Single Sign-on and Identity Management

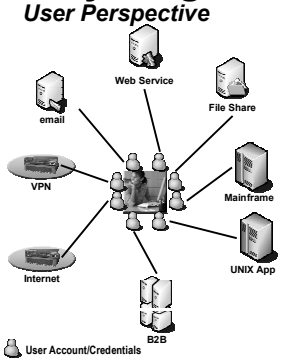
Joe Donahue
Federal Program Manager
Directory Services
Microsoft

Agenda

- Why Single Sign-on
- The Challenges of SSO
- Implementing SSO today
  - Windows SSO
  - Reduced Sign-on (Enterprise SSO)
  - Web SSO (B2E, B2B & B2C)
- Microsoft Identity Roadmap

Why Single Sign-on

User Perspective



The Problem

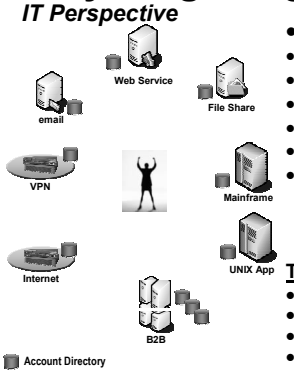
- Too many credentials
- Which one for which app
- Multiple logons

The Business Impact

- Increases risk of compromise
- Reduced productivity
- Increased helpdesk expenses

Why Single Sign-on

IT Perspective



The Problem

- Provisioning new accounts
- Password management
- Auditing user activity
- De-provisioning users
- Managing non-employee access
- Deploying Enterprise Applications

The Business Impact

- People Intensive
- Delayed access for new hires
- Risk of unauthorized access
- No single view of the user

The Challenges

- **Multiple Platforms and Application Models**
  - Windows Server, multiple versions of UNIX, OS390, AS400
  - Legacy & custom applications
  - Web applications and services
  - Network gateways (VPN, Wireless, Internet)
- **Different Security Mechanisms**
  - Kerberos
  - Basic Authentication
  - X.509 Certificates
  - Passport
  - Proprietary (eg database lookups)
- **Multiple Account Directories**
  - Active Directory
  - LDAP
  - Databases
  - Application integrated
- **Complexities with B2B and B2C**
  - Concerns about mixing partner & customer accounts with employee accounts
  - Privacy (outbound) as well as security (inbound) concerns
  - Are external users & their entitlements up to date?
  - Day to day management issues (eg password reset)

Implementing Single Sign-on Today

Windows Single Sign-on	❑ Active Directory – The foundation for Identity management ❑ Windows Integrated Applications ❑ Network Single Sign-on with Windows Server
Reduced Enterprise Sign-on	❑ Extending Windows SSO to non-integrated applications ❑ Using Active Directory for LDAP authentication ❑ The role of Microsoft Metadirectory Server (MMS) ❑ Active Directory in Application Mode (ADAM) usage
Web Single Sign-on	❑ B2E using Active Directory and IIS ❑ B2C using Active Directory and Passport ❑ Extranet Access Management using Active Directory

© 2002 Microsoft Corporation. All rights reserved.
This presentation is for informational purposes only. Microsoft makes no warranties, express or implied, in this summary.

Implementing Single Sign-on Today

Windows Single Sign-on	❑ Active Directory – The foundation for Identity management ❑ Windows Integrated Applications ❑ Network Single Sign-on with Windows Server
Reduced Enterprise Sign-on	❑ Extending Windows SSO to non-integrated applications ❑ Using Active Directory for LDAP authentication ❑ The role of Microsoft Metadirectory Server (MMS) ❑ Active Directory in Application Mode (ADAM) usage
Web Single Sign-on	❑ B2E using Active Directory and IIS ❑ B2C using Active Directory and Passport ❑ Extranet Access Management using Active Directory

Windows Single Sign-on

Active Directory – Foundation for Identity Management

Central Repository for:
- User Accounts & Attributes
- System Accounts & Attributes
- Organizational & Security Groups
- Application & Service Locations
- Management Policy
- Security Policy
- Digital Certificates
- Network Access Permissions
- Printer Locations
- File Shares Locations

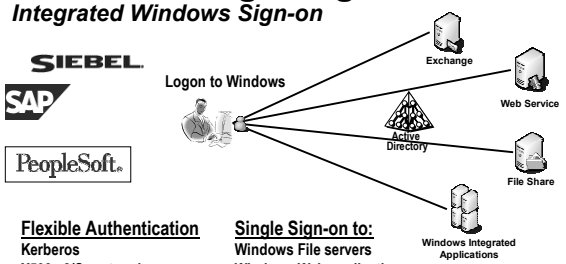
...

Integrated Security
- Kerberos v5
- x.509 Certificates (PKI)
- Security Domain

Directory Access Protocols
- LDAP v3 – Standards-based access
- ADSI – Simple COM-based Interface
- DSML – XML Interface

Windows Single Sign-on

Integrated Windows Sign-on

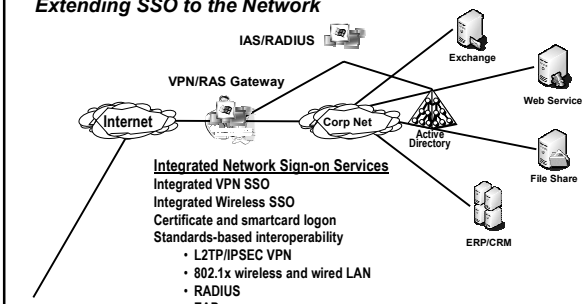


Flexible Authentication
Kerberos
X509 v3/Smartcard
Biometrics
Passport (Web)
Basic (Web)
Digest (Web)

Single Sign-on to:
Windows File servers
Windows Web applications
Exchange email
SQL Server
BizTalk Server
Other Microsoft applications
3rd Party Integrated Apps

Windows Single Sign-on

Extending SSO to the Network



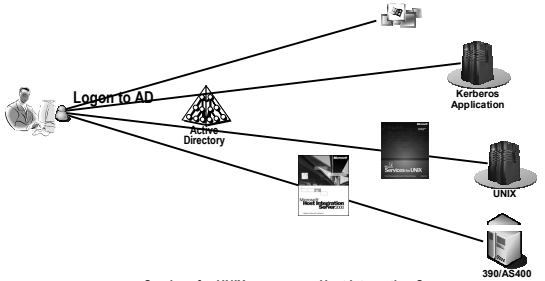
Integrated Network Sign-on Services
Integrated VPN SSO
Integrated Wireless SSO
Certificate and smartcard logon
Standards-based interoperability
- L2TP/IPSEC VPN
- 802.1x wireless and wired LAN
- RADIUS
- EAP
- PEAP (Windows Server 2003)

Implementing Single Sign-on Today

Windows Single Sign-on	❑ Active Directory – The foundation for Identity management ❑ Windows Integrated Applications ❑ Network Single Sign-on with Windows Server
Reduced Enterprise Sign-on	❑ Extending Windows SSO to non-integrated applications ❑ Using Active Directory for LDAP authentication ❑ The role of Microsoft Metadirectory Server (MMS) ❑ Active Directory in Application Mode (ADAM) usage
Web Single Sign-on	❑ B2E using Active Directory and IIS ❑ B2C using Active Directory and Passport ❑ Extranet Access Management using Active Directory

Reduced Enterprise Sign-on

Extending Windows SSO



Kerberos
- Native AuthN protocol
- MIT v5 Compliant
- Carries group info in PAC
- Windows PAC is open

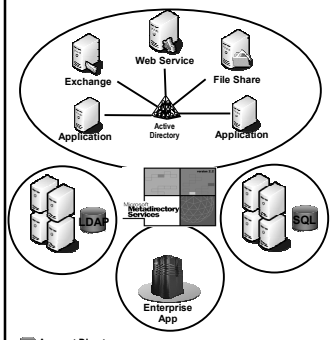
Services for UNIX
- NIS Server for AD
- NIS-AD directory sync
- Password synchronization
- User name mapping

Host Integration Server
- Windows to RACF accounts
- Windows to 0S/400 Security System
- Bi-Directional Password Synchronization

© 2002 Microsoft Corporation. All rights reserved.
This presentation is for informational purposes only. Microsoft makes no warranties, express or implied, in this summary.

Reduced Enterprise Sign-on

LDAP Authentication & Directory Integration



Integrate LDAP with AD

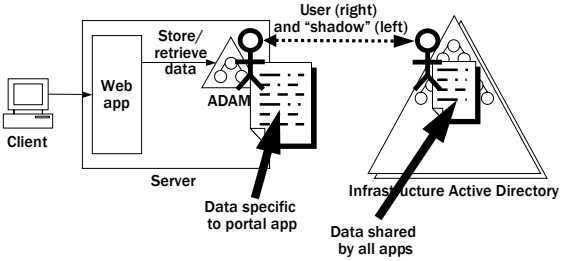
- LDAP v3 compliant
- Single AD and LDAP user account
- ADAM for personalization data

Microsoft Metadirectory Server

- Directory synchronization
  - LDAP (eg iPlanet & others)
  - Relational databases
  - DSML
  - Application specific
- Account Provisioning
  - Automate account creation
  - Automate account de-provisioning
- Password Management (MMS 2003)
  - Self-service password reset
- Certificate Management

ADAM Usage

Integrating extended LDAP app with AD



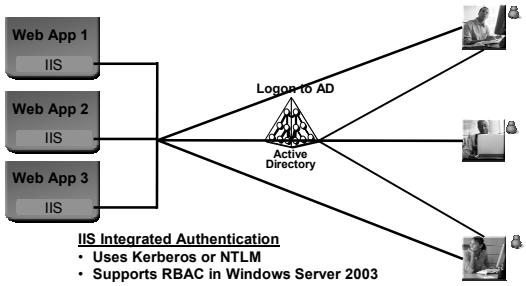
- Store app data without extending infra DS schema
- App data keyed off identifier from infra directory
- Maintain central user repository!

Implementing Single Sign-on Today

Windows Single Sign-on	❑ Active Directory – The foundation for Identity management ❑ Windows Integrated Applications ❑ Network Single Sign-on with Windows Server
Reduced Enterprise Sign-on	❑ Extending Windows SSO to non-integrated applications ❑ Using Active Directory for LDAD authentication ❑ The role of Microsoft Metadirectory Server (MMS) ❑ Active Directory in Application Mode (ADAM) usage
Web Single Sign-on	❑ B2E using Active Directory and IIS ❑ B2C using Active Directory and Passport ❑ Extranet Access Management using Active Directory

Web Single Sign-on

B2E Using Active Directory and IIS

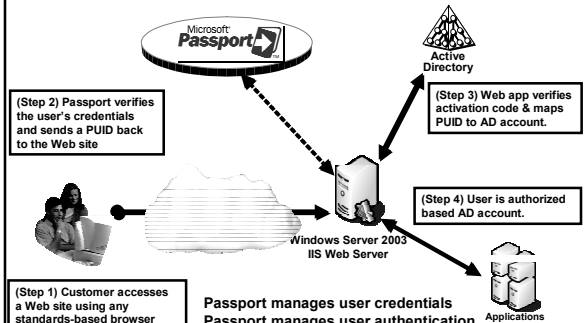


IIS Integrated Authentication

- Uses Kerberos or NTLM
- Supports RBAC in Windows Server 2003
- Supports URL authorization in Windows Server 2003

Web Single Sign-on

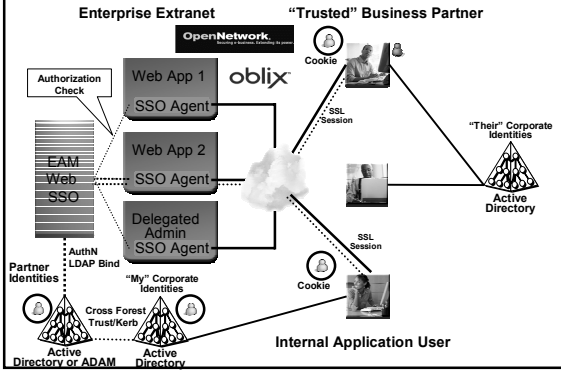
B2C Using Passport and Active Directory



Passport manages user credentials
Passport manages user authentication
You manage user access controls

Web Single Sign-on

Extranet Access Management using AD

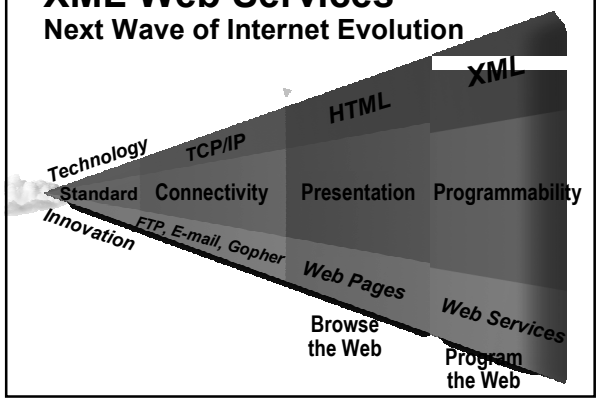


© 2002 Microsoft Corporation. All rights reserved.
This presentation is for informational purposes only. Microsoft makes no warranties, express or implied, in this summary.

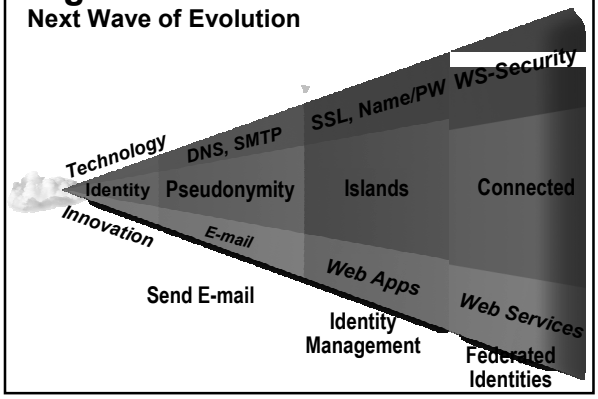
What's Next?

Vision and Roadmap

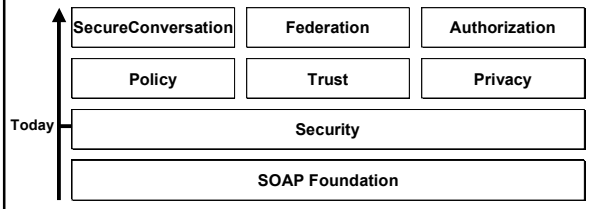
XML Web Services
Next Wave of Internet Evolution



Digital Identities
Next Wave of Evolution



Web Services Security



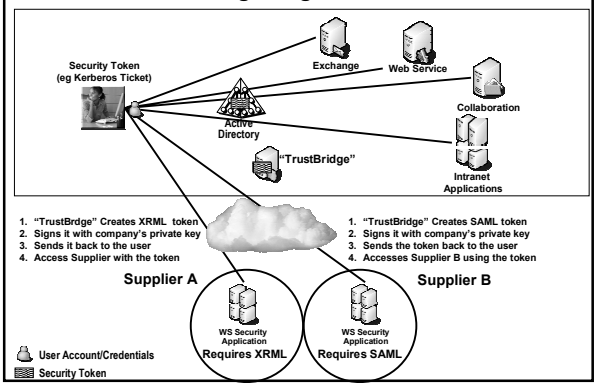
Security in a Web Services World
– IBM/MSFT White Paper

WS-Security Specification
– At OASIS, broad industry support

The Vision of Single Sign-on

- **A *Single* User Identity**
  - **A single corporate identity**
  - **A single consumer identity**
- **Strong multifactor authentication**
  - **Certificates**
  - **Biometrics**
- **Interoperability (client and server)**
  - **Multi-Platform**
  - **Multi-Application**
  - **Multi-Protocol**
- **Federated Authentication and Access**
  - **Single Sign-on that spans businesses**
  - **Single sign-on that spans consumer applications**

The Vision and Future of SSO
B2B Federated Single Sign-on



© 2002 Microsoft Corporation. All rights reserved.
This presentation is for informational purposes only. Microsoft makes no warranties, express or implied, in this summary.

Identity Management Roadmap

- **XML Web Services Specifications**
  - Broad set of specifications to enable federation of Web Services
  - In collaboration with IBM, Verisign, etc.
  - WS-Security working group within OASIS
    - Kerberos, X509v3, SAML and XrML "security tokens"
- **Windows Server 2003 – April 2003**
  - Cross Forest Trust – *Intranet* Federation
  - Native support for Passport authentication
  - Integrated Role-Based Access Control
  - Web Services integration (.NET framework and UDDI)
- **MMS 2003 – Windows Server 2003 + 90 days**
  - Directory Integration & Synchronization
  - Account Provisioning
  - Password Management
  - Single view of a user across the enterprise
- **Active Directory Application Mode – Windows Server 2003 + 90 days**
  - Enables AD to be deployed as a "simple" LDAP directory
  - Used for application specific user information
- **"Jupiter" (e-business server) – Q4 2003**
  - SSO through adapters to enterprise applications
- **Passport Federation Support – H2 2003**
  - Authentication authority for consumer web services
  - Federation support in 2003 based on Web Services
- **"TrustBridge" – TBD**
  - Based on WS-Security for identity interoperability
  - True federated Single Sign-on (no duplicated or mapped ids)
  - Web Security runtime to enable federated applications

Summary

- ***Standardize on a Single Directory Technology***
  - Consolidate LDAP directories with Active Directory
  - Use AD with integrated security for Windows SSO
  - Use AD/AM for application specific user information
- ***Use Kerberos for Interoperability***
  - Industry standard protocol for authentication
  - Native protocol used by Windows Servers and Clients
  - Used by many UNIX-based applications
- ***Use MMS to Simplify Identity Management***
  - Directory integration synchronization
  - Simple Account provisioning
  - Password management
  - Single view of the user across the enterprise
- ***Plan for Federated Identity Management***
  - Utilize Web services standards (XML, SOAP, UDDI)
  - Get familiar with WS-Security
  - "TrustBridge" will enable secure identity federation

Microsoft Government

© 2002 Microsoft Corporation. All rights reserved.
This presentation is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY.

© 2002 Microsoft Corporation. All rights reserved.
This presentation is for informational purposes only. Microsoft makes no warranties, express or implied, in this summary.