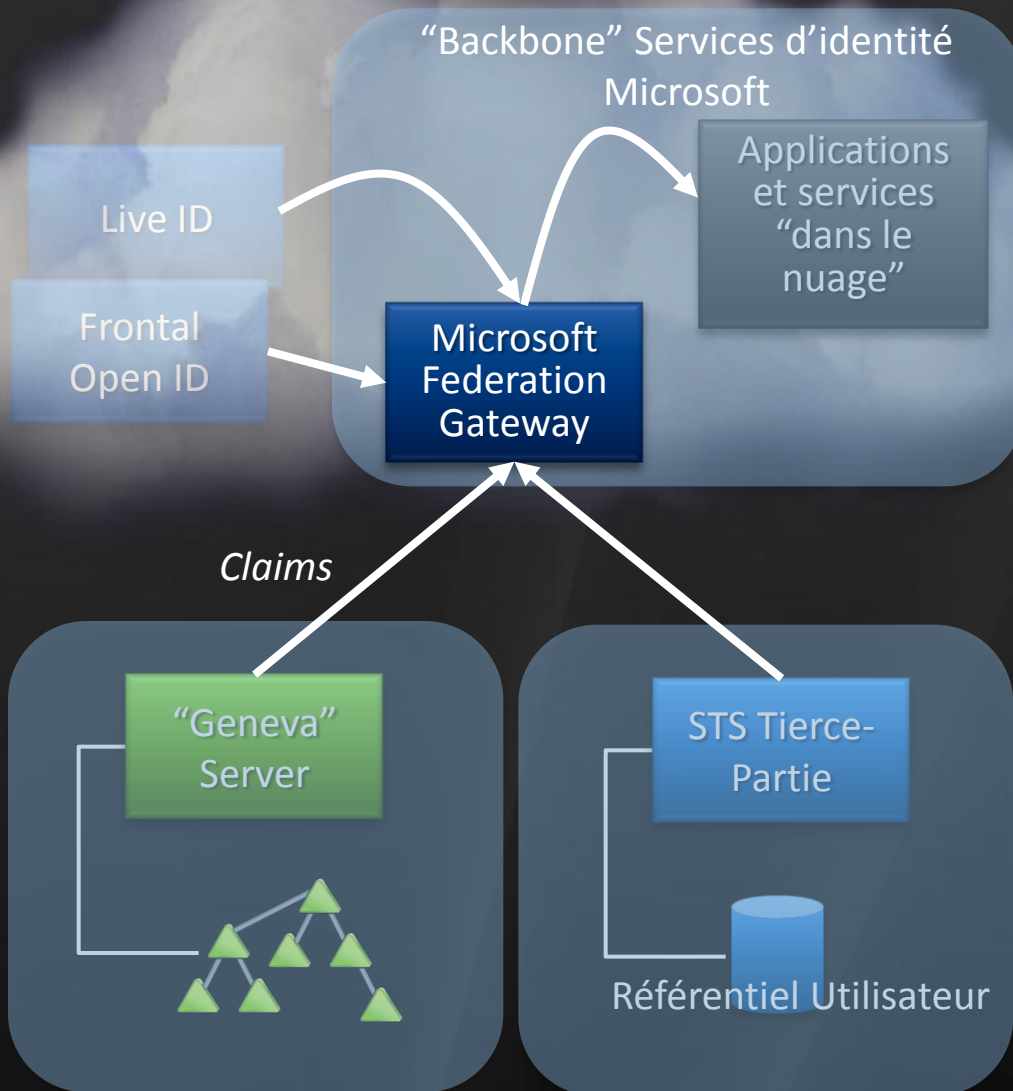
▶ Protocoles AD FS

- ▶ Décrit au niveau du programme Windows Server Protocols (WSPP)
 - ▶ <http://msdn.microsoft.com/en-us/library/cc197979.aspx>
 - ▶ [[MS-MWBF](#)] et [[MS-MWBE](#)]

▶ Solutions d'identité tierce interopérables

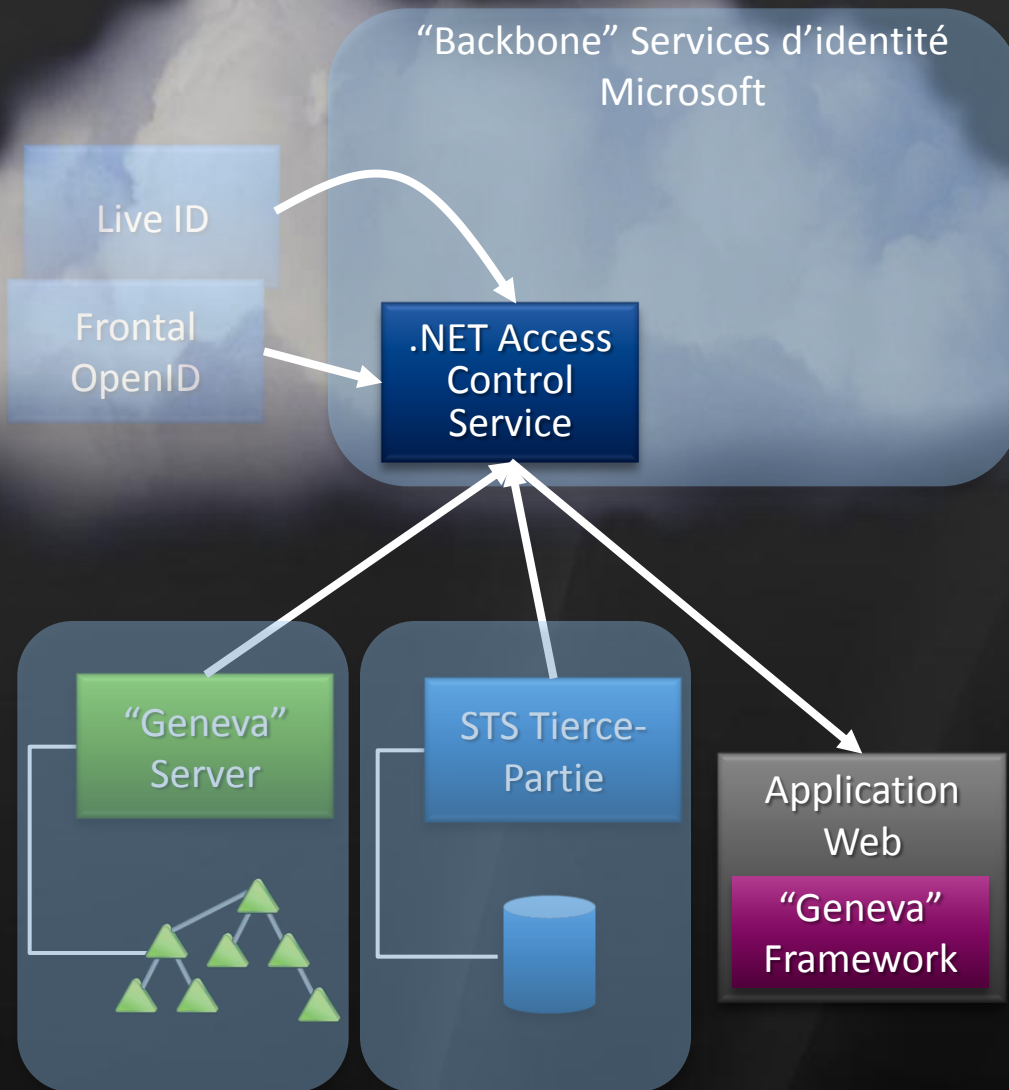
- ▶ BMC Universal Identity Federator
- ▶ CA eTrust SiteMinder Federation Security Services (6 SP5)
- ▶ IBM Tivoli Federated Identity Manager
- ▶ Internet2 Shibboleth System (1.3)
- ▶ Oracle Identity Federation
- ▶ Ping Identity PingFederate Server
- ▶ RSA Federated Identity Manager (4)
- ▶ symLABS Federated Identity Suite
- ▶ Version3 Enhanced Authentication Edition
- ▶ Novell Access Manager
- ▶ Sun OpenSSO

Des applications en entreprise vers le nuage



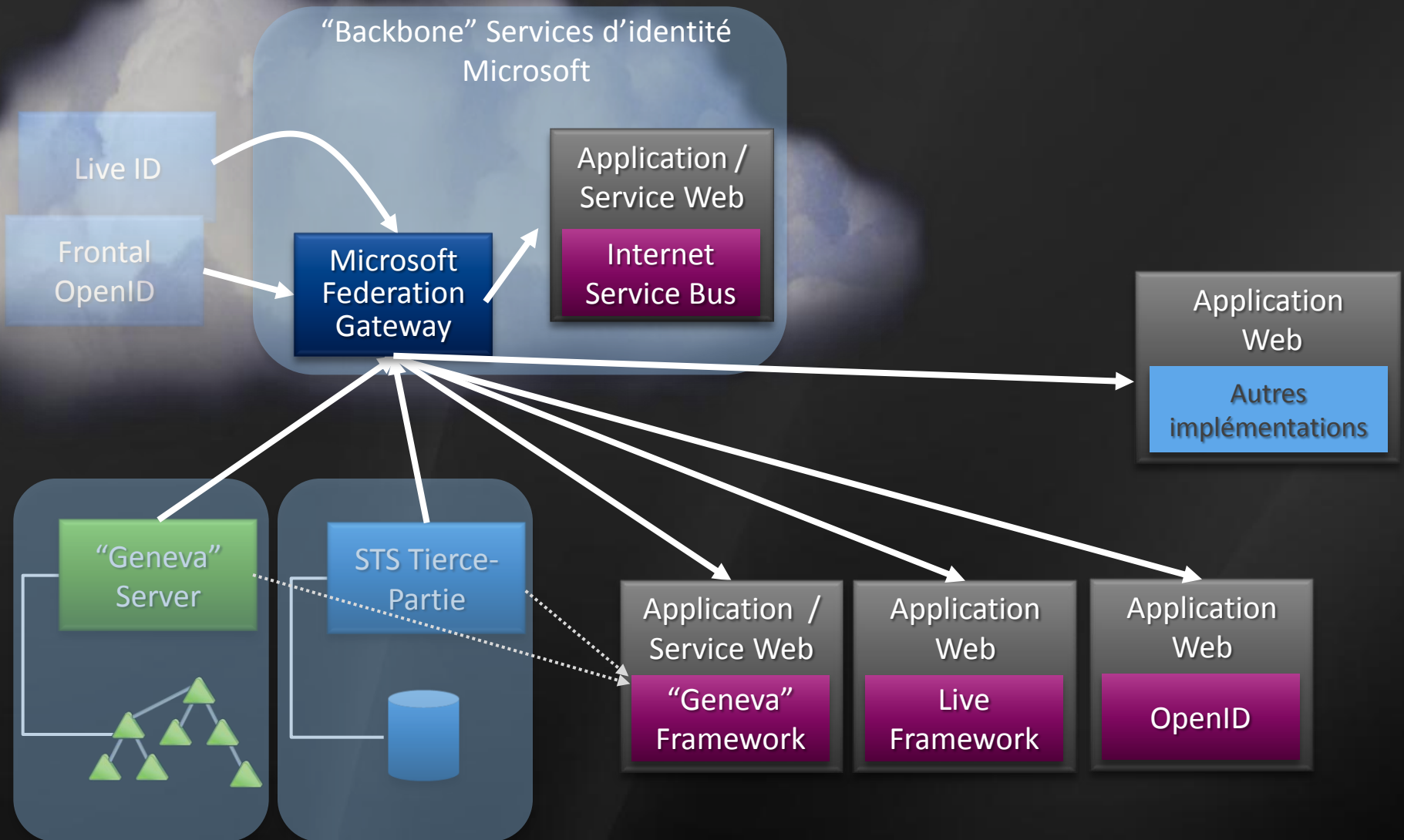
- ▶ Le service Microsoft Federation Gateway (MFG) constitue le socle du "backbone" identité de Microsoft
- ▶ Accès par "Broker" au applications et services dans le nuage Microsoft
- ▶ Une seule relation de fédération pour accéder à n'importe quel service
- ▶ Conforme avec WS-Federation, WS-Trust

Utiliser des *claims* pour le contrôle d'accès



- ▶ Les *claims* sont destinées à plus que juste du login
- ▶ .NET Access Control Service : un STS qui émet des *claims* pour le contrôle d'accès
- ▶ Factorise la logique de contrôle d'accès d'une application en une collection de règles
- ▶ Portail de gestion, API pour la création et la gestion de collection de règles

Choix du protocole et du Framework

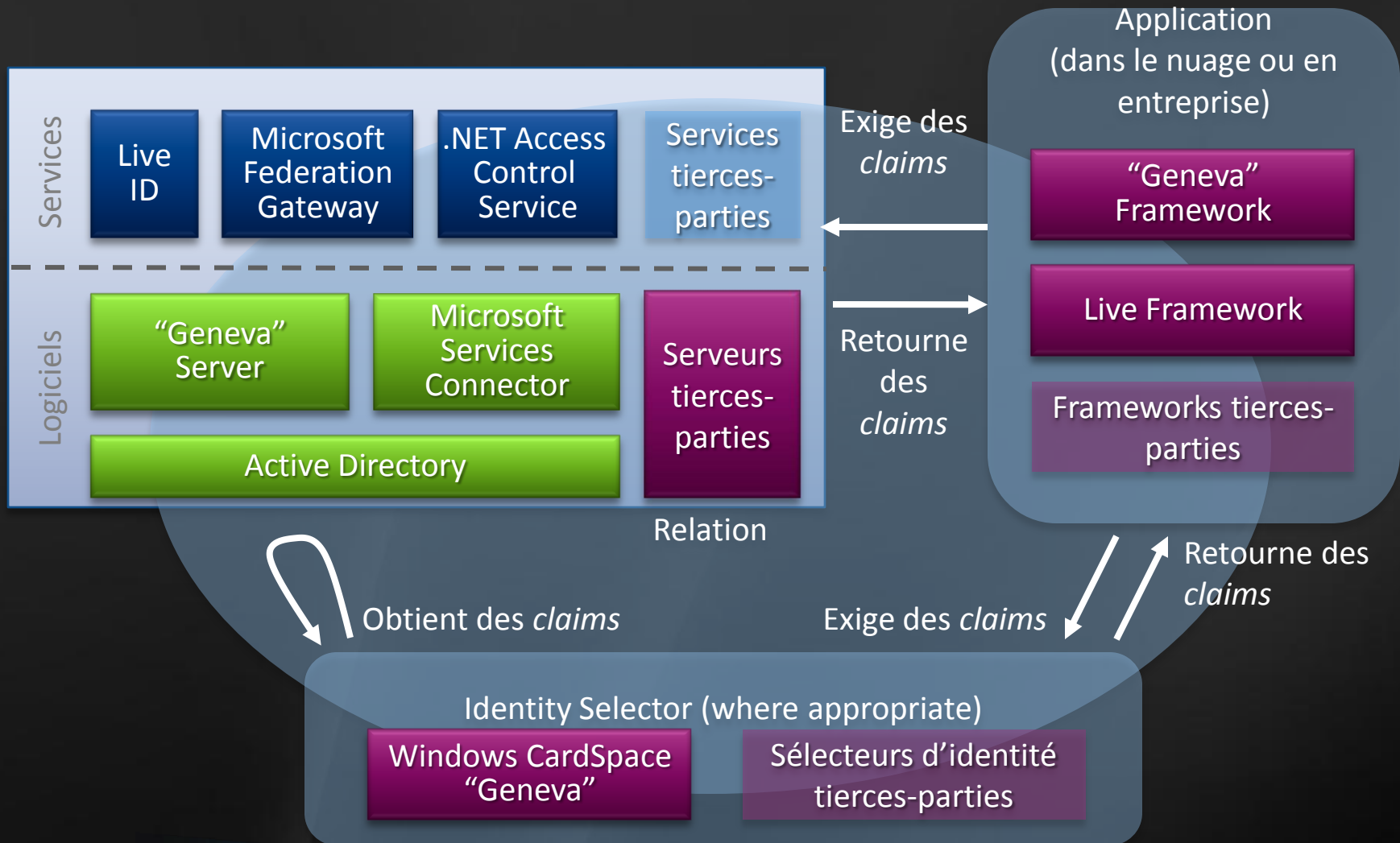


Software + Services Identité de Microsoft

- ▶ Jeu d'options riche supportant virtuellement tout type de scénario d'identité
 - ▶ L'architecture est la même que ce soit en entreprise "Geneva" Server ou avec les services dans le nuage
 - ▶ Les entreprises peuvent se fédérer avec le "backbone" en ligne de la même façon qu'elles se fédèrent avec d'autres entreprises
 - ▶ MFG donne aux entreprises la possibilité d'accepter des identités Live ID de consommateurs au même titre que des identités gérées
 - ▶ Les entreprises peuvent démarrer avec "Geneva" Server pour de la fédération directe...
 - ▶ ...Elles peuvent ensuite opter pour MFG de façon à simplifier leur gestion des identités avec les entreprises qui souhaitent faire de même
- ▶ Le modèle de programmation utilisé par les développeurs reste le même : un modèle d'identité qui met les utilisateurs de logiciels et de services en contrôle de leurs identités

Software + Services Identité de Microsoft

Méta-système d'identité et modèle basé sur les *claims*



Feuille de route

	PDC08 October'08	H2 CY 2008	H1 CY 2009	H2 CY 2009
"Geneva" Server	Beta 1		Beta 2	RTM
Microsoft Service Connector	CTP		Beta RTM	
"Geneva" FW, CardSpace	Beta 1		Beta 2	RTM
Live Framework	In Production			
Live Identity Services	OpenID Beta			OpenID RTM
Microsoft Federation Gateway	En Production			
.Net Access Control Service	CTP	Refresh	Beta 1	

Technologie UProve



- ▶ Technologie de cryptographie développée dans les années 90 par le Dr Stefan Brands
 - ▶ Académiquement bien établie
 - ▶ +25 publications de pairs
 - ▶ Ouvrage MIT (préfacé par Rivest)
 - ▶ http://www.credentica.com/the_mit_pressbook.html
 - ▶ Enseigné à MIT, Stanford, ENS, ETH, etc.
 - ▶ Visant à l'amélioration du respect de la vie privée
 - ▶ Acquis par Microsoft en mars 2008 suite au rachat de la société Credentica
 - ▶ Destinée à être intégrée dans la plateforme "Geneva" et au sein de WCF, l'implémentation Microsoft de la pile protocolaire standardisée WS-*



Authentification forte et Cartes eID

- ▶ Microsoft Windows Smartcard Framework
 - ▶ Mini-pilotes
 - ▶ Windows Update
 - ▶ Expérience Plug'N'Play avec Windows 7
- ▶ Microsoft Identity Lifecycle Manager (ILM) 2007
 - ▶ Cartes IAS 1.01 Premium officiellement supportées via le middleware IAS PKCS#11
 - ▶ Cartes IAS ECC en cours de validation
- ▶ ILM "2"
 - ▶ Support d'IAS comme dans ILM 2007

Pour aller plus loin

- ▶ Centre de développement MSDN sur “Geneva”
 - ▶ <http://www.microsoft.com/geneva>
 - ▶ Quelques livres-blancs
 - ▶ “Geneva” Claims Based Access Platform
 - ▶ http://download.microsoft.com/download/7/d/0/7d0b5166-6a8a-418a-addd-95ee9b046994/Introducing_Geneva_Beta1_Whitepaper.pdf
 - ▶ “Geneva” Framework
 - ▶ <http://download.microsoft.com/download/7/d/0/7d0b5166-6a8a-418a-addd-95ee9b046994/GenevaFrameworkWhitepaperForDevelopers.pdf>
 - ▶ Télécharger l’ensemble des livres-blancs et la fiche produit “Geneva”
 - ▶ <http://www.microsoft.com/downloads/details.aspx?FamilyID=9ca5c685-3172-4d8f-81cb-1a59bdc9f7e3&displaylang=en>
- ▶ Forum MSDN “Geneva”
 - ▶ <http://social.msdn.microsoft.com/Forums/en-US/Geneva/threads/>
- ▶ Blog “Geneva” team
 - ▶ <http://blogs.msdn.com/card/default.aspx>

Pour aller plus loin

- ▶ Centre de développement MSDN sur “Geneva”
 - ▶ <http://www.microsoft.com/geneva>
 - ▶ Sessions Web MSDN
 - ▶ “Geneva” Server and Framework Overview (niveau 300)
 - ▶ <https://msevents.microsoft.com/CUI/EventDetail.aspx?EventID=1032394338&culture=en-US>
 - ▶ “Geneva” Deep Dive (niveau 400)
 - ▶ <https://msevents.microsoft.com/CUI/EventDetail.aspx?EventID=1032394340&culture=en-US>
 - ▶ Windows CardSpace “Geneva” Under the Hood (niveau 400)
 - ▶ <https://msevents.microsoft.com/CUI/EventDetail.aspx?EventID=1032394342&culture=en-US>

Pour aller plus loin

- ▶ “Geneva” sur Microsoft Connect

- ▶ <http://go.microsoft.com/fwlink/?LinkId=122266>

- ▶ Quelques articles/livres-blancs

- ▶ “Geneva” Server Overview

- ▶ Getting Started with “Geneva” Server

- ▶ <https://connect.microsoft.com/content/content.aspx?ContentID=10105&SiteID=642>

- ▶ Guides “Geneva” Server How-To

- ▶ <https://connect.microsoft.com/Downloads/DownloadDetails.aspx?SiteID=642&DownloadID=14705>

- ▶ Initial Configuration of “Geneva” Server, Adding an Identity Provider to “Geneva” Server, Adding a Relying Party to “Geneva” Server, Adding Claims and Claim Rules to “Geneva” Server, Configuring “Geneva” Server for Windows CardSpace Clients, etc.

Informations additionnelles

- Suite aux discussions sur le blog Kim Cameron sur l'identité

- <http://www.identityblog.com>

- « The Laws of Identity »

- <http://www.identityblog.com/?p=354>

- « The Identity Metasystem »

- <http://www.identityblog.com/?p=355>

- « A Privacy-Compliant Identity Metasystem »

- http://www.identityblog.com/wp-content/resources/Identity_Metasystem_EU_Privacy.pdf



- Et le numéro de 16 du Journal d'architecture

- <https://www.msarchitecturejournal.com/Default.aspx>



Informations additionnelles

▶ Autres blogs

▶ Blog Stefan Brands

▶ <http://www.idcorner.org>

▶ Blog Don Schmidt : des on Federated Identity ... less is more

▶ <http://identity-des.com>

▶ Blog Mike Jones : Self-issued

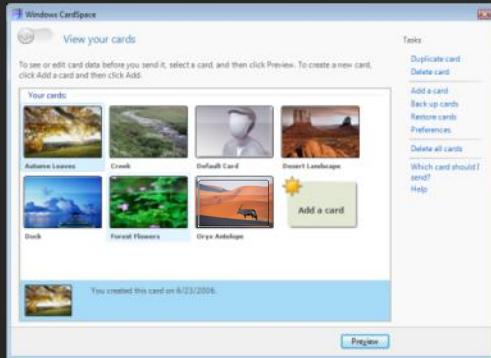
▶ <http://self-issued.info>

▶ Blog Vibro.NET

▶ <http://www.cloudidentity.net>

Questions / Réponses

Utilisation d'une carte managée



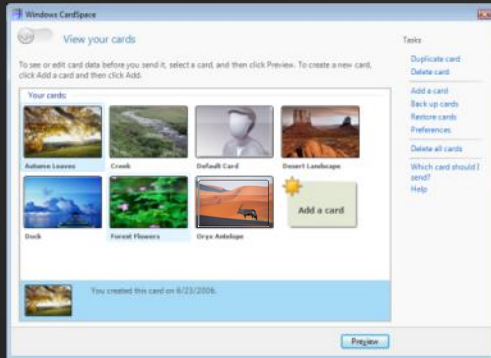
Sujet



Consommateur
d'identité

- ▶ Le consommateur d'identité précise les attributs dont il a besoin (liste et éventuellement issuer)

Sélection d'une carte



Sujet



- Le sujet sélectionne une carte compatible avec les demandes du consommateur d'identité



Consommateur d'identité

Sélection d'une carte

Sujet



Auth':
X509, Kerb, SIC, U/PWD
...



Fournisseur d'identité



Consommateur
d'identité

Demande d'un jeton

- ▶ Le sujet précise au fournisseur d'identité les attributs désirés



Transmission du jeton

Sujet

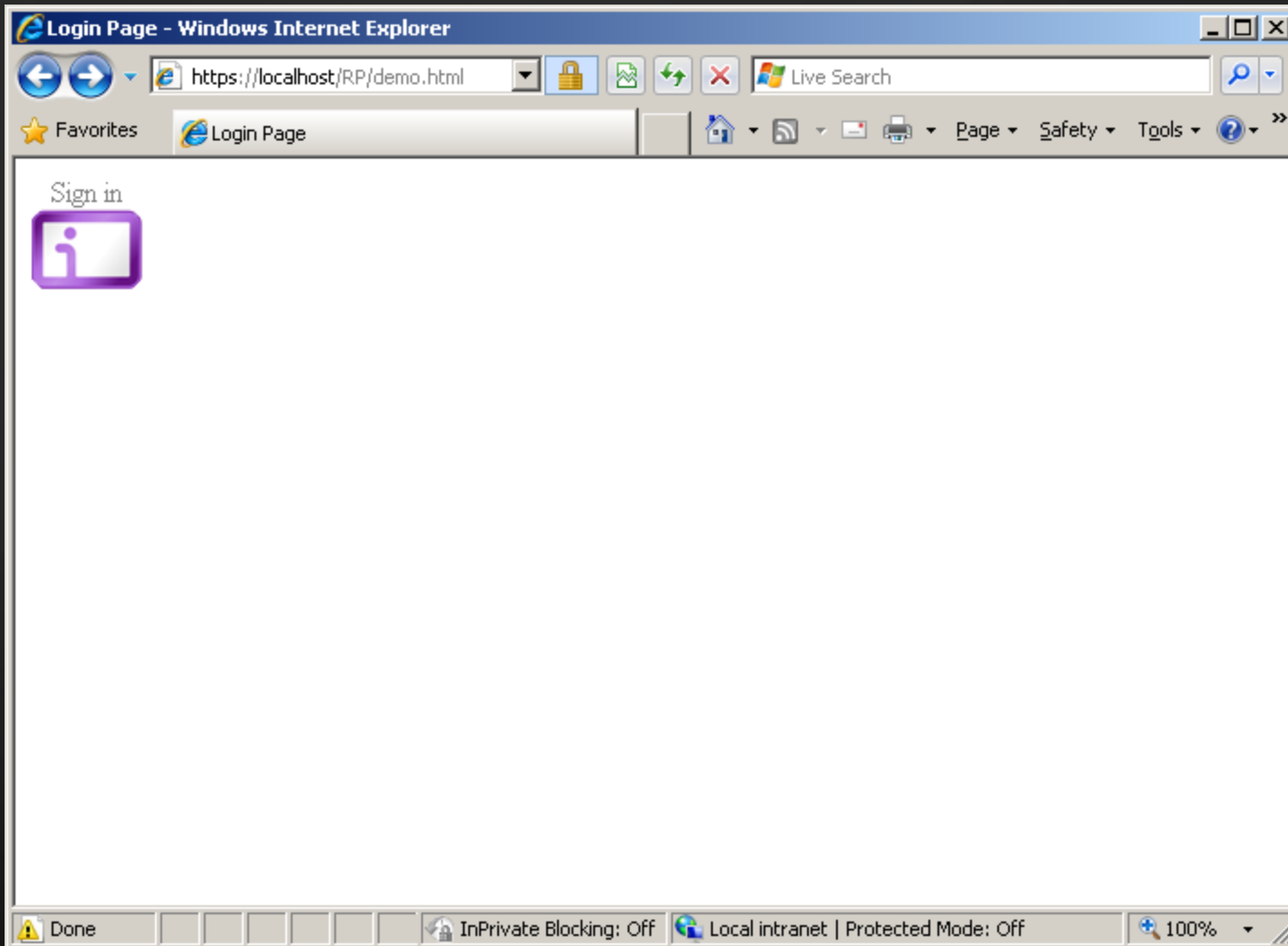


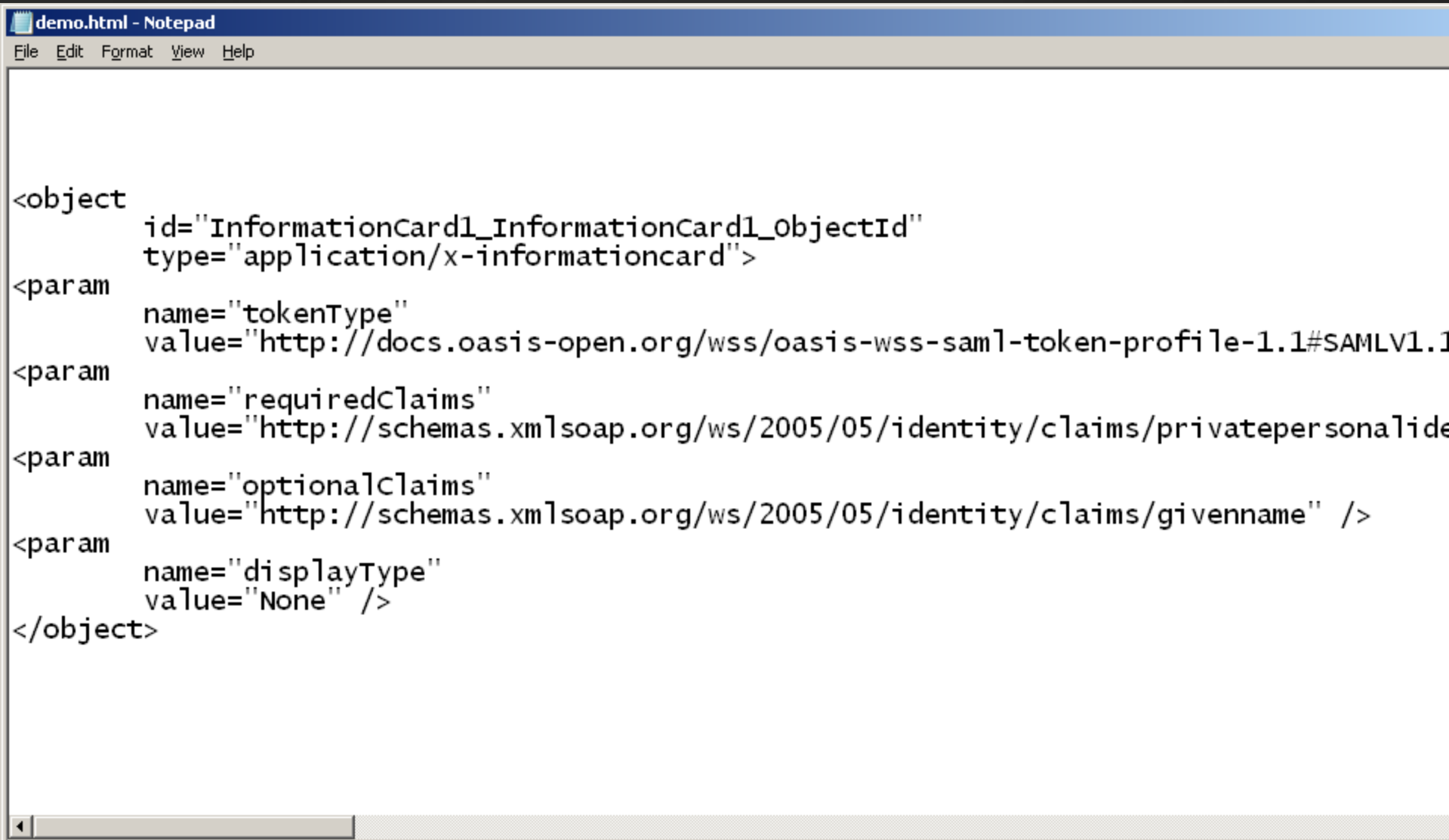
Fournisseur d'identité



Consommateur
d'identité

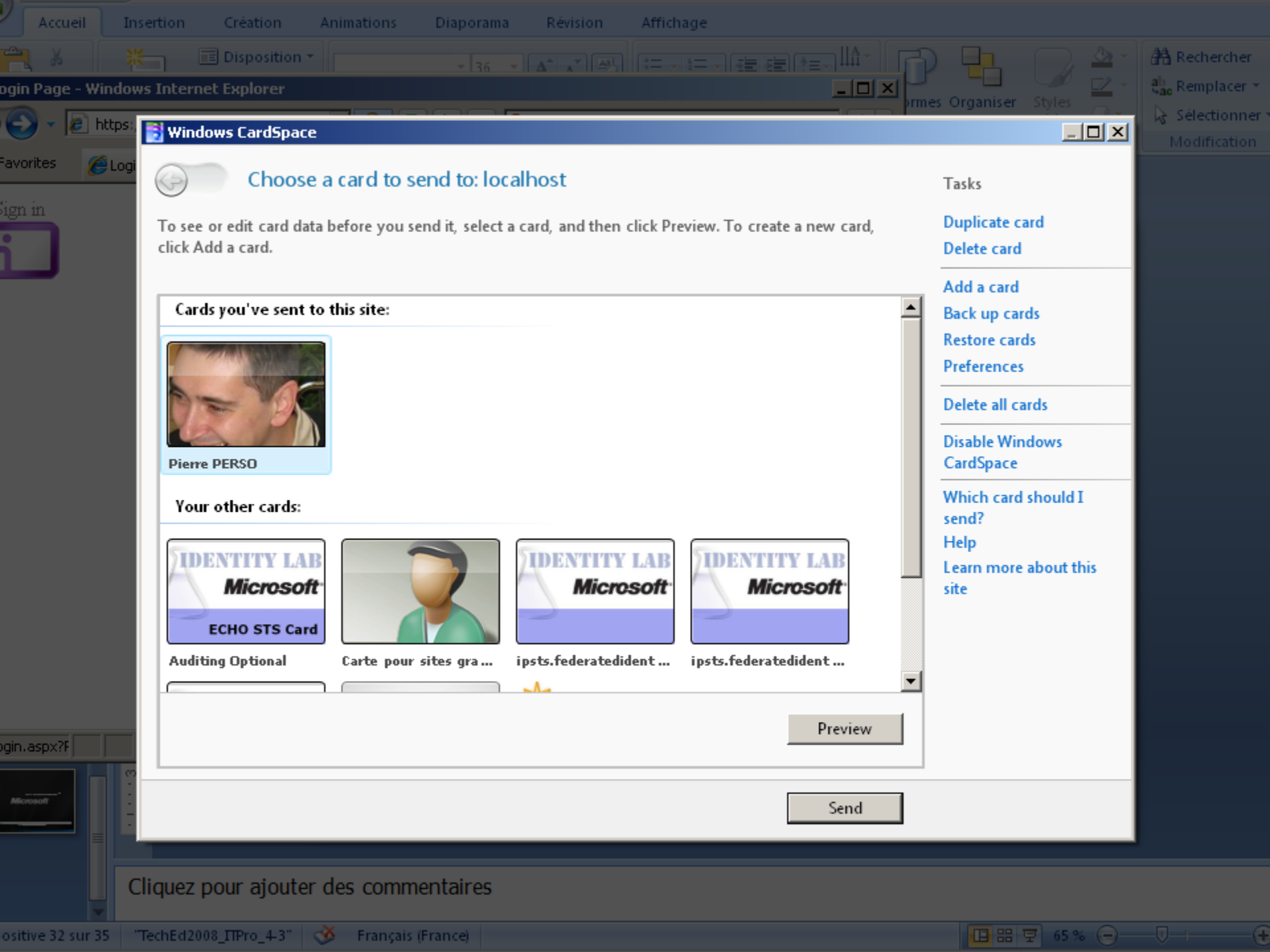
Identification via Cardspace - vu par l'utilisateur





```
demo.html - Notepad
File Edit Format View Help

<object
  id="InformationCard1_InformationCard1_ObjectId"
  type="application/x-informationcard">
  <param
    name="tokenType"
    value="http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV1.1" />
  <param
    name="requiredClaims"
    value="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/privatepersonalidentifier" />
  <param
    name="optionalClaims"
    value="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname" />
  <param
    name="displayType"
    value="None" />
</object>
```



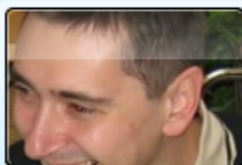
Windows CardSpace



Choose a card to send to: localhost

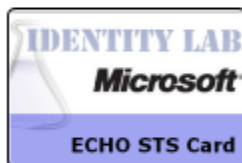
To see or edit card data before you send it, select a card, and then click Preview. To create a new card, click Add a card.

Cards you've sent to this site:



Pierre PERSO

Your other cards:



Auditing Optional



Carte pour sites gra ...



ipsts.federatedident ...



ipsts.federatedident ...

Preview

Send

Tasks

[Duplicate card](#)

[Delete card](#)

[Add a card](#)

[Back up cards](#)

[Restore cards](#)

[Preferences](#)

[Delete all cards](#)

[Disable Windows CardSpace](#)

[Which card should I send?](#)

[Help](#)

[Learn more about this site](#)

Cliquez pour ajouter des commentaires

Windows CardSpace

Do you want to send this card to: localhost

Review the data that this site is requesting. To edit the data, name, and picture for this card click Edit.

Pierre PERSO

Personal Card

12/1/2008:

www.sitededemo.fr

11/30/2008:

www.sitededemo.fr

1/15/2009:

www.identityblog.com

3/12/2009:

localhost

2/5/2009:

www.fabrikam.com

Card data that will be sent to this site:

Fields marked with an asterisk (*) are required

* Site-specific card ID: 33L-3B62-Y2B

Recent card history (not sent):

Additional card details (not sent):

Created On: 11/30/2008

☐ Include optional data

Tasks

[Edit card](#)

[View card history](#)

[Lock card](#)


[What data will be sent?](#)

[Help](#)

Send

Edit

Windows CardSpace

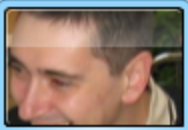
 Do you want to send this card to: localhost

Review the data that this site is requesting. To edit the data, name, and picture for this card click Edit.

Tasks

Edit card
View card history
Lock card

What data will be sent?
Help


Pierre PERSO

Personal Card

Card data that will be sent to this site:

Fields marked with an asterisk (*) are required

First Name: Pierre

* Site-specific card ID: 33L-3B62-Y2B

Recent card history (not sent):

12/1/2008:	www.sitededemo.fr
11/30/2008:	www.sitededemo.fr
1/15/2009:	www.identityblog.com
3/12/2009:	localhost
2/5/2009:	www.fabrikam.com

Additional card details (not sent):

Created On: 11/30/2008

☒ Include optional data

Send

Edit

Votre potentiel, notre passion TM

Microsoft[®]

© 2009 Microsoft Corporation. All rights reserved. Microsoft, Windows, Windows Vista and other product names are or may be registered trademarks and/or trademarks in the U.S. and/or other countries. The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.