Identity Management Strategy and Solutions

Sandeep Sinha

Lead Product Manager

Windows Server Product Management

Microsoft®

HP WORLD 2003

Solutions and Technology Conference & Expo

Agenda

- Business Needs
- Microsoft's Strategy
- Customer Scenarios
- Solution Accelerators
- Customer Examples
- IdM Roadmap
- Next Steps

Business Needs

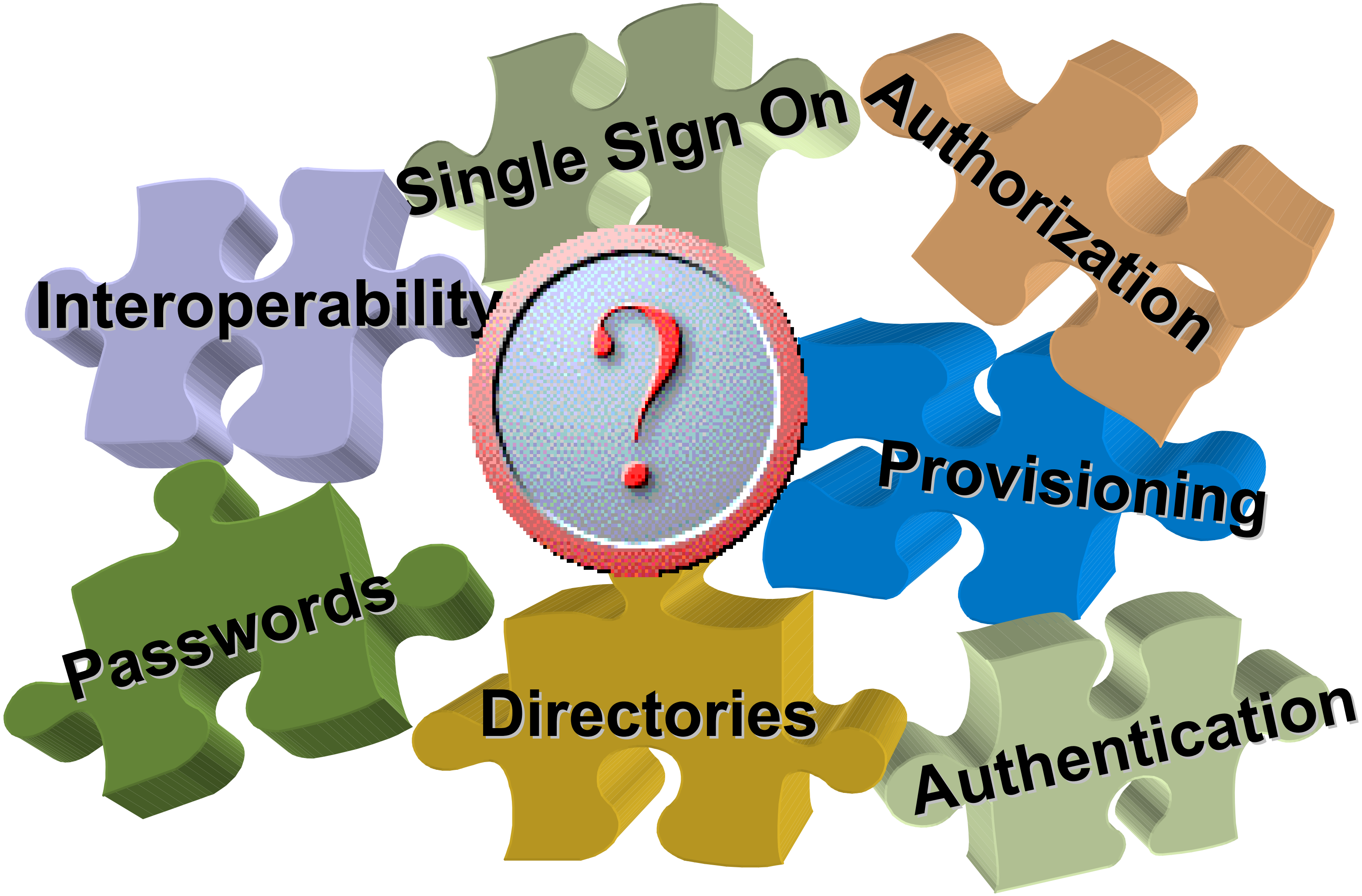
Extended Enterprise	- Integrate Partners in Supply Chain - Connect with Customers - Empower the information workers
Reduce Operational Costs	- Provide self-service capability - Decrease IT Security and Management Costs - Lower application development costs
Improve Security	- Reduce number of userid/password - Reduce De-provisioning risks - Enforce policies and improve audit capability
Regulatory Compliance	- HIPAA - Sarbanes Oxley Act - Gramm-Leach-Bliley

Consider the facts

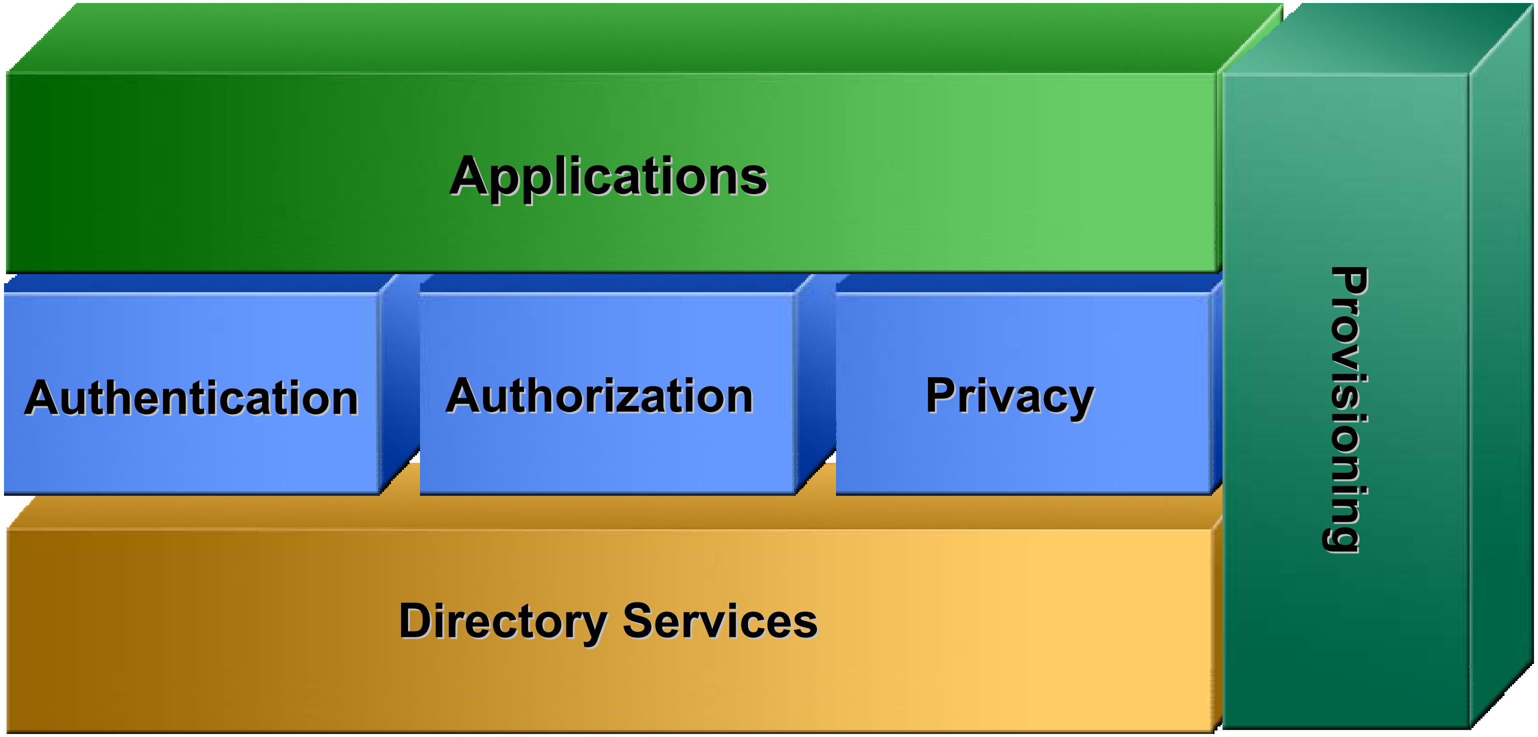
- Too Many User Repository
  - Enterprises have 68 internal and 12 external account stores
  - 75% of internal users and 38% of external users are in multiple stores
- Inefficient Account Provisioning/De-Provisioning
  - User management consumes 34% of the total time IT spends on IdM
  - Users gets provisioned in 16 systems and de-provisioned in 10.
- Impact on User Productivity
  - On average IT is managing access to 73 unique applications requiring user access.
  - Average user spends 16 minutes a day for logins
  - SSO increases user productivity by 15% and efficiency by 18%
- Increasing IT Operational costs
  - 45% of all help desk calls are for p/w resets
  - 15% of users will call help deck for p/w reset
  - Organizations are managing on average 46 suppliers, spending over 1380 hours managing changes to access privilege.

Source: META Group research conducted on behalf of PricewaterhouseCoopers, June 2002; MSFT Internal

The Confusion



Digital Identity Framework



Microsoft’s Approach

Windows Server *Integrated Foundation*

- Directory Services
- Authentication Services
- Authorization Services
- Auditing Infrastructure

Products to Simplify Managing the Identity Lifecycle

- MIIS – Directory Integration & Provisioning
- BizTalk Server – Workflow and Enterprise SSO
- Microsoft Audit Collection System (MACS)

Technology and Services Partnerships

- GSIs – PwC, Unisys, HP, E&Y, CGEY
- ISVs – Oblix, OpenNetwork, Verisign
- IHVs – DigitalPersona, Authentec

Federated Identity and Trust Management through Web Services

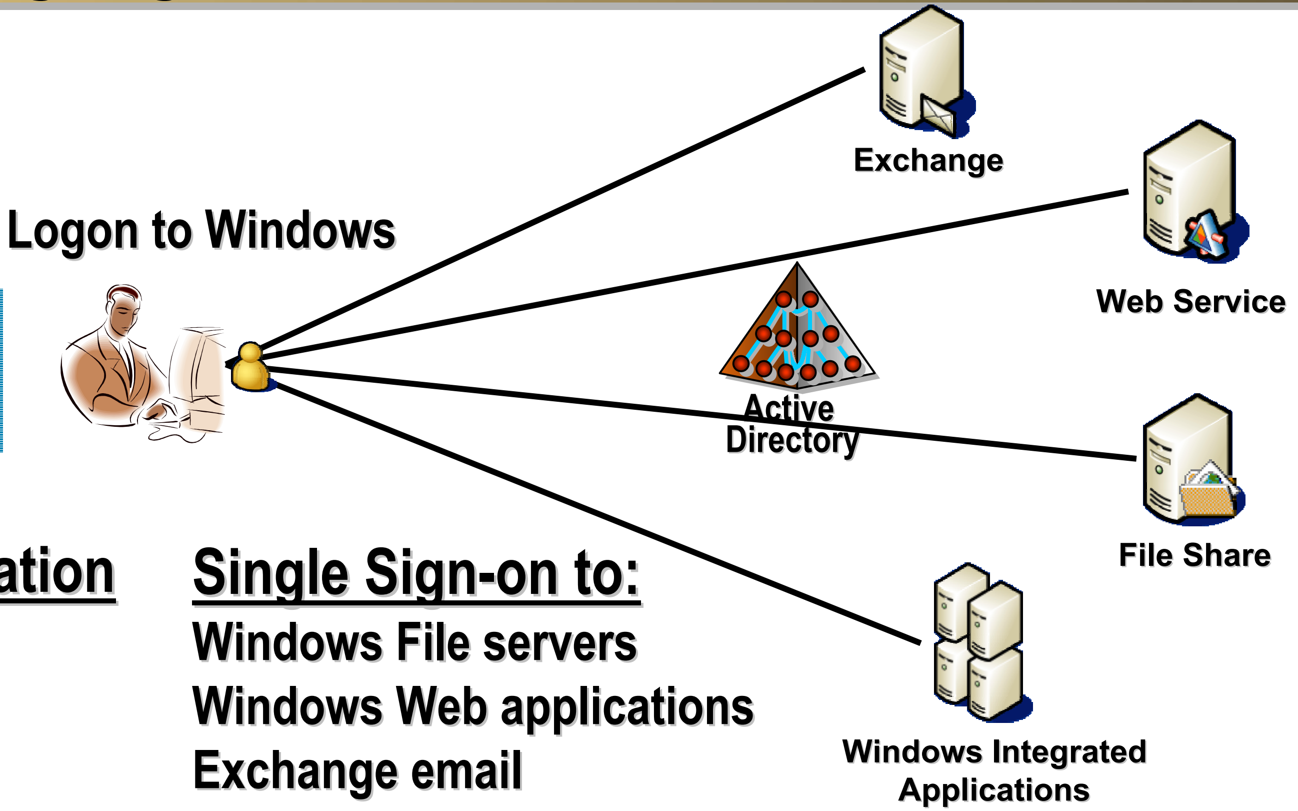
- Standards-based identity interoperability
- Identity and trust federation
- Simplicity

Key Solution Scenarios

Business to Employees	▪ Reduced Sign-on ▪ User provisioning/de-provisioning ▪ Password Management
Business to Customers	▪ Customer Portals – Web Single Sign-on ▪ Customer Self-service ▪ Password Resets
Business to Business	▪ Partner Portal – Web Single Sign-on ▪ Delegated Administration ▪ Partner Self-service

Business To Employee

Integrated Windows Single Sign-on



Flexible Authentication

Kerberos

X509 v3/Smartcard

Biometrics

Single Sign-on to:

Windows File servers

Windows Web applications

Exchange email

SQL Server

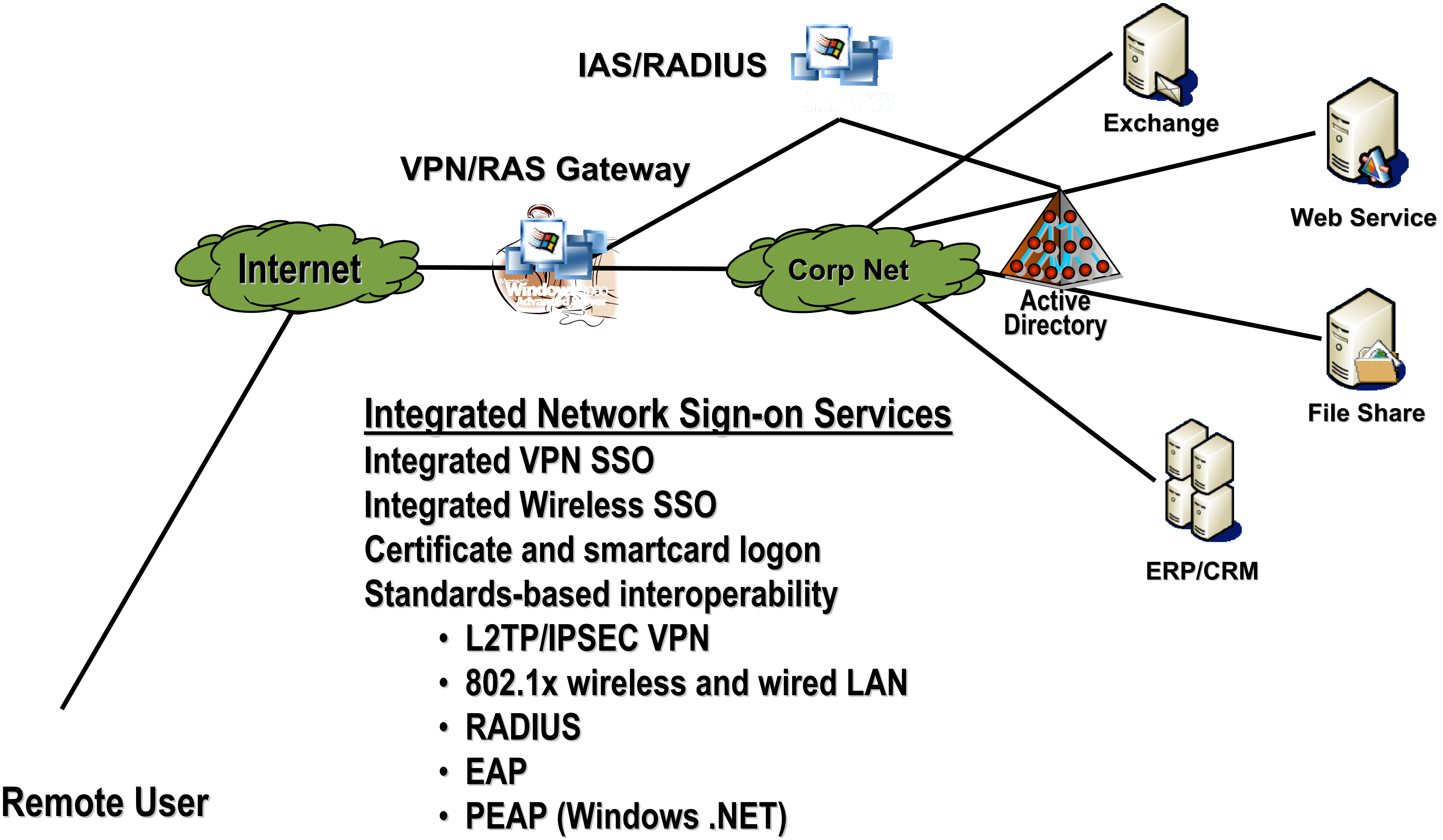
BizTalk Server

Other Microsoft applications

3rd Party Integrated Apps

Business to Employee

Extending SSO to the Network



Integrated Network Sign-on Services

Integrated VPN SSO

Integrated Wireless SSO

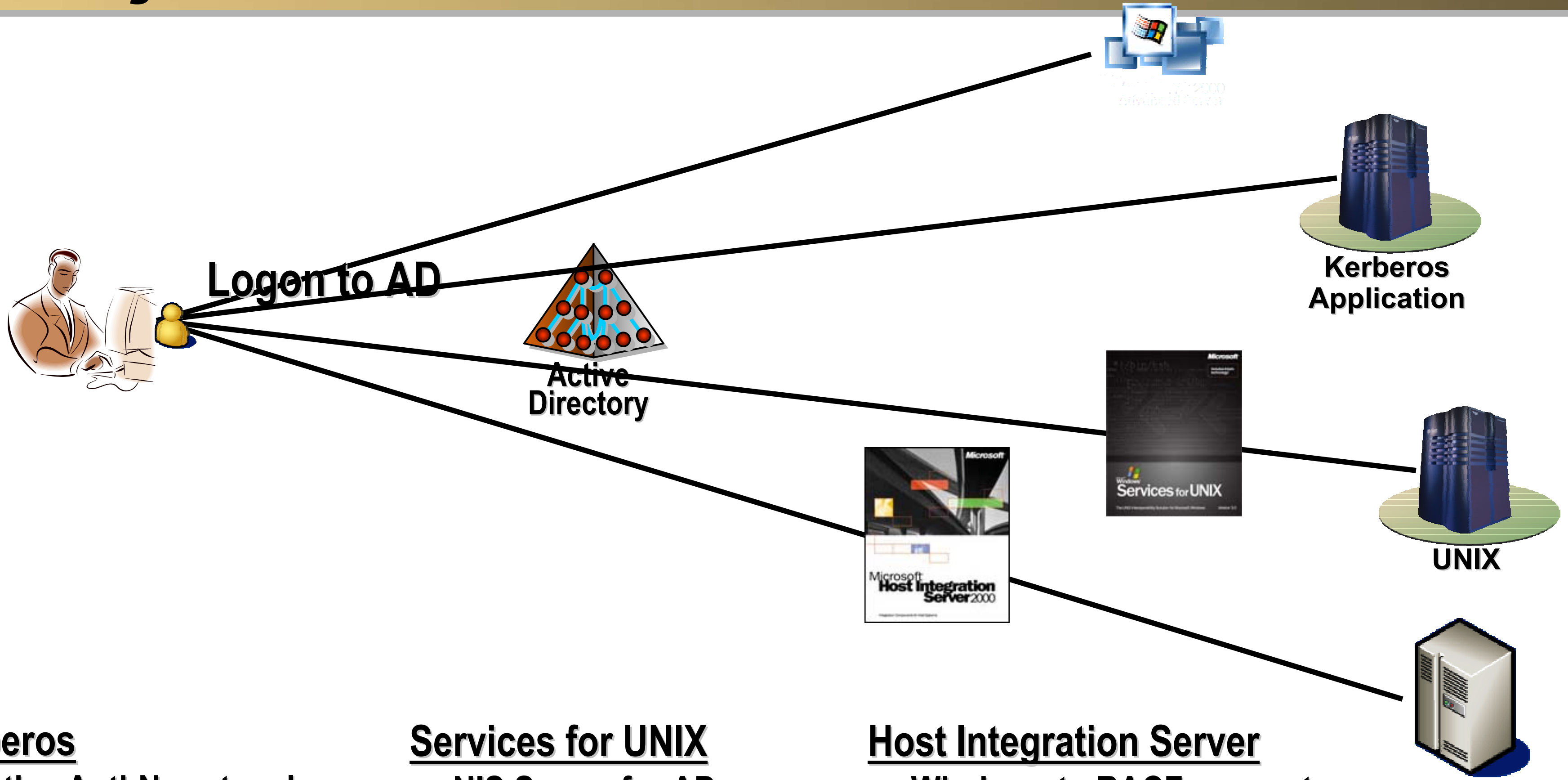
Certificate and smartcard logon

Standards-based interoperability

- L2TP/IPSEC VPN
- 802.1x wireless and wired LAN
- RADIUS
- EAP
- PEAP (Windows .NET)

Business to Enterprise

Extending Windows SSO



Kerberos

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

Services for UNIX

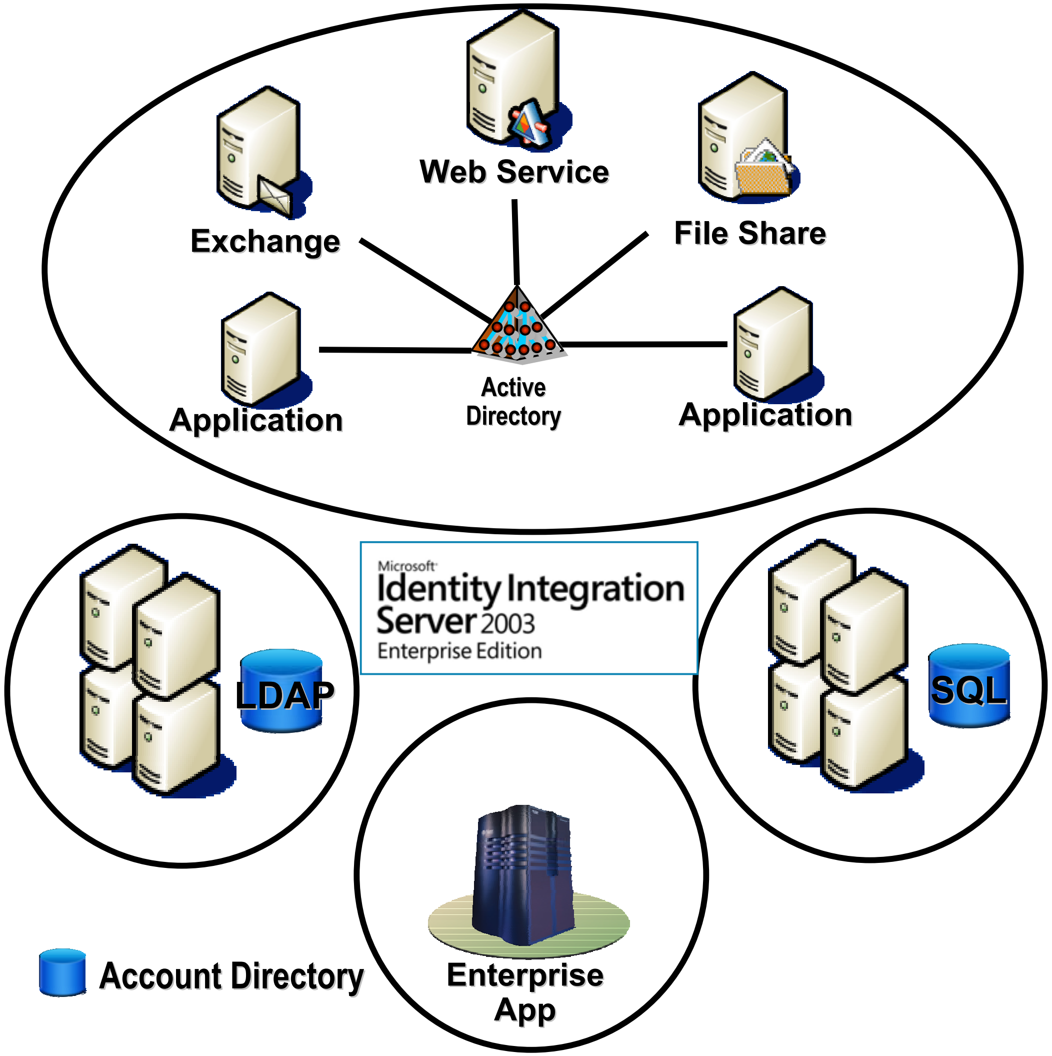
- NIS Server for AD
- NIS-AD directory sync
- Password synchronization
- User name mapping

Host Integration Server

- Windows to RACF accounts
- Windows to AS/400 Security System
- Bi-Directional Password Synchronization

Business to Enterprise

LDAP Authentication & Directory Integration



Integrate LDAP with AD

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

Microsoft Identity Integration Server

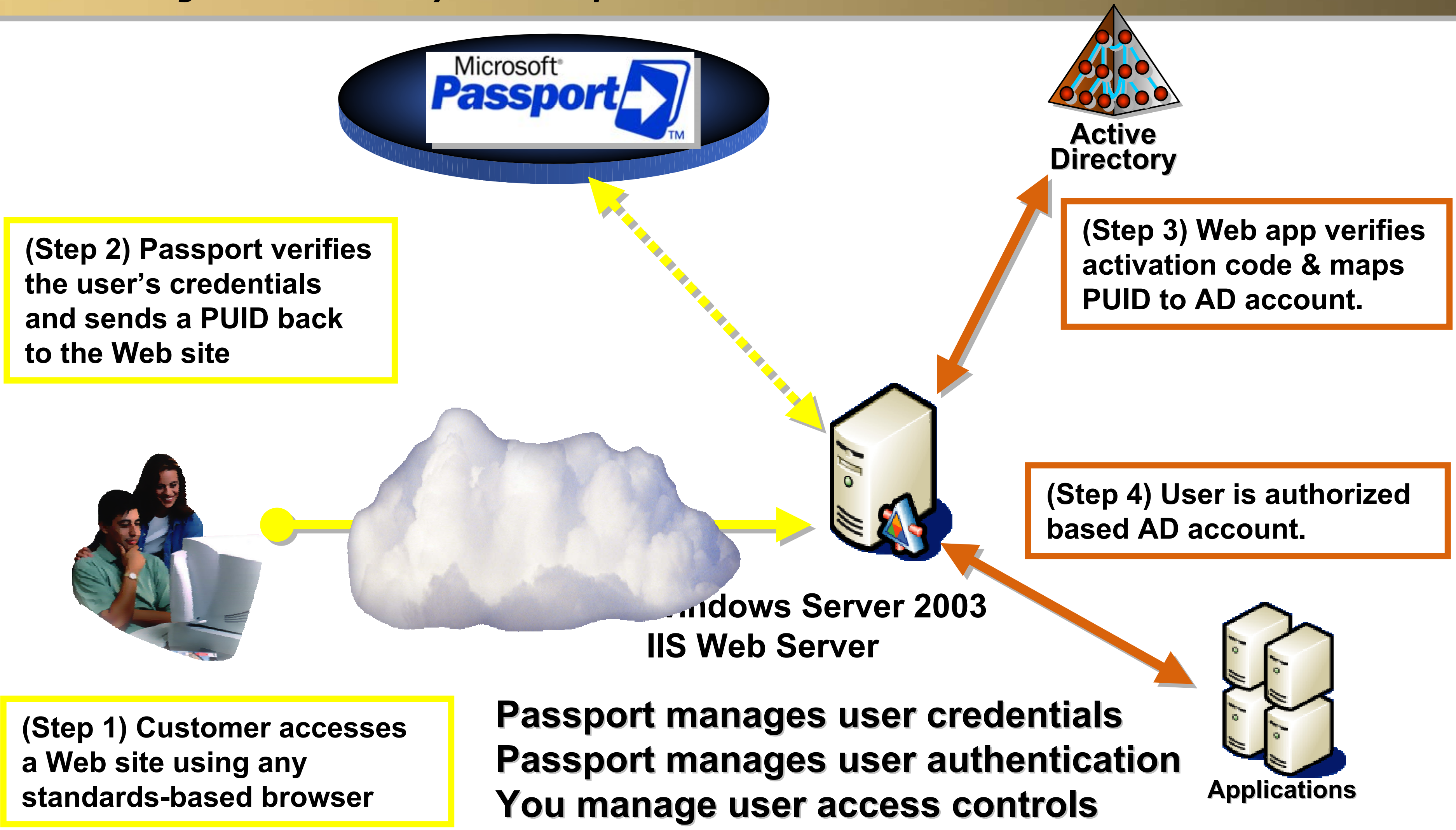
- Directory synchronization
  - LDAP (eg iPlanet & others)
  - Relational databases
  - Application specific
- Account Provisioning
  - Automate account creation
  - Automate account de-provisioning
- Password Management (MIIS 2003)
  - Self-service password reset

Key Solution Scenarios

Business to Employees	▪ Reduced Sign-on ▪ User provisioning/de-provisioning ▪ Password Management
Business to Customers	▪ Customer Portals – Web Single Sign-on ▪ Customer Self-service ▪ Password Resets
Business to Business	▪ Partner Portal – Web Single Sign-on ▪ Delegated Administration ▪ Partner Self-service

Business to Customers

B2C Using Active Directory and Passport



(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 1) Customer accesses a Web site using any standards-based browser

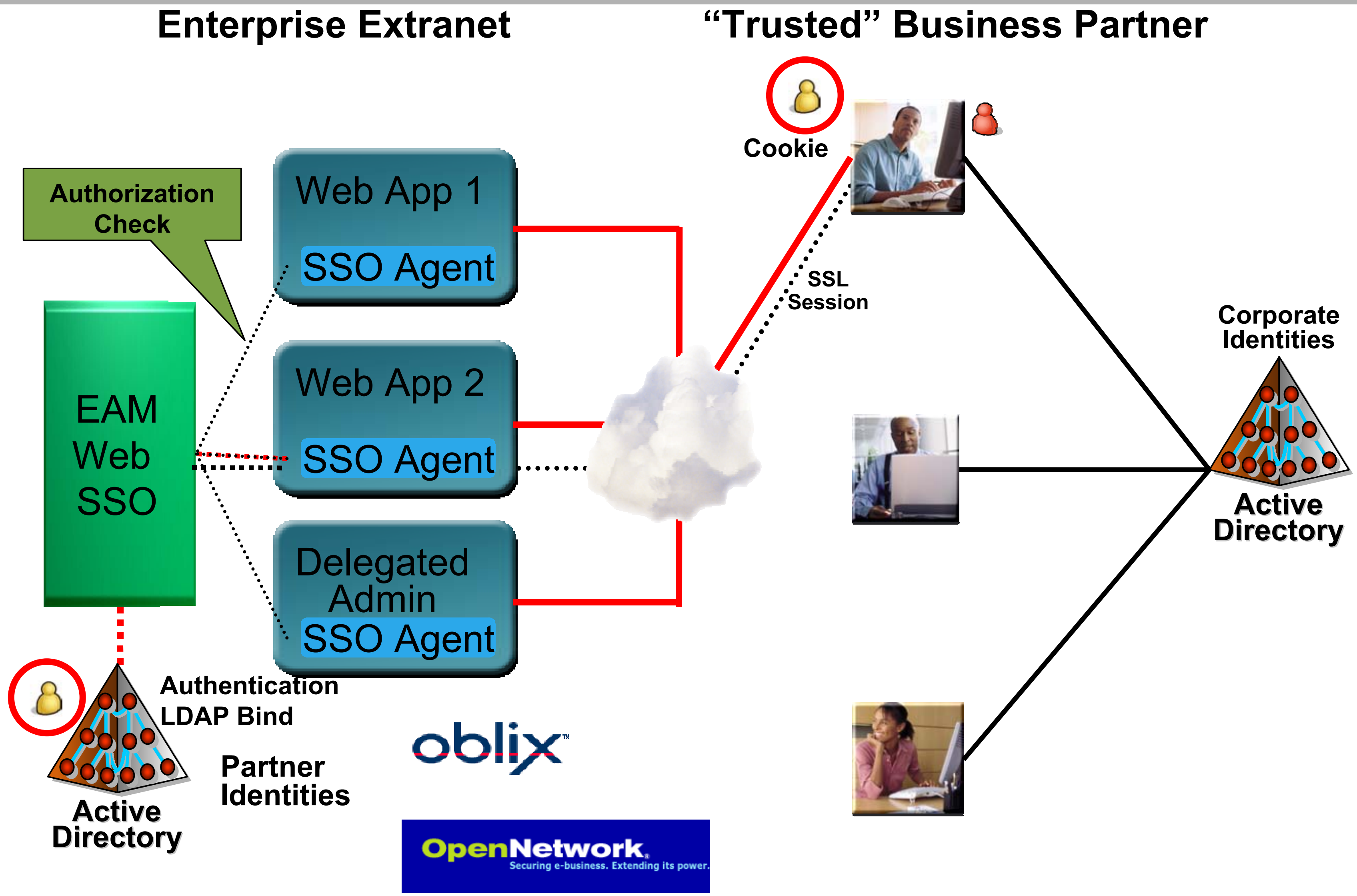
Passport manages user credentials
Passport manages user authentication
You manage user access controls

Key Solution Scenarios

Business to Employees	▪ Reduced Sign-on ▪ User provisioning/de-provisioning ▪ Password Management
Business to Customers	▪ Customer Portals – Web Single Sign-on ▪ Customer Self-service ▪ Password Resets
Business to Business	▪ Partner Portal – Web Single Sign-on ▪ Delegated Administration ▪ Partner Self-service

Business to Business

Extranet Access Management using AD



IdM Solution Accelerator

- Planning and Implementation Guide
- Scenarios – Implementation focus
  - Identity aggregation and integrity (multi-systems)
  - Provisioning and de-provisioning
  - Web portal self-provisioning
  - Delegated administration
  - Web SSO
  - SAP integration
  - UNIX workstation Kerberos integration
- Technologies
  - Directory
  - Certificate Authority
  - Kerberos (Windows and UNIX)
  - 3rd party Web Single Sign On (OpenNetwork, Oblix)

Microsoft

Microsoft Solutions for Security

Planning Guide for
Securing Wireless LANs – A Windows Server 2003 Certificate Services Solution

Microsoft
Solutions for Security

IdM Partners

Business Layers™

digitalPersona

oblix™

OpenNetwork. Securing e-business. Extending its power.

VeriSign® The Value of Trust℠

CAP GEMINI ERNST & YOUNG

ERNST & YOUNG
Quality In Everything We Do

hp invent

PRICEWATERHOUSECOOPERS PwC

UNISYS

Barclays Global Investors

"Active Directory's greatest value comes from cost avoidance and cost reduction. We determined that every dollar saved or avoided by Active Directory was either adding a dollar of pure profit to the company's bottom line, or adding a dollar of immediately available funding for other IT projects."

-Jeff Shore, Manager of Intel Systems, BGI

Result

Based on actual costs, AD has helped BGI to realize:

- Net benefit of $3.6M over 3 yrs
- 248% Return on investment
- Payback of costs in 8 months

Case study available at:
http://www.microsoft.com/AD

Pre-existing Environment

- Netscape directory and over 400 Windows NT servers organized in 4 master domains and many resource domains
- Mixed environment w/Unix-based workstations

Reasons for Migrating to Active Directory

- *Increasingly complex NT domain structure was becoming an administrative burden*
- *Netscape Directory Services did not meet demands for sophisticated permissioning and security*
- *Complex cross-platform authentication problems delayed access to business critical information*

Results Achieved

- Single sign-on across multiple platforms reduces logon time, helpdesk calls and improves security
- Intellimirror reduced end-user time spent on application installs by 60%
- Security administrators reduced by 21%
- Security administration costs decreased by 38%

BlueCross BlueShield

"As we expand and improve our e-business solutions, AD and DirectorySmart give us a unified and manageable security infrastructure. Combined, they enable us to reduce our security risks and protect the privacy of our members by simplifying the complexities of managing identities, privileges, and security operations both within and beyond the enterprise."

-Steve Wiggins, Chief Information Officer, BlueCross BlueShield of South Carolina

Result

Avoided licensing fees of $1.34M over the next 5 years and lowered overall TCO

Case study available at: http://www.microsoft.com/AD

Business Goals

- An identity management solution that could meet its current and future needs
- Reliable, scalable, secure extranet directory
- No costly directory licensing fees

Technology Impact

- *Achieved 99.9% reliability and fault tolerance*
- *Deployed to serve 1.4M customers in < 70 days*
- *Enhanced security for HIPAA compliance*

Results Achieved

- Active Directory deployed in an extranet role
- AD's multi-master replication capability provides the reliable, fault-tolerant directory service
- Easy integration of 3rd party WebSSO software from OpenNetwork

Sallie Mae

"We were impressed! Price, performance and partnership — that's what we got out of this project. Microsoft went above and beyond to help us position the project internally and achieve a strategic objective that we otherwise would not have accomplished."

- Jon Jones, IT Director

Result

- Avoided $2M iPlanet and $3M Novell licensing fees
- "Considerable savings with Windows s/w & h/w"
- Development projects reduced from ~700 hrs to ~200 hrs each

Case study available at: http://www.microsoft.com/AD

Business Goals

- A directory server platform that could handle millions of users with speed, accuracy & ease
- Lower total cost of ownership than competitors
- Enable growth, easily, to 7 million borrowers

Technology Impact

- *Enabled Web single sign-on solution*
- *Improved administration with single store*
- *Single userid, password for all customers*

Results Achieved

- Active Directory deployed in an extranet role
- Easy integration of 3rd party WebSSO software
- Identity Management foundation now built
  - PeopleSoft, Siebel AD integration next

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”
- MIIS 3.0 – RTM
  - Directory Integration & Synchronization
  - Account Provisioning
  - Password Management
- Active Directory Application Mode – Summer 2003
  - 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
- “TrustBridge” – “Longhorn Wave”
  - 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

- Identity management essential part of business strategy
  - Highly leveraged – simultaneously increase security and productivity while reducing costs
  - Competitive advantage - quickly enable new scenarios, business opportunities
- Microsoft and partners deliver complete solution
  - Get more from investment in Active Directory
  - Cross-platform capable

Next Steps

- Assign an owner
- Develop a vision and strategy
- Start small with focus on ROI
- Leverage Solution Accelerators
  - Planning
  - Implementation
- Establish policy
  - New applications must leverage Identity infrastructure
- Engage MCS and/or Partners
- For more Information http://www.microsoft.com/idm

Microsoft®

© 2003 Microsoft Corporation. All rights reserved.

This presentation is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY.

HP WORLD 2003
Solutions and Technology Conference & Expo

HP WORLD 2003

Solutions and Technology Conference & Expo

Interex, Encompass and HP bring you a powerful new HP World.

interex
shared knowledge • shared power

encompass
AN HP USER GROUP

hp
invent