Single Sign-on and Identity Management

Joe Donahue
Federal Program Manager
Directory Services
Microsoft

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

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, OS/2, AIX
  - Legacy & custom applications
  - Web applications and services
  - Network gateways (VPNs, 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

- Active Directory – The foundation for Identity management
- Windows Integrated Applications
- Network Single Sign-on with Windows Server
- 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
- B2E using Active Directory and IIS
- B2C using Active Directory and Passport
- Extranet Access Management using Active Directory

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
Implementing Single Sign-on Today

- Active Directory – The foundation for Identity management
- Windows Integrated Applications
- Network Single Sign-on with Windows Server

- 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

- 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
- Active Directory in Application Mode (ADAM) usage

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

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

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

- Windows Integrated Applications
  - BiTalk 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)

Reduced Enterprise Sign-on
Extending Windows SSO

- Kerberos
  - Native Authentications protocol
  - RFT v5 Compliant
  - Cross group info in PAC
  - Windows PAC is open

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

- Host Integration Server
  - Windows to RACF accounts
  - Windows to IBM System z Access
  - Cross-Platform Password Synchronization

Reduced Enterprise Sign-on

- Integrated Network Sign-on
- Remote User
- 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)
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
    - Automatic account creation
    - Automatic 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

- Window 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

Web Single Sign-on
B2E Using Active Directory and IIS

Web App 1
IIS
Logon to AD
IIS Integrated Authentication
- Uses Kerberos or NTLM
- Supports RBAC in Windows Server 2003
- Supports URL authorization in Windows Server 2003

Web App 2
IIS
Web App 3
IIS

Web Single Sign-on
B2C Using Passport and Active Directory

- (Step 1) Customer accesses Web site using any standards-based browser
- Passport manages user credentials
- Passport manages user authentication
- You manage user access controls

- (Step 2) Passport verifies the user’s credentials and sends a PUID back to the Web site

- (Step 3) Web app verifies activation code & maps PUID to AD account.

- (Step 4) User is authorized based AD account.

- (Step 5) Web app verifies protection code & maps PUID to AD account

Web Single Sign-on
Extranet Access Management using AD

Enterprise Extranet
“Trusted” Business Partner

- “My” Corporate Identities
  - Cross Forest Trust/Kerberos
  - SSL Session Cookie

- “Their” Corporate Identities
  - Internal Application User

- Partner Identities
  - Corporate Website

Directory of ADAM

Internal Application User

SSL Session Cookie

Directory of ADAM

Internal Application User

© 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

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

Security in a Web Services World
- IBM/MSFT White Paper
WS-Security Specification
- At OASIS, broad industry support

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

- **Windows Server 2003 – April 2003**
  - Cross Forest Federation
  - Native support for Passport authentication
  - Integrated Role-Based Access Control
  - Web Services integrations (J2EE framework and UDDI)

- **MMS 2003 – Windows Server 2003 + 90 days**
  - Directory integration & synchronization
  - Account Provisioning
  - Password Management
  - Single sign-on of a user across the enterprise

- **Active Directory Application Mode – Windows Server 2003 + 90 days**
  - Enable AD to be deployed as a "virtual" LDAP Directory
  - Used for application-specific user information

- **"Jupiter" (e-business server) – Q4 2003**
  - Used for application-specific user information

- **Passport Federation Support – H2 2003**
  - Authorization and identity for consumer Web sites
  - Federation support in Java 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