

ORACLE®

# Oracle AS10g Identity Management



Marcin Odrowaz-Sypniewski  
*Fusion Middleware Sales Consultant*

ORACLE

# Oracle Fusion Middleware

## COLLABORATIVE ENTERPRISE PORTAL



Portals, Collaboration, Mobile, Desktop, Search

## DEVELOPMENT TOOLS



Modeling,  
Development Tools,  
Frameworks

## COMPOSITION & PROCESS ORCHESTRATION



BPM, ESB, B2B

## INFORMATION AGGREGATION & ANALYSIS



ETL, Hubs, Content Mgmt., BI, BAM

## MANAGEMENT



Systems  
Management

## ENTERPRISE APPLICATION SERVER



J2EE, WS-\*, Events, Metadata, Registry

## SECURITY



Identity, Services  
Management

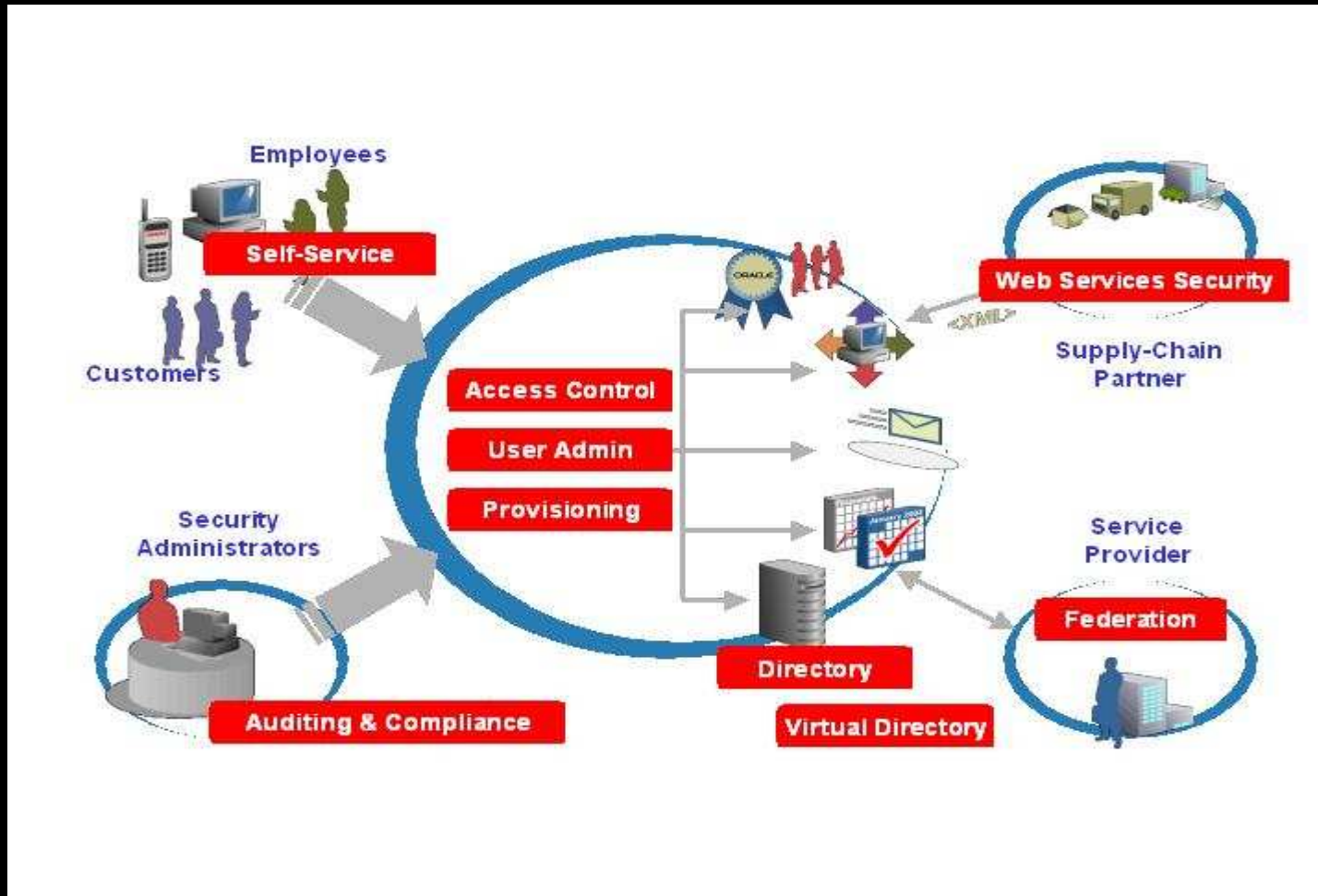
## GRID COMPUTING



Clusters, Resource Management, High Availability

ORACLE

# Oracle Application Server 10g Identity Management



# Oracle Application Server 10g Identity Management

**Access and Identity**

**Provisioning**

**Federation**

**Directory Services**

**Virtual Directory**

**Web Services Mng**

# Why Oracle invests in IdM ?

- Because it's a fast growing market
- Because it's a fundamental part of every application
- Because it's an integral part of middleware
- Because there's no other way.....

# Key Business Drivers

## Better security

- Adding / deleting user accounts
  - According to the security regulations
- Workflow approval mechanism
  - Eliminates the paperwork
- Business processes automation

## Following the rules & regulations

- Centralised security policy
  - Enforces to follow the regulations
  - Is a single-source of **every** single data about the user
- Reports & Audit

## Federated Identity

- Eliminates the need of managing access credentials for external users
- Multiplies number of applications users have access to

# Benefits of using Oracle IdM

- **Cost reduction**
  - How much does password reset cost ?
  - How much effort does it take for your developers to create an access procedures to new application ?
  - How critical for you is your application TTM ?
  - Free up your resources for new projects
- **Following regulations and better security**
  - Is there a possibility to quickly examine the access privileges for all users ?
  - How much time does it take to create a new account ?
  - Do you really know who has access to company materials ?
  - How do you provision access to applications ? Do you monitor high quality of passwords ?
  - Is the information about users and their privileges stored in a secure way ?
- **Being prepared for success = business growth**
  - How do you manage user accounts ? Will you follow the same manner if there are 1000 times more ?
  - What if you want to provide a secure access to your applications for external users ?

# Oracle acquires OBLIX

*In March 2005, Oracle has acquired Oblix, a market-leader in IdM solutions*

- **COREid**
  - a traditional Web SSO/Access Control and Identity Administration suite. Key product strengths include powerful authorization functionality, sophisticated workflow for managing user profiles, user selfregistration and self-service, dynamic group management, unified audit reporting, and integrations with many third-party platforms and products. In conjunction with third-party metadirectory and virtual directory products, COREid also provided user-provisioning capabilities.
- **SHAREid**
  - a federated SSO server for cross-domain single sign on. Key product strengths include support for multiple federation standards such as SAML 1.0, 1.1 and WS-Federation, bridges to multiple authorization products including COREid and CA eTrust SiteMinder, and a simple selfcontained design for easy distribution and deployment to partners.
- **COREsv**
  - a Web Services security and management product. Key product strengths include a flexible architecture of gateways and agents, WS-Security support, XML encryption/decryption, SOAP and non-SOAP support, and Web Service Monitoring.

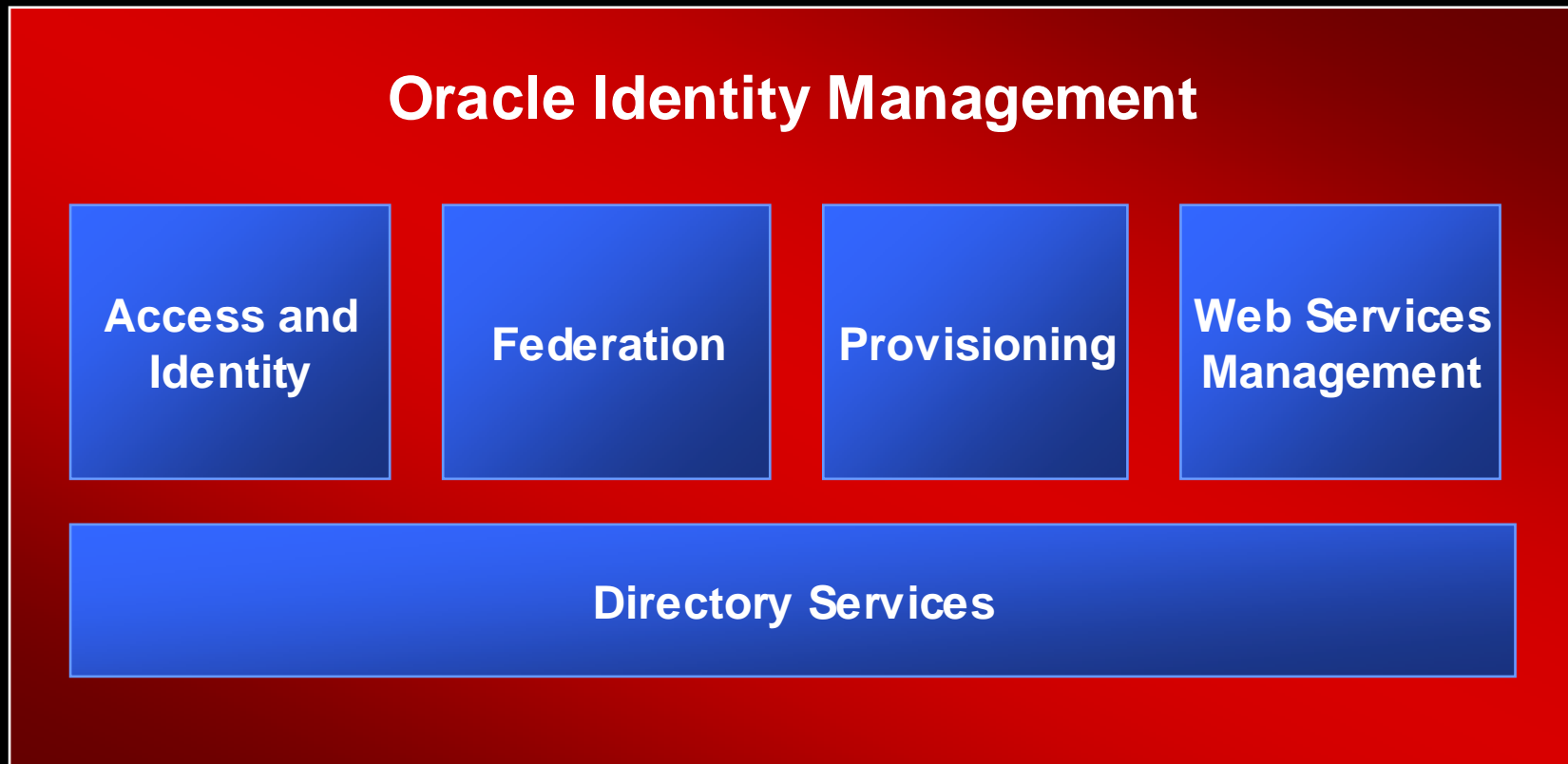
# Oracle acquires Thor and OctetString

- Xellerate Provisioning (Thor)
- VirtualDirectory (OctetString)

# Supported standards

- **LDAP v3** (directory client interface protocol)
- **X.509 v3** (PKI certificate standard)
- **SAML** (Security Assertions Meta Language) is intended to facilitate interoperability and federation among security services like Oracle9iAS Single Sign-On.
- **SPML** (Service Provisioning Meta Language) is an XML standard that facilitates integration among provisioning environments by defining the protocol for interaction between Provisioning service components and agents representing provisioned services.
- **DSML** is an XML standard for exchanging directory data as well as invoke directory operations over the Internet.
- **XKMS** is the XML Key Management Specification. It is intended to simplify deployment of PKI in a web services environment.
- **WS-Security** standards define a set of SOAP extensions that can be used to provide message confidentiality, message integrity, and secure token propagation between Web Services and their clients

# Oracle Identity Management provides a complete solution



# Oracle Identity Management

Product	Functionality
Oracle Identity Management	Directory server (OID), synchronization, SSO, user administration
Oracle COREid Access and Identity	SSO mechanism supporting different directory servers, unified administration over user profiles using roles, privileges, groups, organizations
Oracle COREid Federation	Embedded into Oracle Identity Management mechanism of Identity Federation
Oracle COREid Provisioning	Set of processes and mechanisms for user creation/deletion/updating
Oracle Web Services Manager	Centralised, policy-based system providing secure communication for Web Services

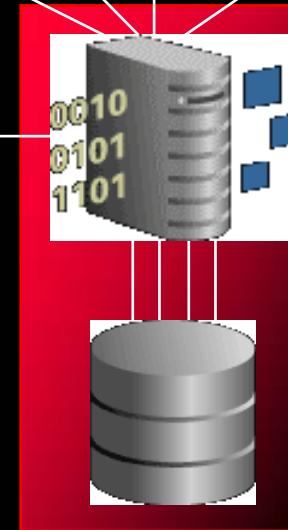
# Oracle Internet Directory

- Scalability
  - Millions of users
  - Thousands of parallel sessions
- High availability
  - Hot backup/recovery, RAC, etc.
- Managing
  - Multi-node monitoring
- Security
  - Extended password managing policy
  - Audits
- Plug-in framework
  - Possibility of creation custom attributes
  - External authorization
  - Custom security policy

LDAP  
Clients



Directory  
Admin  
Console



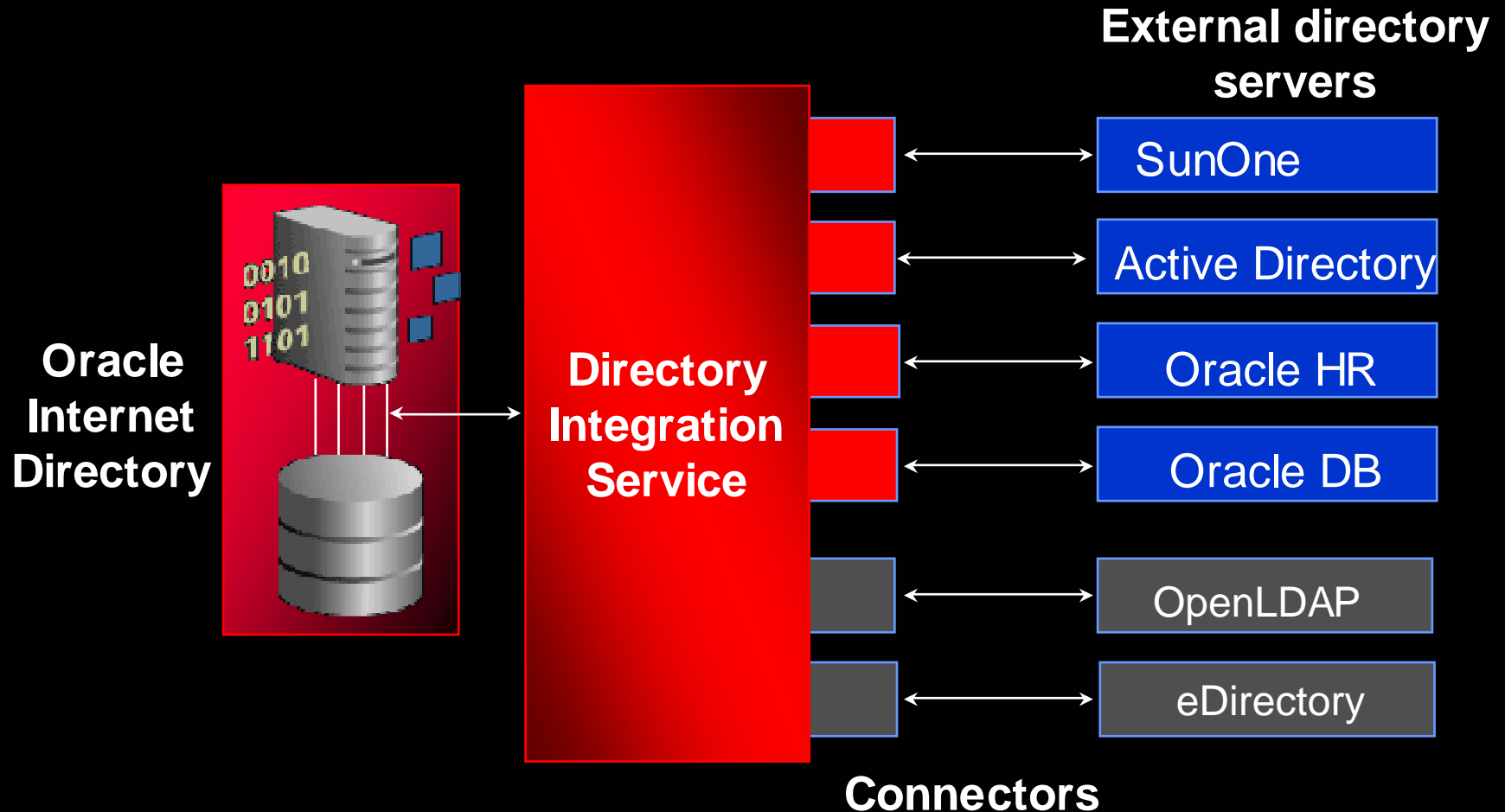
Oracle  
Internet  
Directory  
Server

Oracle  
Database

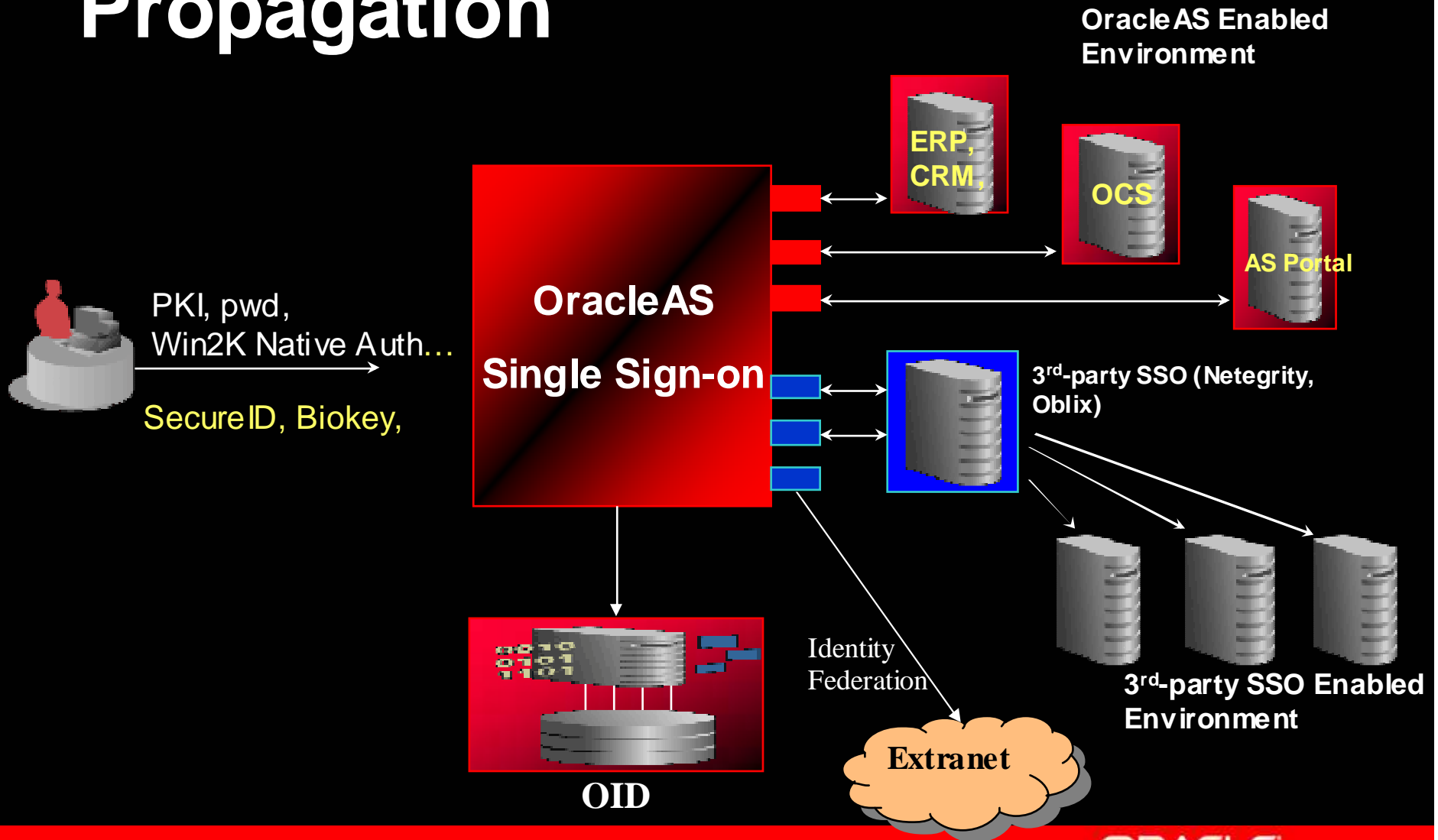
# What is new in OID 10.1.4?

- Out-of-the-box synchronization with:
  - Oracle Human Resources
  - Oracle Database
- Out-of-the-box agents for LDAP synchronization:
  - Sun Java System
  - Directory Server
  - Microsoft AD
  - nowy adapter do Novell Directory (od wersji 8.7.3)
  - OpenLDAP (od wersji 2.1)
- Oracle Password Filter for Microsoft AD
- Server Chaining (remote access to external directory servers)
- DSML (LDAP interface for WebServices)
- GUI tool for replication of data from different directory servers

# Directory Integration

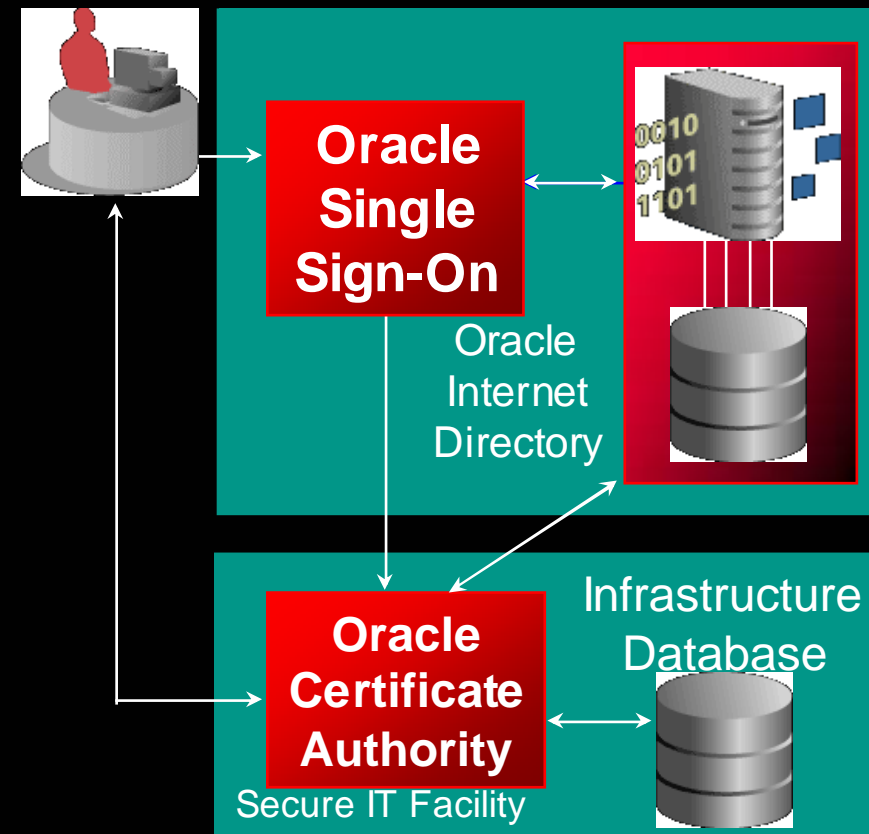


# Single Sign-on & Identity Propagation

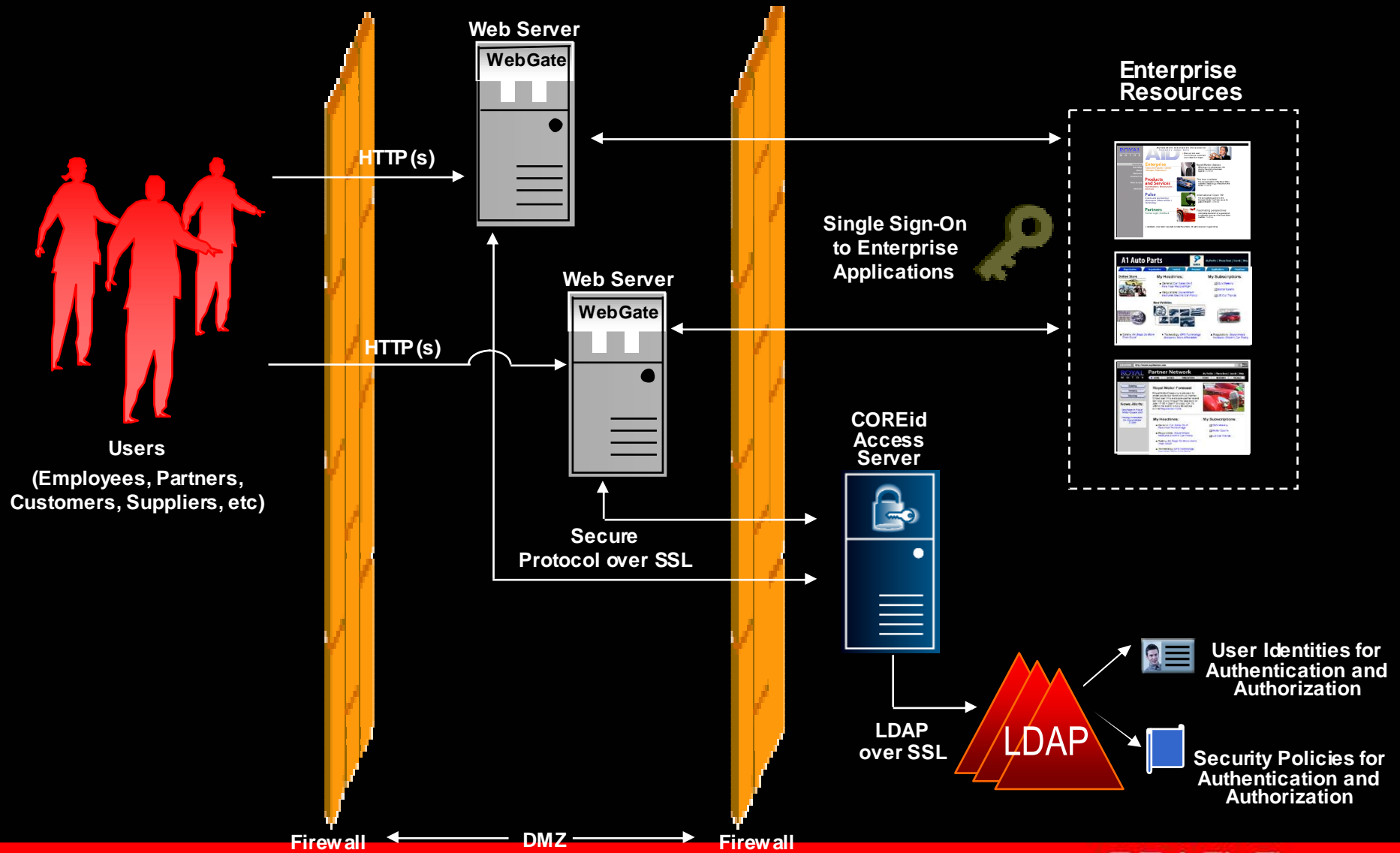


# Oracle Certificate Authority

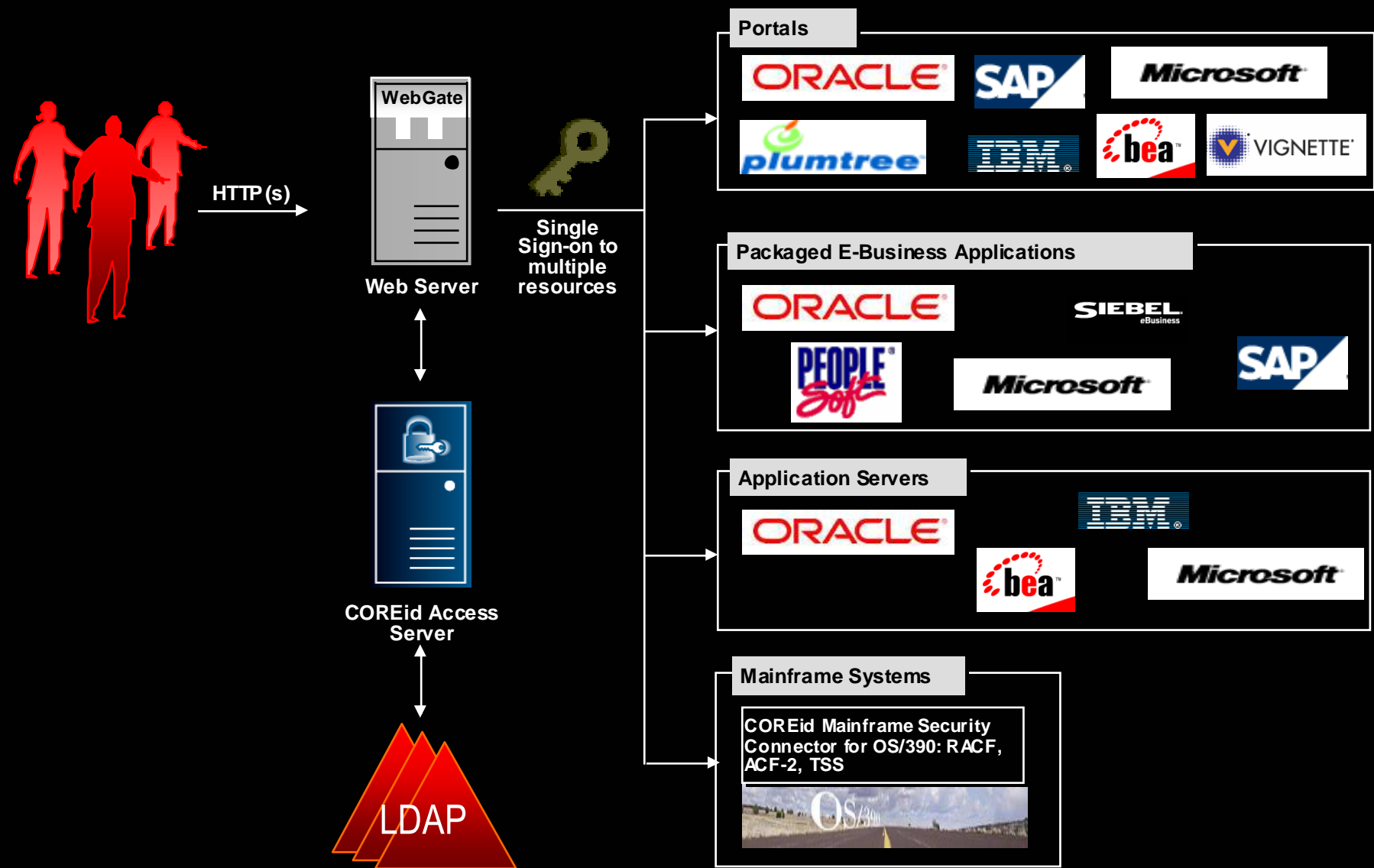
- Out-of-the-box PKI solution
- Easy implementation of X.509v3 certificates
- Web interface
- Integration with Single Sign-On & Oracle Internet Directory



# COREid Access



# Integration



# Oracle COREid Access and Identity Certificates

- Oracle and Third Party Integrations

- OracleAS 10g R2 (10.1.2.0.0) Single Sign-On
- IBM WebSphere v5.0.(0,1,2) EE
- IBM WebSphere v5.1 EE
- IBM WebSphere 6.0
- IBM WebSphere Portal 5.0.2.2 with CMR
- BEA WebLogic 7.0
- BEA WebLogic 8.1 SP2 (via SSPI)
- BEA WebLogic 8.1 SP3 (via SSPI)
- BEA WebLogic PS 8.1 SP3 (via SSPI)
- Plumtree Portal 5.0.4
- Siebel 7.5.2, 7.5.3
- mySAP e-Business R3 v4.6D ITS v6.10, 6.20
- SAP Portal v5.0 SP2
- SAP Portal v6.0
- Microsoft MIIS

- **Web Servers for Web Gate**

- Oracle HTTP Server 10g Release 2 (10.1.2.0.0)
- Sun One 6.0
- Sun Java System 6.1 SP2
- Domino R6.5.3
- Apache 2.0.52
- Apache 2.0.52 as reverse proxy server
- Apache 1.3.33
- Apache 1.3.33 as reverse proxy server
- IHS 1.3.26
- IHS 2.0.47
- IHS 2.0.47 as reverse proxy server
- IIS6
- MS ISA 2000 SP1

- **Web Servers for WebPass and Access Manager**

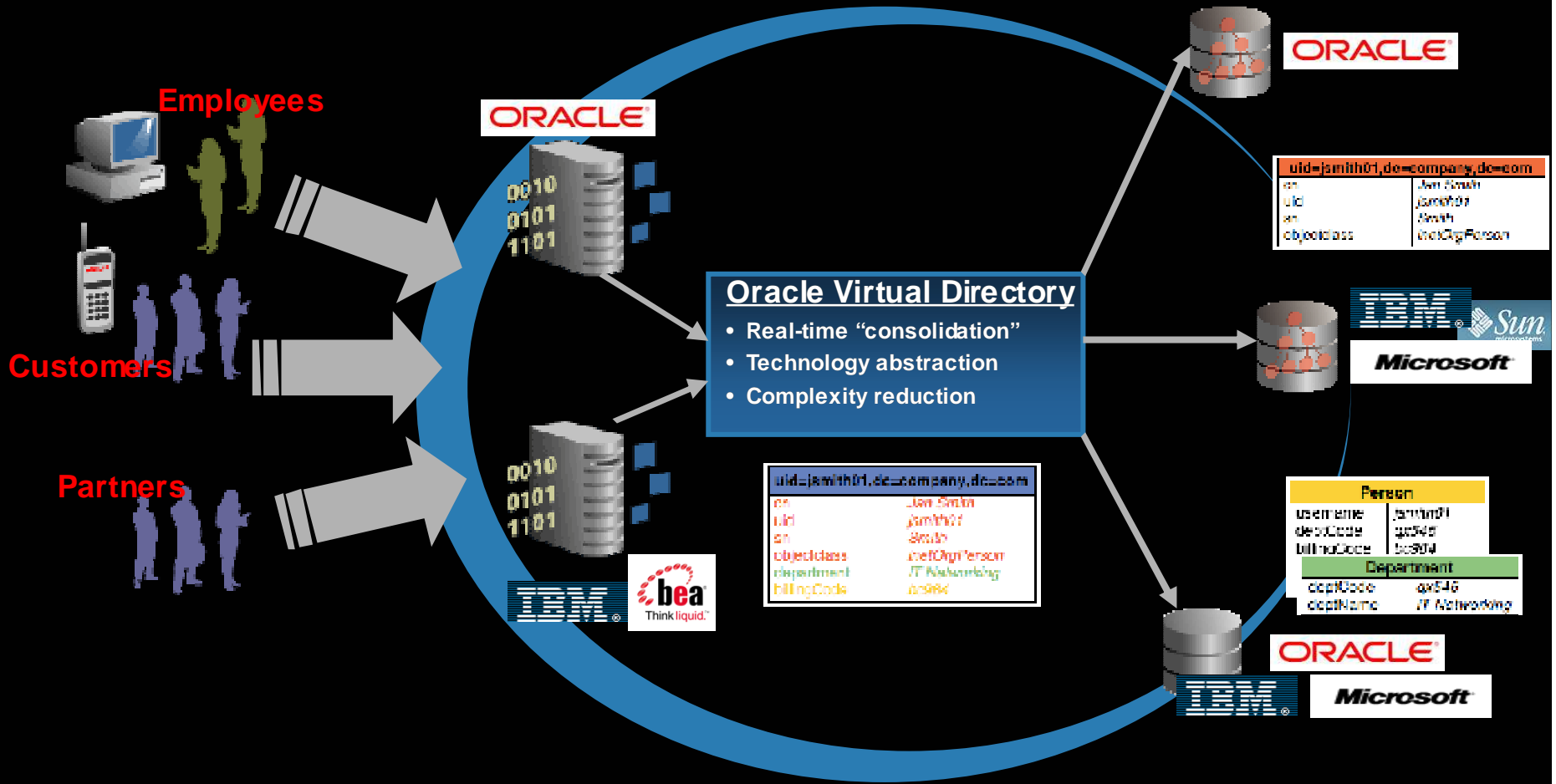
- Sun Java System 6.1 SP2
- Apache 2.0.52
- Apache 1.3.31
- IIS5
- IIS6
- IHS 1.3.26
- Access SDKs
- Any standard C compiler
- hp ANSI C compiler
- hp ANSI C++ compiler
- Any standard Java 1.4 compiler
- CGG 3.3.2 C++ compiler
- AIX C v6 C++ compiler
- .NET support - VS .NET 2003 7.0

# Oracle COREid Access and Identity

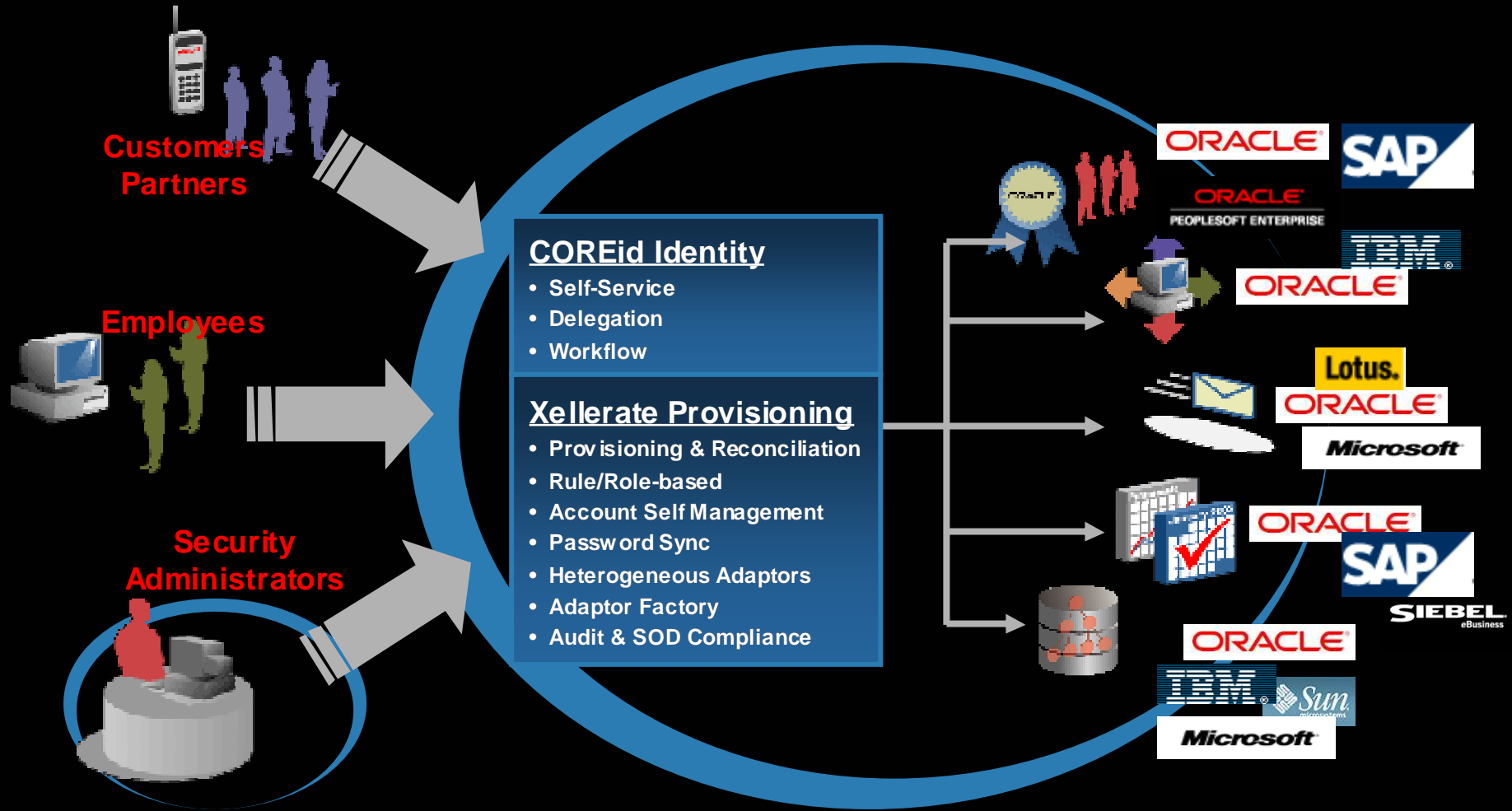
## *Certificates*

- Customer Directory Services
  - Oracle Internet Directory 10g Release 2 (10.1.2.0.0)
  - Sun Java System Directory Server 5.2
  - Siemen DirX v2.0B
  - Novel eDirectory 8.7.3
  - IBM Directory Server 5.1
  - IBM Tivoli Directory Server 6.0
  - Microsoft AD 2000
  - Microsoft AD 2003
  - Microsoft ADAM 1.0
  - OctetString Data Anywhere v3.0 (VDE)
- **Browsers for Administrators and End Users**
  - Netscape 6.2.2
  - Internet Explorer 5.5, Internet Explorer 6.0 or later
  - Firefox 1.0
- **Browsers for End Users**
  - Safari 1.2
  - Netscape 4.08
  - Netscape 4.7x
  - Netscape 6.1
  - Netscape 6.2

# Oracle Virtual Directory



# Oracle Xellerate Identity Provisioning



# COREid Federation

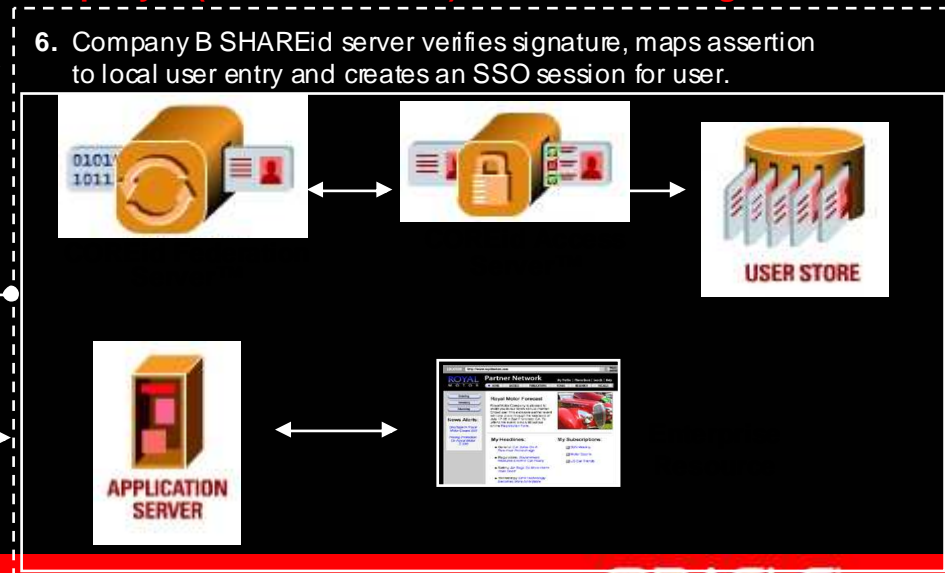
## Example

- B  
R  
O  
W  
S  
E  
R**
1. Company A employee logs into employer's corporate portal.
  2. Portal authenticates and authorizes user.
  3. Employee clicks on a link to access protected resource at Company B (transfer request). Portal sets a header variable that identifies the user.
  4. Request transfer to Company A SHAREid server, which uses the header variable to identify the user and creates a signed SAML assertion with attributes from the user's LDAP or RDBMS profile.
  5. Browser posts SAML assertion to Domain B SAML receiver service.
  6. Company B SHAREid server verifies signature, maps assertion to local user entry and creates an SSO session for user.
  7. Company B uses the SSO cookie to determine authorization to requested resource.
  8. If authorized, browser redirects to target URL, and sets Company B SSO Cookie on user's browser.
  9. User can now go directly to any protected resource at Company B until the SSO session expires.

### Company A (Source Site) LDAP or RDBMS IdMBridge



### Company B (Destination Site) COREid IdMBridge



# Oracle Web Services Manager (WSM)

- Offers centralised platform for applying policies to applications based of Web-Services
  - Provides security & managing mechanisms for Web-Services
  - Does not imply any changes in application code
  - Supports WS-\* standards like WS-Security, WS-Policy, etc.
  - Offers a tool for defining and monitoring of policies
  - Delivers mechanisms for policy-execution in real-time

# References: General Motors

- **Business needs**

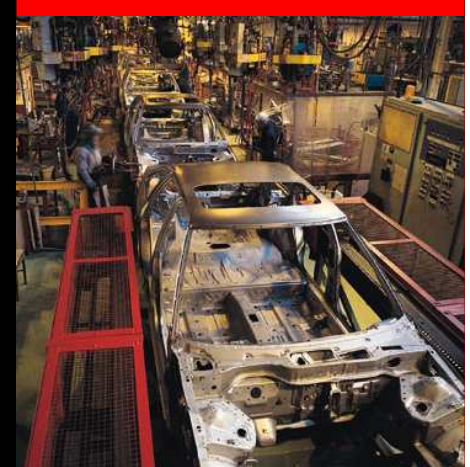
- Provide a secure access to corporate resources for 53 000 external suppliers and 17 000 employees. Integration required usage of existing security infrastructure IBM (Tivoli).

- **Solution**

- GM has implemented Oracle COREid, using functionality to remote management for administrators, employees and suppliers.

- **Benefits**

- ✓ Secure infrastructure
- ✓ Cost reduction
- ✓ Faster deployment of new applications
- ✓ Standardization of Identity Management aspects



ORACLE

# References: Lehman Brothers

- **Business needs**
  - Standardization of maintenance of business-critical systems written in old, non-extensible manner
  - Lack of information about user privileges
- **Solution**
  - Implementation of Xellerate Provisioning for 22 000 users. In production since 2003. Around 650 systems have been connected to Xellerate platform.
- **Benefits**
  - ✓ Rapid process of user account creation & privileges provisioning < 5 minutes
  - ✓ Deletion of unused accounts
  - ✓ Common security policy
  - ✓ Possibility to track & audit every change in the system



LEHMAN BROTHERS  
*Where vision gets built.™*

ORACLE®

# Success Story: Boeing

- **Business needs**
  - Boeing has faced problems with running 401K program for it's employees. There was a need of a common reporting & audit system.
  - Need of cutting the costs of system maintenance – password reset, privilages management, etc.
- **Solutuion**
  - Boeing has implemented Oracle COREid in order to provide 930 000 employees with a secure and fast tool to manage their accounts in 401K programm.
  - **Benefits:**
    - ✓ Number of calls to help-desk decreased 3 times (ca. 1 million \$ savings every year)



ORACLE

A large, stylized graphic of a question mark 'Q' and an answer 'A' in a dark grey color, serving as a background for the text. The 'Q' is positioned above the 'A', and they are both rendered in a bold, sans-serif font.

**Q U E S T I O N S**  
**A N S W E R S**

ORACLE®