Identity Management
Roadmap and Maturity Levels

Martin Kuppinger
Kuppinger Cole + Partner
mk@kuppingercole.de
Major Trends in Identity Management Guidelines for an IAM roadmap

Service-orientation:
- Identity Management has to provide defined services for applications and systems

Integration in Business Service Lifecycles
- Identity Management will become part of central approaches for Service Lifecycle Management, in the context of ITIL and change/configuration management

Convergence of Access Management and Federation
- Federation will become increasingly important as a means of centralized, policy-driven access management

End-to-End Auditing
- Auditing must be end-to-end, from the system up to the business level, to fulfill compliance requirements

Integrated User-centric IAM and “claims-based” approaches
- Users and their open identities will be fully integrated in enterprise IAM models
- Claims and Federation as a means for identity interoperability
## Level 1: Basic Identity Management

| Trusted Identity | • Internal users (no customers, no suppliers, no partners)  
|                  | • One trusted, central directory |
| Provisioning and Role Management | • Basic Provisioning, mainly HR-driven, focus on creation of users  
|                                  | • No or rudimentary role management |
| Single Sign-On and Authentication | • None beyond the level of network operating systems (Windows authentication) and isolated SSO-solutions |
| Access and Federation | • Web Access Management as point solution, no application integration  
|                       | • No Federation |
| Auditing, Policies, and Compliance | • Auditing only on system level  
|                                  | • No consistent policy-driven approach  
|                                  | • If at all, only point solutions for compliance |
# Level 2: Advanced Identity Management

**Trusted Identity**
- Internal user, customers, suppliers
- One consistent view on identities, independent of the type of user

**Provisioning and Role Management**
- Defined processes for creation, change, and deletion of users, consistent across all types of user
- Basic role management on the provisioning layer

**Single Sign-On and Authentication**
- Enterprise Single Sign-On
- Strong Authentication for internal users (Two-factor)

**Access and Federation**
- Multiple Access Management concepts on portal, application server and web access management level
- Singular Federation implementations

**Auditing, Policies, and Compliance**
- Policy-driven control for singular systems, no consistent approach
- Auditing and Compliance solutions on the system level, some degree of integration
Concept: Consistent identity

Central ID

Roles

System A
System B
System C
System D
System E

Employee
Customer
Supplier
...
Concept: Provisioning processes

Add new user
Change Attribute A
Request Role B
Delete
...

HR System
OM
Dept. Manager
HR Dept.
...

Defined Workflow
Defined Workflow
Defined Workflow
...

Provisioning-System

ERP
AD/eDir
LDAP
...

© Kuppinger Cole + Partner 2007
Concept: „Distributed“ Access Management

Web Access Management

- Browser
- Browser
- Browser
- Browser
- PEP
- App 1
- App 2
- App 3

Enterprise Portal

- Browser
- Browser
- Browser
- Browser
- Directory
- Portlet 1
- Portlet 2
- Portlet 3
- Portlet 4

Partial integration on different levels...
Concept: Basic compliance integration

Centralized Audit Application

Centralized Log Data

Decentral Audit Logs

Audit Log  Audit Log  Audit Log  Audit Log  Audit Log

Application  Provisioning-System  Application  Directory  Firewall
# Level 3:
Service-oriented Identity Management

<table>
<thead>
<tr>
<th>Category</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Trusted Identity</strong></td>
<td>• Defined storage service interfaces&lt;br&gt;• Separating applications and identity storage, use of identity storage virtualization</td>
</tr>
<tr>
<td><strong>Provisioning and Role Management</strong></td>
<td>• External/open provisioning workflows&lt;br&gt;• Enterprise Entitlement approaches in provisioning&lt;br&gt;• Enhanced role concepts</td>
</tr>
<tr>
<td><strong>Single Sign-On and Authentication</strong></td>
<td>• Authentication service, enabling Single Sign-On for applications&lt;br&gt;• Federation as a means for Single Sign-On</td>
</tr>
<tr>
<td><strong>Access and Federation</strong></td>
<td>• Federation as standard approach for distributed authentication and authorization&lt;br&gt;• Centralized federation services for service-oriented applications</td>
</tr>
<tr>
<td><strong>Auditing, Policies, and Compliance</strong></td>
<td>• Consistent policy approach across systems&lt;br&gt;• Audit log service interfaces for access to different logs&lt;br&gt;• Pre-defined compliance services</td>
</tr>
</tbody>
</table>
Concept: Identity storage services

Providing a virtual set of attributes to applications

Application

Virtual Directory

Virtual Directory

Virtual Directory

Virtual Directory

Virtual Directory Services

Active Directory

Corporate Directory

...
Concept: Further identity services
Concept: Provisioning and enterprise entitlement

Today
- Provisioning System
  - Workflows
  - Account Management
  - Group/Role Assignment
- Rights Assignment
- Connected Systems Layer

Tomorrow - optional
- Workflow System
  - Workflows
- Provisioning System
  - Account Management
  - Group/Role Assignment
  - Rights Assignment
- Rights Assignment
- Connected Systems Layer

© Kuppinger Cole + Partner 2007
### Level 4: Business-driven Identity Management

| **Trusted Identity** | • Full integration with external identities and user-centric IAM  
|                       | • Integration of all identity systems (e.g. CRM, Supplier Management,...) |
| **Provisioning and Role Management** | • Business role management for control of information and system access  
|                                     | • Role-driven Information rights management  
|                                     | • Full integration into business service management |
| **Single Sign-On and Authentication** | • Single Sign-On for all types of users with the appropriate mechanism |
| **Access and Federation** | • Consistent access management and authorization in integration with federation technologies and business-driven control |
| **Auditing, Policies, and Compliance** | • Cross-system policies for control of information and system access  
|                                     | • Consistent compliance automation across all systems |
Concept: Consistent identities and Sign-On

Example: Customer identity

„Internet“-ID maps to „Enterprise“-ID

„Enterprise-ID maps to still existing accounts and systems with customer data
Concept: Business-driven control of information and systems

- Business Role Management
  Assignment through Dept. Manager

- Information Rights Management:
  Assignment through Information Owner

- Mapping of Business Roles to "tech roles/groups":
  Provisioning layer

- Assignment of concrete rights:
  Controlled through business, implemented consistently from Business layer to system layer

© Kuppinger Cole + Partner 2007
Concept: Business service integration
Concept: Compliance automation

Compliance Dashboard

Compliance Policies

Policy Enforcement

Audit Log Collection

System A
System B
System C
System D
Roadmap: Trusted identity

Basic Identity Management
- Establishing Identity Information Quality

Advanced Identity Management
- Establishing a central ID concept

Service-oriented Identity Management
- Separating ID storage from applications and systems

Business-driven Identity Management
- Integrating ID-driven business systems
Roadmap overview

- **Basic Identity Management**
  - Establishing Identity Information Quality

- **Advanced Identity Management**
  - Establishing a central ID concept

- **Service-oriented Identity Management**
  - Separating ID storage from systems and applications

- **Business-driven Identity Management**
  - Integrating ID-driven business systems

- **Trusted Identity**
  - Basic Identity Management

- **Provisioning and Role Management**
  - Advanced Identity Management
  - Service-oriented Identity Management
  - Business-driven Identity Management

- **Single Sign-On and Authentication**
  - Basic provisioning processes
  - Role-based, complete Provisioning
  - Enhanced role and entitlement management
  - Business role-driven, Business service-driven

- **Access and Federation**
  - System-oriented, decentralized Sign-On
  - E-SSO e/ strong authentication
  - Defined authentication services
  - SSO for all types of users

- **Auditing, Policies, and Compliance**
  - Basic (Web) Access Management
  - Decentralized access management integration
  - Centralized federation services
  - Integrated access management
  - Audit an compliance services
  - Consistent, policy-driven compliance automation

© Kuppinger Cole + Partner 2007
Roadmap: Provisioning and Role Management

Basic Identity Management
- Basic provisioning processes

Advanced Identity Management
- Role-based, complete Provisioning

Service-oriented Identity Management
- Enhanced role and entitlement management

Business-driven Identity Management
- Business role-driven, Business service-driven
Roadmap: Single Sign-On and Authentication

Basic Identity Management
- System-oriented, decentralized Sign-On

Advanced Identity Management
- E-SSO w/ strong authentication

Service-oriented Identity Management
- Defined authentication services

Business-driven Identity Management
- SSO for all types of users
Roadmap: Access and Federation

- Basic Identity Management
  - Basic (Web) Access Management

- Advanced Identity Management
  - Decentralized access management integration

- Service-oriented Identity Management
  - Centralized federation services

- Business-driven Identity Management
  - Integrated access management

© Kuppinger Cole + Partner 2007
Roadmap: Auditing, Policies and Compliance

- Basic Identity Management
  - System-level auditing

- Advanced Identity Management
  - Policy approaches on system level

- Service-oriented Identity Management
  - Audit and compliance services

- Business-driven Identity Management
  - Consistent, policy-driven compliance automation
Measuring your status: Fulfilment on different levels

Basic Identity Management
- Establishing Identity Information Quality

Advanced Identity Management
- Establishing a central ID concept

Service-oriented Identity Management
- Separating ID storage from systems and applications

Business-driven Identity Management
- Integrating ID-driven business systems

Trusted Identity
- Basic provisioning processes

Provisioning and Role Management
- Role-based, complete Provisioning

Single Sign-On and Authentication
- System-oriented, decentralized Sign-On

E-SSO e/ strong authentication

Defined authentication services

SSO for all types of users

Access and Federation
- Basic (Web) Access Management

Decentralized access management integration

Centralized federation services

Integrated access management

Auditing, Policies, and Compliance
- System-level auditing

Policy approaches on system level

Audit an compliance services

Consistent, policy-driven compliance automation

© Kuppinger Cole + Partner 2007
Defining the next steps: Identifying work areas

Target:
1. Business control of information
2. Integration with Business Service Management
3. Defined Application Security Infrastructure

Basic Identity Management
- Establishing Identity Information Quality
- Establishing a central ID concept
- Separating ID storage from systems and applications
- Integrating ID-driven business systems

Advanced Identity Management
- Role-based, complete Provisioning
- Enhanced role and entitlement management
- Business role-driven, Business service-driven

Service-oriented Identity Management
- Basic provisioning processes
- Role-based, complete Provisioning
- Enhanced role and entitlement management
- Business role-driven, Business service-driven

Business-driven Identity Management
- Basic Identity Management
- Advanced Identity Management
- Service-oriented Identity Management
- Business-driven Identity Management

Provisioning and Role Management
- Trusted Identity
- Establishing Identity Information Quality
- Role-based, complete Provisioning
- Enhanced role and entitlement management
- Business role-driven, Business service-driven

Single Sign-On and Authentication
- System-oriented, decentralized Sign-On
- System-oriented, decentralized Sign-On
- SSO for all types of users
- Integrated access management

Access and Federation
- Basic Identity Management
- Advanced Identity Management
- Service-oriented Identity Management
- Business-driven Identity Management

Auditing, Policies, and Compliance
- Basic Identity Management
- Advanced Identity Management
- Service-oriented Identity Management
- Business-driven Identity Management
Identity Management Roadmap Fast Track

- Define and implement a central ID concept
- Create an identity service layer at least for storage and authentication
- Start with business role management
- Use pre-defined provisioning processes (GenericIAM)
- Implement E-SSO
- Use Federation whenever appropriate
- Focus on policy-driven systems

Not complete, but feasible...
Vendor call to action: Missing technologies

- Exchangeable provisioning processes – using BPEL?
- Exchangeable policies
- Standardization of audit log entries and interfaces
- Role-drive, cross-platform/-vendor Information Rights Management
- Optional enterprise entitlement to the system level