

Understanding CardSpace in an Enterprise Setting

September 2006

Presented by:
Patrick Harding
CTO
Ping Identity Corporation

PingIdentity™

Agenda

- Federation in the Enterprise Today
- Why CardSpace in the Enterprise?
- Sample Scenarios
- Demo

Federation Today

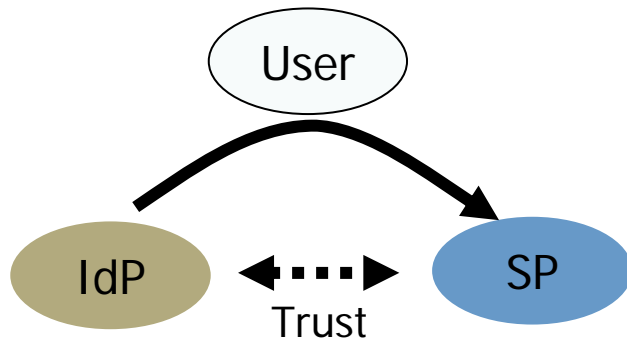
- Protocol Wars are Over – SAML 2.0 and WS-Federation
- Enterprise Federation Hubs Have Enabled 5 - 10 Spokes
 - ▶ The Value of Federation Has Been Justified
- Common Enterprise Scenarios Have Become Apparent
 - ▶ Employee SSO to ASP's
 - ▶ Business Partner SSO to Enterprise Apps
 - ▶ ASP's and Portals Seamlessly Integrating 3rd Party Services

What is CardSpace?

- CardSpace is the New Digital Identity Initiative in Vista
- A New, Secure Visual Metaphor for Managing identity Information and Performing Online Authentication
- In an Enterprise Context it's the Digital Equivalent of Your Employee Badge
- Enables Active Federation

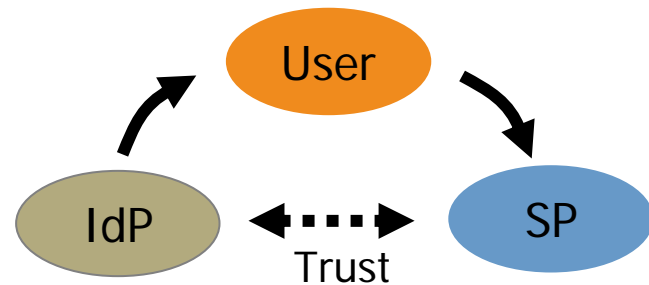
Passive & Active Federation

Passive Federation



SAML 2.0 Web SSO Profiles, WS-Federation

Active Federation



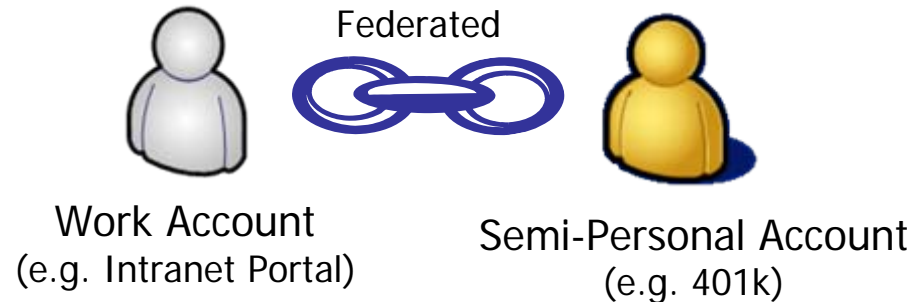
Microsoft CardSpace, Higgins, SAML 2.0 ECP

Passive and Active Federation Work Together to Enable a Myriad of Different Business Use Cases

Why CardSpace?

- Self-Asserted Identity Information
- Standard Identity and Authentication UI Metaphor
- User Actively Controls Flow of Identity Information
- User Manages Privacy and Consent During the Federation Process

Scenario 1: Mixing Privacy Domains



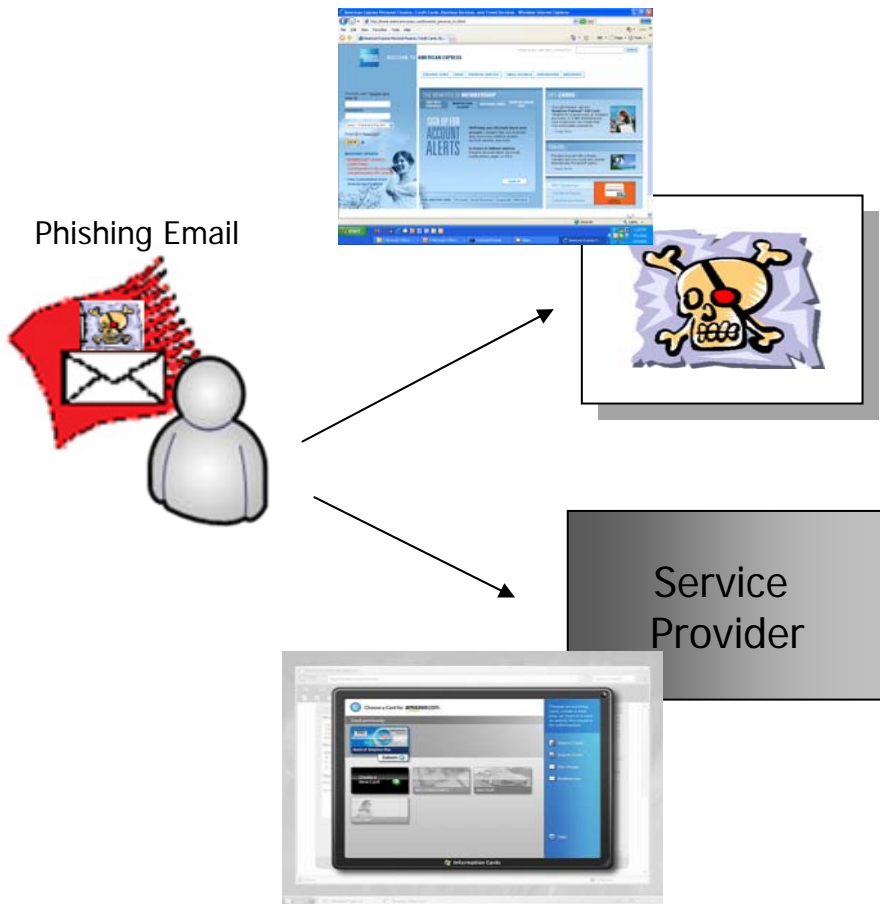
- Employer Enables Federated SSO Between Work Accounts and Semi-Personal Accounts
- CardSpace Enables Employees to Choose Whether or Not to Use Federated SSO

Scenario 2: IdP Selection/Discovery



- Passive Federation handles IdP Selection/Discovery poorly
- CardSpace Enables User Controlled IdP Selection

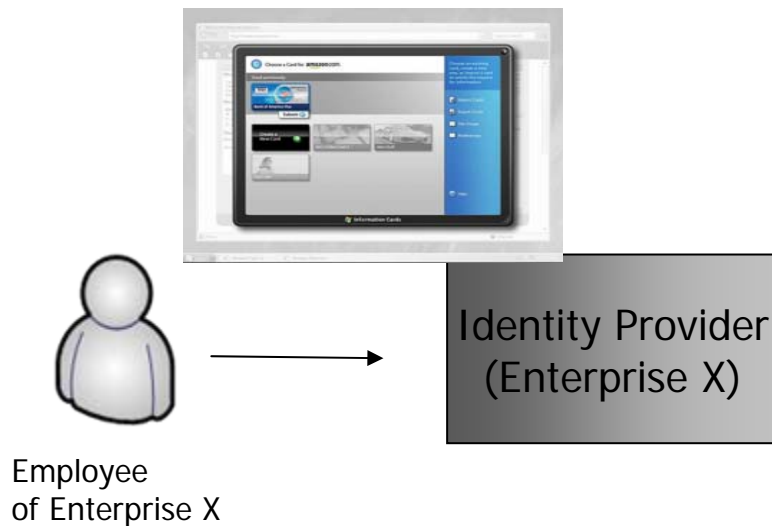
Scenario 3: Reduce Phishing Risks



- Employees Are at Risk of Phishing Attacks
- CardSpace Enables a Secure, Graphically Distinct Authentication Mechanism to Prevent Today's Phishing Attacks

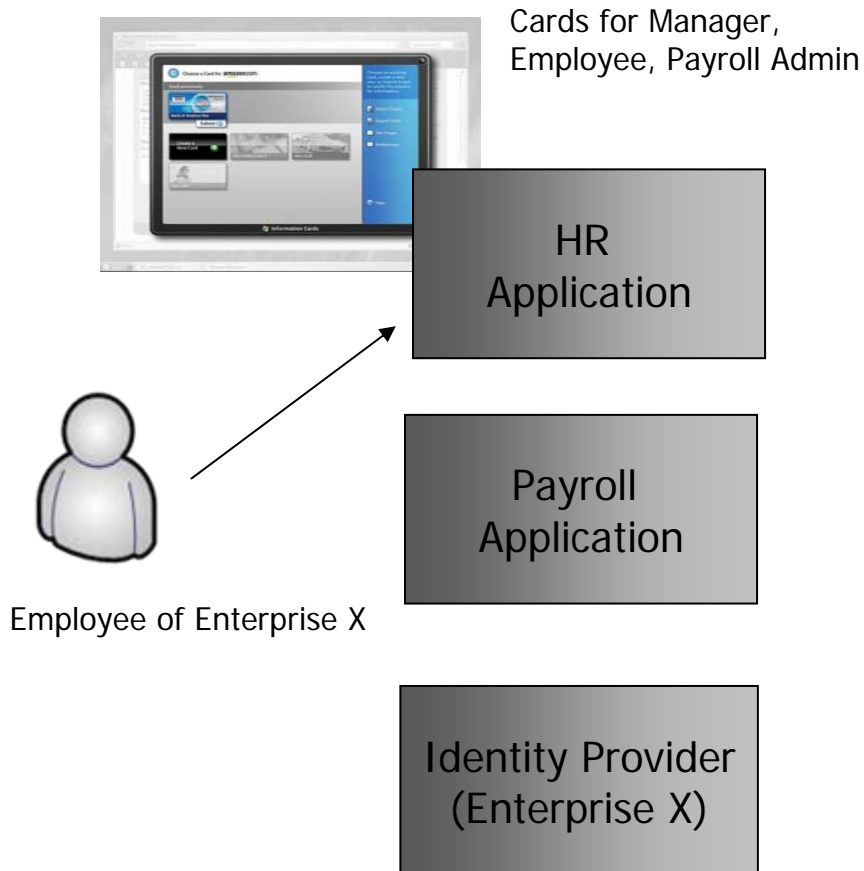
Scenario 4: Strong Authentication

Cards for Password, One Time Password, X.509 Certificate



- Employees are required to leverage alternate stronger forms of authentication
- CardSpace enables a Standard UI Metaphor for All Authentication Mechanisms

Scenario 5: Role Management



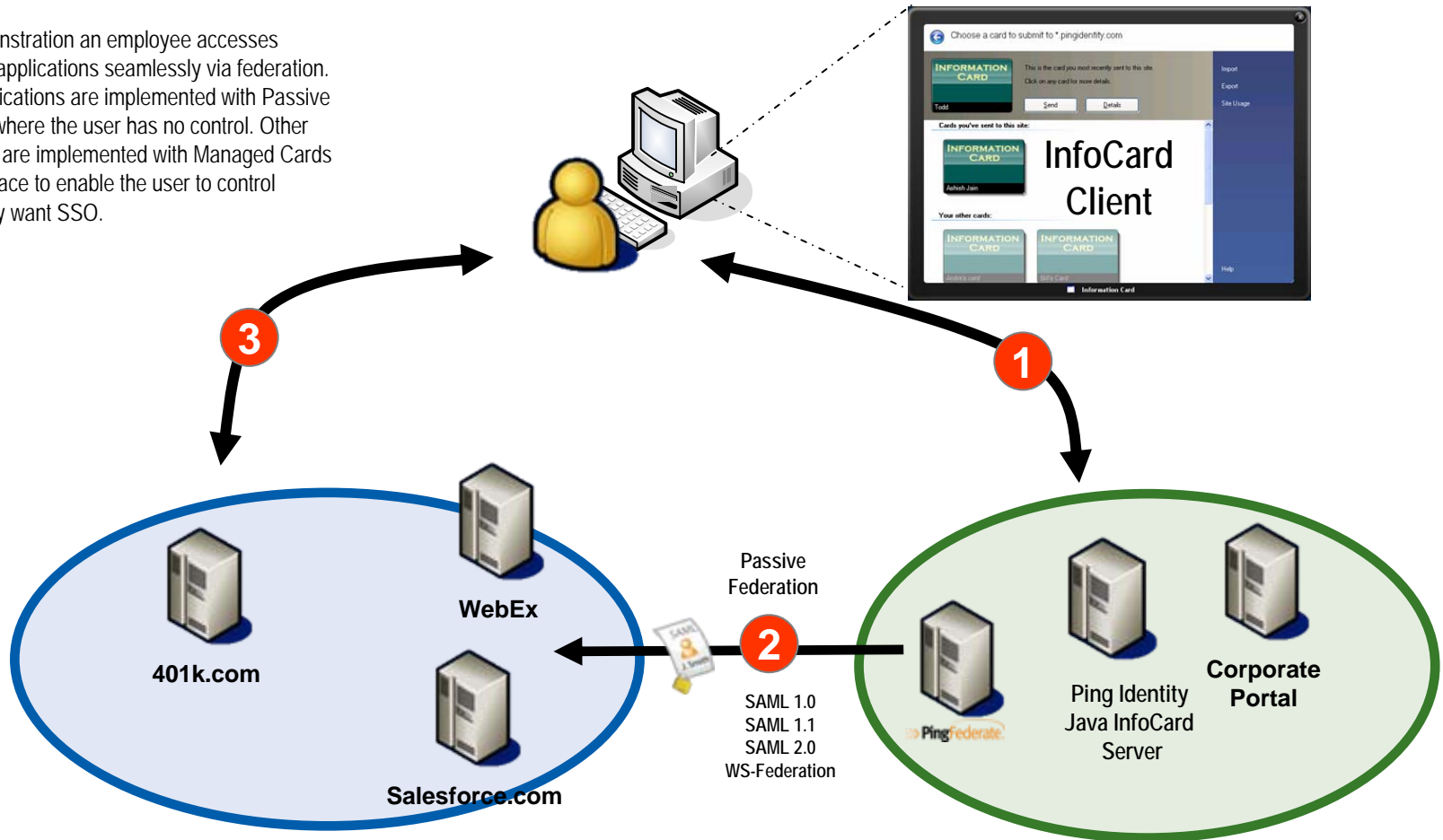
- Employees maintain different roles within the enterprise
- CardSpace Allows User to Choose Different Roles for Accessing Different Applications
- Different Cards can Represent Different Corporate Roles
- Simplifies Delegation

CardSpace Managed IdP/STS

Demo

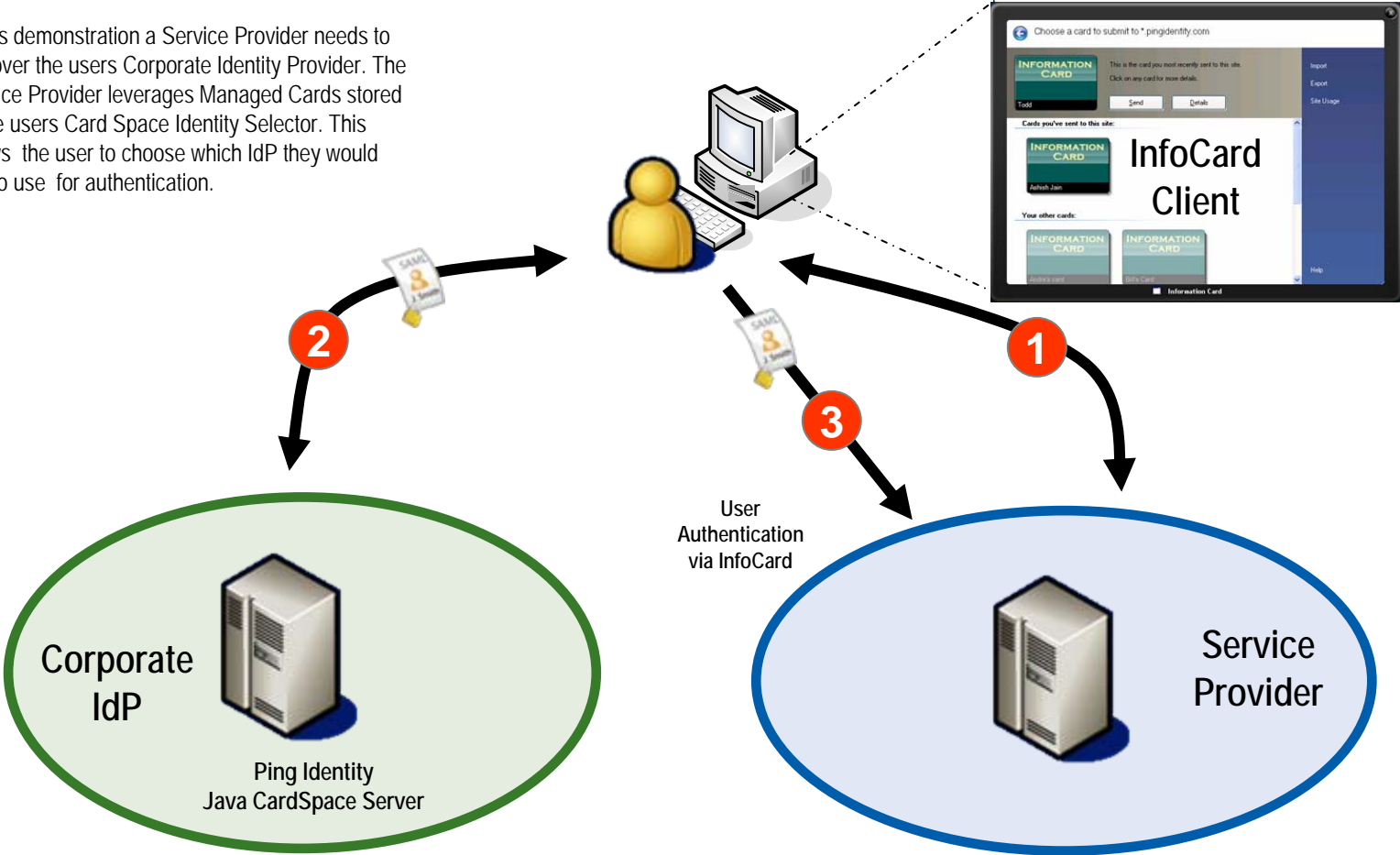
Demo – Scenario 1

In this demonstration an employee accesses outsourced applications seamlessly via federation. Certain applications are implemented with Passive Federation where the user has no control. Other applications are implemented with Managed Cards and CardSpace to enable the user to control whether they want SSO.



Demo - Scenario 2

In this demonstration a Service Provider needs to discover the users Corporate Identity Provider. The Service Provider leverages Managed Cards stored in the users Card Space Identity Selector. This allows the user to choose which IdP they would like to use for authentication.



1. The Service Provider causes a managed Card to be presented to the user.
2. User authenticates to Corporate IdP and An industry-standard SAML token is created
3. The SAML token is used to create a session at the Service Provider

Understanding CardSpace in an Enterprise Setting

September 2006

Presented by:
Patrick Harding
CTO
Ping Identity Corporation

PingIdentity™