

Identity Federation

Daniel Meyer
 Identity and Access Management Lead, EMEA
 Microsoft EMEA HQ

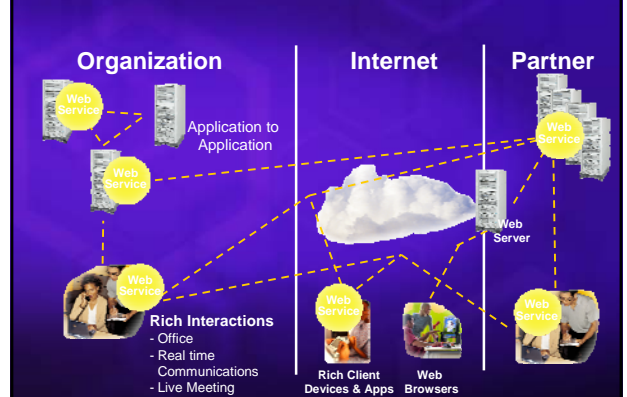
Agenda

- Federation - Why?
- General Concepts
- ADFS – Overview

What changed?



Services as Identities



Extranets Proliferate User Accounts



The Business Drivers



Agenda

- Federation - Why?
- General Concepts
- ADFS – Overview

Identity Federation Goals

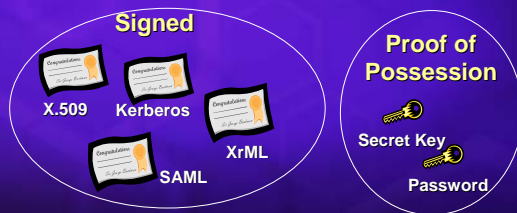
- **Projecting** user Identity from a single logon ...
- **Providing** distributed authentication & claims-based authorization ...
- **Connecting** islands (across security, organizational or platform boundaries) ...
- **Enabling** web single sign-on & simplified identity management

Security Tokens & Claims

Distributed authentication/authorization

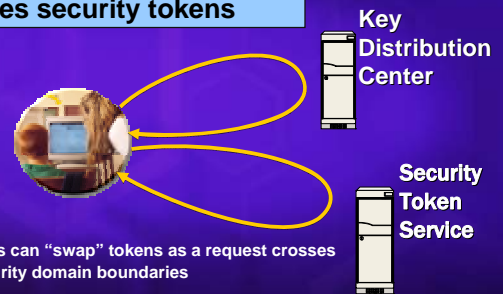
Security tokens assert claims

Claims – Statements authorities make about security principals (name, identity, key, group, privilege, capability, etc).



Security Token Service

A security token service issues security tokens



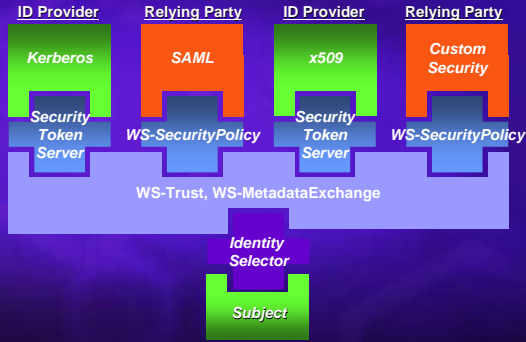
Tokens in the Real World



Main benefits of a Federation Architecture

IT/Helpdesk Efficiency	End User Productivity	Security	Regulatory Compliance
<ul style="list-style-type: none"> • No active external user accounts • No external user password resets • May need shadow accts 	<ul style="list-style-type: none"> • One account • One password • One logon 	<ul style="list-style-type: none"> • Automatic termination of external user access • No risk from orphaned external user accounts 	<ul style="list-style-type: none"> • No accounts for external users protects privacy • Out-bound auditing of external user access

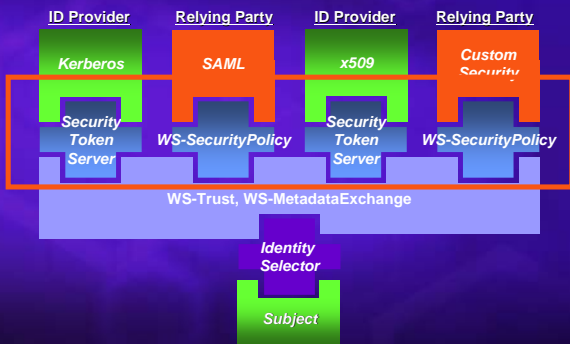
WS-* Metasystem Architecture



Agenda

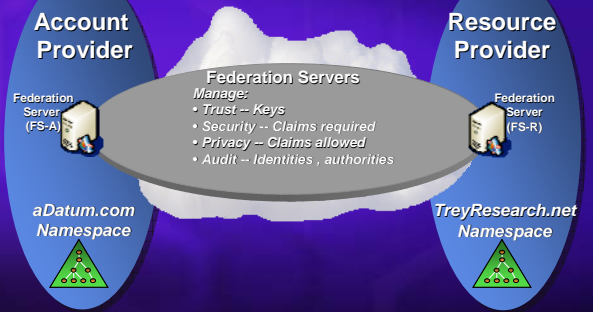
- Federation - Why?
- General Concepts
- ADFS – Overview

WS-* Metasystem Architecture

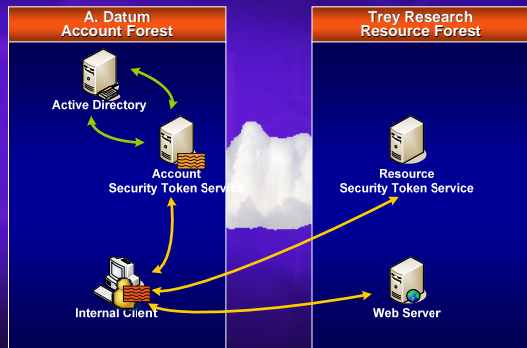


ADFS Identity Federation

Projects AD Identities to other security realms



ADFS Authentication Flow

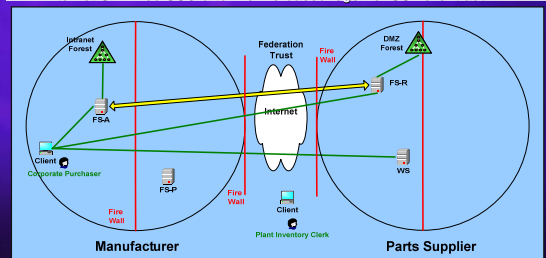


B2B: Federated Web SSO

Partners do NOT need local accounts

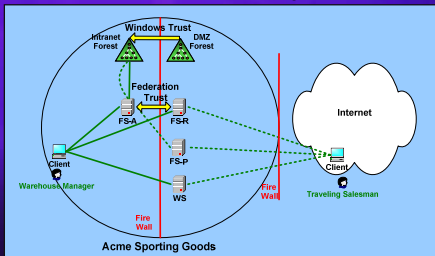
Web-based Purchasing & Inventory Control apps

- Partner employees use their corporate AD accounts
- Intranet UX: Web SSO after Windows desktop logon
- Internet UX: Web SSO after Forms-based logon or SSL client authN



B2E: Web SSO + Forest Trust

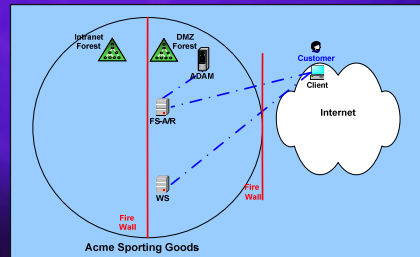
- Single sign-on for HQ & "Road Warrior" users
- Web-based Wholesale Order Entry app in DMZ
- All employees have accounts in intranet AD
 - Intranet UX: Web SSO after Windows desktop logon
 - Internet UX: Web SSO after Forms-based logon or SSL client.authN



B2C: Classic Web SSO

Classic Web SSO for Internet customers

- Web-based Retail Order Entry & Customer Service apps
- Customers issued user accounts in DMZ (AD or ADAM)
 - Internet UX: Web SSO after Forms-based logon



ADFS Security Tokens

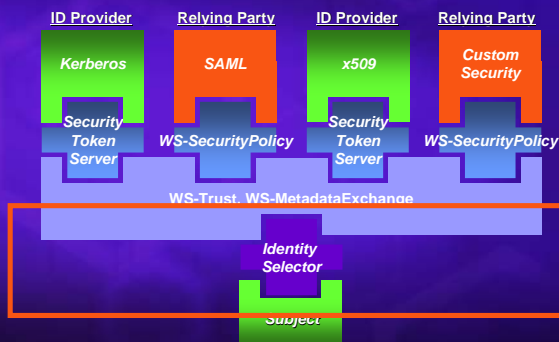
- SAML 1.1 assertion syntax
 - WS-Trust RequestSecurityTokenResponses
- Tokens are not encrypted
 - All messages are over HTTPS
- Tokens are signed
 - Vendor interoperable (default)
 - Signed with RSA Private key and signature verified with public key from X.509 certificate
 - ADFS internal key management (optional)
 - FS-R tokens for Web Agent can be signed with Kerberos session key

Shibboleth Interoperability

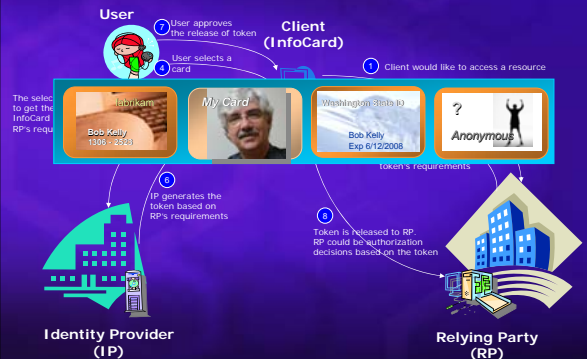
Shibboleth project sponsored by Microsoft and ADFS

- Shibboleth System 1.3 release
- Developing plug-ins for SAML 1.1 Identity and Service Providers
 - Support WS-Federation Passive Requestor Interoperability Profile
 - Enables Interop with ADFS and other compliant vendor products
- Shibboleth Beta version available now
- Need "qualified" customers for testing

WS-* Metasystem Architecture



CardSpace - End-to-end



What's in a Card?

Name: Alice's Book Club Card
 Expires: 9/15/2006
 Image
 Issuer: Fabrikam
 Supported Claims: {
 GivenName
 LastName
 Address
 City
 ...
 }
 Issuer Token Service EPRc
 Supported Token Type: {
 SAML 1.1
 ...
 }



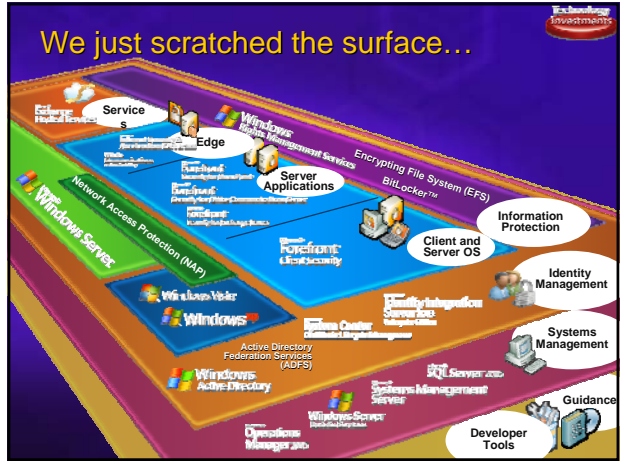
Alice's Book Club Card

claim values are owned by Identity Provider



Identity Provider

We just scratched the surface...



Microsoft
 Your potential. Our passion.™