Architecting the Identity-Enabled Enterprise

The Directory Interoperability Forum

Ed Harrington, Chair
(Principal Consultant & CEO, EPH Associates LLC)
edh@ephassociates.com
Some Relevant and/or Irreverent Quotes

“Noble life demands a noble architecture for noble uses of noble men. Lack of culture means what it has always meant: ignoble civilization and therefore imminent downfall.”

- Frank Lloyd Wright

“No architecture is so haughty as that which is simple”

- John Ruskin, British art critic

“Architecture is the art of how to waste space”

- Philip Johnson
Agenda

- The difficulties of architecting for identity management
- Designing identity management for the enterprise
- Identity management building blocks
- The four strategies for identity management implementation
- Using TOGAF
- Conclusions
The Difficulties
The Difficulties

- Understanding the role of Identity Management
- Making it support the rest of the solution
- Integrating with existing infrastructure
The Role of Identity Management in the Enterprise

- Identity information creation, modification and deletion:
  - by administrators
  - by users

- Identity information provision:
  - to users
  - to applications
  - to access control decision points.
The Role of Identity Management in the Enterprise

Enabling personalised services
Supporting the Whole Solution
Integrating with Existing Infrastructure
Designing Identity Management for the Enterprise
Designing Identity Management for the Enterprise

Business Drivers and Requirements

Enterprise Identity Store

Enterprise Logic

Bought-in Products and Services

External Identity Stores and Applications

Identity-Dependent Services
Building Blocks
Available Products and Services

- Directory, metadirectory, virtual directory
- Identification (biometrics, smart cards)
- Authentication (eg. via corporate & 3rd party databases)
- Single Sign-on (to web services, corporate applications)
- Access Control (including fine-grained, role-based)
- Identity Information Provisioning (ids, passwords, certificates, permissions, privileges, attributes, profiles, . . . )
- Identity Information Administration
- Identity Information Synchronization
- Account federation
- Identity policy management
Standards for Interoperability

- Directory
  - X.500
  - LDAP
  - DSML

- Application Interaction
  - SAML - enables trusted access to external identity information
  - XACML - access control
  - SPML - provisioning

- Only X.500 and LDAP are mature
- LDAP is preferred to X.500 DAP over the Internet
- SAML (Liberty profiles) may become established
Standard Identity Management
Building Blocks

- Directories (X.500 and LDAP)
Identity Management Strategies
Identity management Strategies

- Synchronization
- Distributed directory
- Metadirectory/Virtual directory
- Federation
Synchronization
Synchronization Example - The Open Group
Distributed Directory

- X.500
- Proprietary
X.500 Model
Examples of Distributed Directory

- The major government chose Nexor X.500 directories
  - [http://www.nexor.com/press_00.asp](http://www.nexor.com/press_00.asp)

- CNN uses distributed Novell directories
Meta/Virtual Directory

Diagram:
- Application
- LDAP
- Metadirectory
- Corporate Directory
Examples of MetaDirectory/Virtual Directory

- Lufthansa uses Novell e-Directory

- ICL uses Microsoft Metadirectory Services

- The Boeing Secure Messaging Challenge
Federated Directories

Directory 1

Federation

Directory 2

LDAP or DSML

SAML and other ML

Application

LDAP or DSML

Application

(C) The Open Group 2003
Composite Strategies

- Metadirectory
- Chaining
- Replication
- Synchronization
- Federation
- External Directory
- Enterprise Directories
Using The TOGAF ADM
The Identity Management View

- People
- Identity Management Strategy
- Identity Store
- Identity Management Applications
- Identity Management Logic
Conclusions
Summary and Conclusions

- Identity Management is an important, specialized, aspect of architecture for the Boundaryless Enterprise
- But incorporating it in the architecture is not easy
- We have reviewed
  - design considerations
  - building blocks
  - implementation strategies
  - use of TOGAF
- More work is needed
  - to identify building blocks
  - to develop and describe the architecture process
Architecting the Identity-Enabled Enterprise

Thank you!