Identity Management.

28 June 2006

Jean-Marie Abighanem
Director
Enterprise Risk Services
Objectives

The purpose of this presentation is to make you aware of:

• Typical trends in an Organization
• Providing an understanding of Identity Management
• A sample of Identity Management initiatives and the associated benefits/challenges
Typical Trends In An Organization
Existing Trends in any Organization

Organizations are continuously implementing IT-related initiatives to achieve business objectives.

**Typical Business Objectives**
- Increase revenue and profitability
- Streamline processes and improving efficiency
- Improve the user experience
- Enhance Security and Improving User Access.
- Reduce operational and back-office costs (TCO)
- Ensure Regulatory Compliance

**Sample IT Initiatives**
- Corporate Portals
- E-Business solutions
- Enterprise Application Integration
- SOA
- ERP / HRMS systems
- Implementing CRM solutions
- Data warehousing
- E-Procurement

These initiatives are based on a rapidly growing portfolio of enterprise and home-grown IT applications.
Convergence of business drivers has stretched the capabilities of existing security infrastructure

• Need to have access and do business regardless of location or employee type
• Web-based content delivery solutions are exposing more sensitive content and services at a greater risk
• User access methods and access points have increased in complexity
• Liability for lack of care in protection of sensitive user information
• Regulatory and Compliance related pressure (Sox, APRA, etc.)
• Ability to provision and de-provision users in a minimum time-frame
The User-ID challenge

The number of user-IDs that a user needs to get the job done has become a potential management and integrity issue

- Number of applications in your network is increasing
- Newer content and services provided to the end-users need to be secure.
- Some information and services require higher security than what is available within your infrastructure
- You need to maintain the control and confidentiality of all your users
- Cost of maintaining increasing number of users and passwords is increasing
Evolution of User-ID driven infrastructure and its disadvantages

**Traditional IT infrastructures evolved from**
- Applications purchased and implemented with independent User-ID’s
- User-ID administration is decentralized and inconsistent across applications
- Increasing number of applications being deployed rapidly
- Point solutions being deployed instead of Enterprise solutions

**User-ID centric infrastructure resulted in**
- Increased maintenance costs
- Decreased user productivity
- Increased risk of unauthorized access
- Decreased ability to quickly adapt to changing needs
Identity Management
What is Identity Management?

The basic Identity-related questions are:

- Who are you?
- What do you need to do your job?
- How can we best manage you?

Identity Management:

- Helps simplifies and automates the answers to the above mentioned questions
- Is a collection of various technologies and concepts
- Consolidates multiple instances of user identity into one virtual identity
- Helps manage the multiple identities across the organization
- Helps business processes and applications leverage these identities in a consistent policy-enforced manner
- Provides consistent access control
Components of Identity Management grouped into high-level categories

• Administration
  – Provisioning
  – Workflow
  – Self Service and Password Management
  – Audit trails
  – Delegated administration

• Authentication
  – Supports multiple identity stores and authentication types

• Authorization
  – Role Based Access Control (RBAC)
  – Web SSO/Reduced sign on
  – Windows SSO
Typical Identity Management Process Flow

Mapping of Identity and Access Management Components on the Identity Lifecycle

Processes
- Identification/Registration
- Termination/Removal
- Identity Creation
- Maintenance/Propagation
- Usage

Business Events and Triggers
- Employees
- Contractors

Authoritative Source
- Human Resources Application
- Enterprise Resource Planning Application or Mainframe Application

Identity Repository
- LDAP Directory
- Databases

User Provisioning
- Delegated and/or Central Administration
- User self-service
- Password Management

Access Provisioning
- Access Policies, Rules and Roles
- User Account Provisioning
- Access Provisioning

Access Management Services
- Authentication
- Authorization
- SSO

Audit and Infrastructure Services
- An authorized origination source for the creation or termination of an identity, e.g., CIS
- A single or multiple places where identities from separate applications and systems are stored and linked
- Admin interfaces for managing user profiles, user credentials and access control services
- Identity-driven access management services: authentication, authorization and SSO

Technologies
- Applications and Users

Identity Management
Copyright 2006 Deloitte Touche Tohmatsu
Identity Management Factors

Typical factors affecting Identity Management Initiative in an Organization

- Institutional Goals
- Standards
- Practices
- Products
- Technology
- Policy & Governance
- Business Drivers
- Requirements
- Ability to Implement
- Budget
- Project Management
- Staff Skills/Expertise
- Identity Management

Identity Management Copyright 2006 Deloitte Touche Tohmatsu
Identifying the need for an Identity Management solution

• Do users have multiple ID’s in your organization?
• Are user Id’s being managed by individual departments and administrators?
• Do you have an effective mechanism for tracking who has access to what system and resource?
• Can you efficiently provide and revoke a user’s access to multiple systems?
• Do you plan to meet audit and regulatory requirements?
• Are you deploying web based applications?
• Do you plan to provide web based access to back end applications through the enterprise portal?
• Do employees and customers get the information they need effectively?
Who benefits from Identity Management?

<table>
<thead>
<tr>
<th>Role</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIO/CFO</td>
<td>• Reduce overall costs, Increase revenue</td>
</tr>
<tr>
<td></td>
<td>• Provides better management capabilities</td>
</tr>
<tr>
<td></td>
<td>• Improves compliance standards</td>
</tr>
<tr>
<td>Operations</td>
<td>• Eliminates number of calls associated with password resets</td>
</tr>
<tr>
<td></td>
<td>• Reduces costs associated with running helpdesk</td>
</tr>
<tr>
<td></td>
<td>• Helps helpdesk focus more on critical issues and better customer service</td>
</tr>
<tr>
<td>Development</td>
<td>• Reduces cost of development</td>
</tr>
<tr>
<td></td>
<td>• Standardized Authentication and Authorization components</td>
</tr>
<tr>
<td>HR</td>
<td>• Reduces Employee Life Cycle costs</td>
</tr>
<tr>
<td></td>
<td>• Increases employee productivity</td>
</tr>
<tr>
<td>Architecture</td>
<td>• Helps set guidelines and standardizes architecture across the enterprise</td>
</tr>
<tr>
<td></td>
<td>• A common infrastructure reduces costs</td>
</tr>
<tr>
<td>Security</td>
<td>• Provides consistent policy enforcement</td>
</tr>
<tr>
<td></td>
<td>• Provides security and audit components</td>
</tr>
</tbody>
</table>
Identity Management Initiatives

• Each organization that contemplates an Identity and Access Management strategy will have a unique combination of goals and priorities

• Identity Management initiatives should:
  – Be business driven and have committed stakeholder support
  – Span the organization; security solutions have far-reaching business and technology impact
  – Receive organizational acceptance
  – Anticipate changes in business needs
Organizational access policies could specify the behaviour and business rules regarding access to organizational entities

• Examples:
  – Account Management policies could dictate that stale accounts be regularly purged from the system
  – Global Password policies could state how complex passwords could be. They could also mandate regular expiration/change of passwords.
  – VPN Access management security policies

<table>
<thead>
<tr>
<th>Benefits</th>
<th>Challenges</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Increased security across organization</td>
<td>• Management challenges with a more complex policy system</td>
</tr>
<tr>
<td>• Better management capabilities</td>
<td>• Decreased efficiency and management overhead of applying policies without automation</td>
</tr>
<tr>
<td>• Regulatory Compliance</td>
<td></td>
</tr>
</tbody>
</table>
Initiative – Identity Aggregation and Synchronization

• It is not always practical to migrate all identity identities to a single store but it is possible to aggregate user identities across various systems and reduce management overhead.
• Identity aggregation consists of linking multiple digital identities from a number of identity stores.
  – Example: “G. Lucas” from the HR system can be linked to “George Lucas” in the email system and to “glucas” on the mainframe.

<table>
<thead>
<tr>
<th>Benefits</th>
<th>Challenges</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Reduced administration overhead</td>
<td>• Determining the authoritative sources of all attributes across systems that form the digital identity</td>
</tr>
<tr>
<td>• A single linked user identity</td>
<td>• Choosing what attributes are owned by what identity store</td>
</tr>
<tr>
<td>• Improved identity administration from a single identity store</td>
<td>• Achieving cross-department collaboration among HR, IT, Legal and other participating business divisions</td>
</tr>
</tbody>
</table>
Initiative – Automate User Provisioning and Workflows

- Automated provisioning can synchronize identities from one identity store to multiple managed identity stores
- Specific rules and workflows can be enabled for this provisioning and de-provisioning process

<table>
<thead>
<tr>
<th>Benefits</th>
<th>Challenges</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Time to provision new accounts across multiple systems is vastly reduced</td>
<td>• Determining and solidifying the business case for provisioning</td>
</tr>
<tr>
<td>• Automated generation of attributes across systems can provide ease of administration</td>
<td>• Figuring out the identity attribute distribution and workflow requirements for provisioned systems</td>
</tr>
<tr>
<td>• Easier group and role membership management</td>
<td>• Choosing what attributes are owned by what identity store</td>
</tr>
<tr>
<td>• Increased security by simplifying the de-provisioning process for leaving employees and contractors</td>
<td>• Achieving cross-department collaboration among HR, IT, Legal and other participating business divisions</td>
</tr>
<tr>
<td>• Provides enhanced security and audit trails</td>
<td></td>
</tr>
</tbody>
</table>
Initiative – Password Management and Self-Service

- Password management is one step further from Identity aggregation
- Involves enforcing password policies, changing/resetting and synchronizing passwords across the multiple managed identity stores
- Password management can enable an helpdesk person to change a user’s HR, network and reporting passwords in one operation
- Can provide password self-service capabilities to end users

<table>
<thead>
<tr>
<th>Benefits</th>
<th>Challenges</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Simplifies password administration</td>
<td>• Coping with existing multiple password policies</td>
</tr>
<tr>
<td>• Reduced helpdesk administration and support costs</td>
<td>• Coping with existing password expiration and history</td>
</tr>
<tr>
<td>• Frees up helpdesk to provide assistance on more</td>
<td>• Securely transmitting and updating passwords to individual identity stores</td>
</tr>
<tr>
<td>important issues</td>
<td></td>
</tr>
<tr>
<td>• Provides vehicle for maintaining consistent and</td>
<td></td>
</tr>
<tr>
<td>strong password policies</td>
<td></td>
</tr>
</tbody>
</table>

Challenges
Initiative – Interoperability and SSO

- Cross application and platform interoperability requirements varies from organization to organization
- Typical interoperability and SSO methods include
  - Integrating with server operating systems (SQL server, exchange, etc.)
  - Using LDAP authentication and authorization for applications
  - Using secure standards based authentication protocol like Kerberos
  - Implementing credential mapping and Enterprise SSO using products available in the market

<table>
<thead>
<tr>
<th>Benefits</th>
<th>Challenges</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Seamless application to application transfer</td>
<td>• Choosing the right technology for integration</td>
</tr>
<tr>
<td>• Eliminate multiple logins and authentication</td>
<td>and SSO</td>
</tr>
<tr>
<td></td>
<td>• Implementation costs increases from reduced</td>
</tr>
<tr>
<td></td>
<td>sign-on to full fledged SSO</td>
</tr>
</tbody>
</table>
### Initiative – Establish SW Development Standards

- Setting and enforcing standards that describe how applications interact with the Identity Management common infrastructure reduces the TCO and improves manageability
  - Standardizing and developing authentication components for custom developed applications
  - Developing Identity Management based standards for software procurement and integration

<table>
<thead>
<tr>
<th>Benefits</th>
<th>Challenges</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Applications can be developed rapidly without re-building IdM components.</td>
<td>• Designing a generic, scalable and robust authentication component</td>
</tr>
<tr>
<td>• Do not create new security problems</td>
<td>• Ensuring that the development specifications are adhered to and maintained</td>
</tr>
<tr>
<td>• Adheres to defined Architecture policies</td>
<td></td>
</tr>
<tr>
<td>• Reduces administrative costs</td>
<td></td>
</tr>
<tr>
<td>• Predefined security configurations specs for purchased applications</td>
<td></td>
</tr>
</tbody>
</table>
Identity Management Roadmap

Incremental value is achieved when adopting each of these identity solutions. However, maximum value is achieved when all aspects of the Identity Roadmap have been implemented.

- **Integrated Authoritative Source**: Populating the Identity Repository from HR, CRM or other authoritative source.
- **Identity Repository**: Consolidate user identities into a centralized repository.
- **Identity Roles**: Define user roles and policies.
- **Access Management**: Access management that provides authorization and authentication of users.
- **User Account Provisioning**: Using identity to provision applications and services.
- **Federated Identity**: Allows the interoperability of identities across companies and networks.
- **Portals**: Web single sign-on, enabled through a portal, provides access to web-enabled applications, content and services based on your identity.
- **Strong Authentication**: Incorporation of encryption, PKI, biometrics, and smart cards provide stronger levels of authentication.
- **Portals**: Web single sign-on, enabled through a portal, provides access to web-enabled applications, content and services based on your identity.
Critical success factors

• A complete view of security
  – Address core security solutions and key elements
  – Ensure management processes are included in the solution

• It takes people, methods and focus to implement solutions
  – Complete buy-in from Upper Management and all involved parties
  – Dedicated and effective Project Management that spans all involved departments
  – An Effective communication plan and escalation process
  – A security team that integrates with the business and IT Organizations

• A successful implementation means more than a functioning technology
  – Organizational alignment
  – Process and people integration
  – Data integration
  – Technical integration
  – Roll-out and maintenance approach
Summary – Things to Keep in Mind

• Identity Management is not cheap
• Identity Management is not a single solution or technology
• Identity Management is not a security panacea
• Implementation does not happen overnight and takes a lot of time and effort
• Implementation has to be carefully planned and needs the support of all the departments within the organization
• It is a foundation for a robust and scalable infrastructure
• As the organization grows more in size and complexity, the cost associated with IDM becomes easier to justify