Identity Management Basics

Derek Browne, CISSP, ISSAP
Derek.Browne@Emergis.com

OWASP

May 9, 2007

Emergis

The OWASP Foundation

http://www.owasp.org

Agenda

1. **Identity Management Overview**
2. Concepts
3. Approach to Identity & Access Management
4. Example Scenarios
5. Product Demonstrations**…hopefully…**

Identity Management Flavours

- Single Sign On is a goal … not a product
- Web application integration -- Web SSO
- Enterprise SSO (eSSO) involves corporate desktop application
  - Some use a server -- TSE, tn3270/5250, SAP, Oracle forms, etc
  - Some authenticate locally -- acrobat protected files
- IdM is different than Access Management
  - One involves who you are and how that is recorded
  - The other involved the policies around how you access resources
- Federation of identities across multiple jurisdictions
  - SAML, SXIP, Identity 2.0, OASIS
  - Passport (HAHA), Kerberos, Liberty

Identity Management Overview

Defined:

- Central infrastructure to manage users, roles, and access to resources
- Concept of “identity” contains all user attributes
- Provisioning capabilities
  - Technology (connectors)
  - Approvals Workflow Management

Features:

- Identity provisioning among integrated directories
- Self-registration and management
- Delegation of approvals and workflows
- Password reset capability

Benefits:

- Meet regulatory & audit requirements around controlled access to resources
- Save costs through efficient workflows for provisioning and approval
- Asset (business) owners in control, rather than technology group

Identity Management Integration

Integrates with:

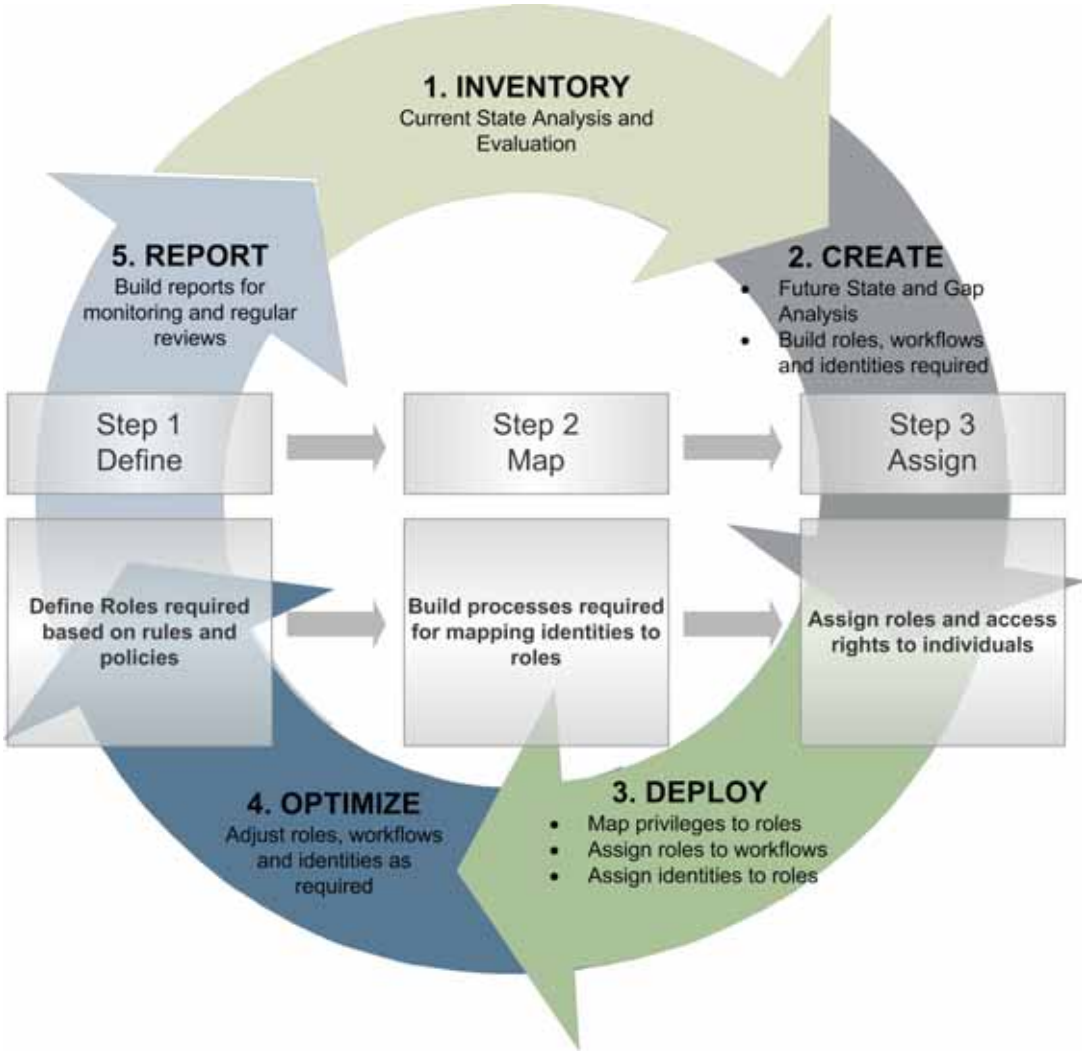
- Enterprise single-sign-on (and related strong authentication)
- Access Management systems
- Role Engineering / Management systems

Integration Risks:

- Focus on technology may distract from importance of roles and processes
- Too many roles (or exceptions) may result if access modeling and identity modeling are not well-planned
- Benefits may not be realized quickly if project scope is not managed
- Not respecting impact on business and applications may have adverse effects on buy-in and acceptance
- Ineffective processes and workflows may prevent cost savings from being realized
- Lack of proper knowledge transfer results in a system that the organization cannot effectively manage

Identity & Access Management Methodology

1. **Inventory:** gather information about users, access requirements, and applications & data
2. **Create:** future state roadmap, associating user groups with access controls, and designing operational support and workflow processes
3. **Deploy:** begin assigning access to systems and data using new processes and workflows
4. **Optimize:** deploy automated and delegated processes only after steady state has been achieved
5. **Report:** leverage investment to satisfy reporting requirements for legislation and internal controls



75 percent of deployment effort will be spent on people & process

Agenda

1. Identity Management Overview
2. **Concepts**
3. Approach to Identity & Access Management
4. Example Scenarios
5. Product Demonstrations

Identity & Access Management Basics

Access Management

- **Access to data or applications is defined by**
  - Business policies (segregation of duties)
  - Security policies
  - Industry regulations and customer requirements
- **Access permissions are mapped to roles and rules to be used when managing identities**

Identity Management

- **Map roles and rules to specific users to allow appropriate access**
- **Process to manage and track access to systems and data**
  - Provisioning
  - Workflow
  - Auditability

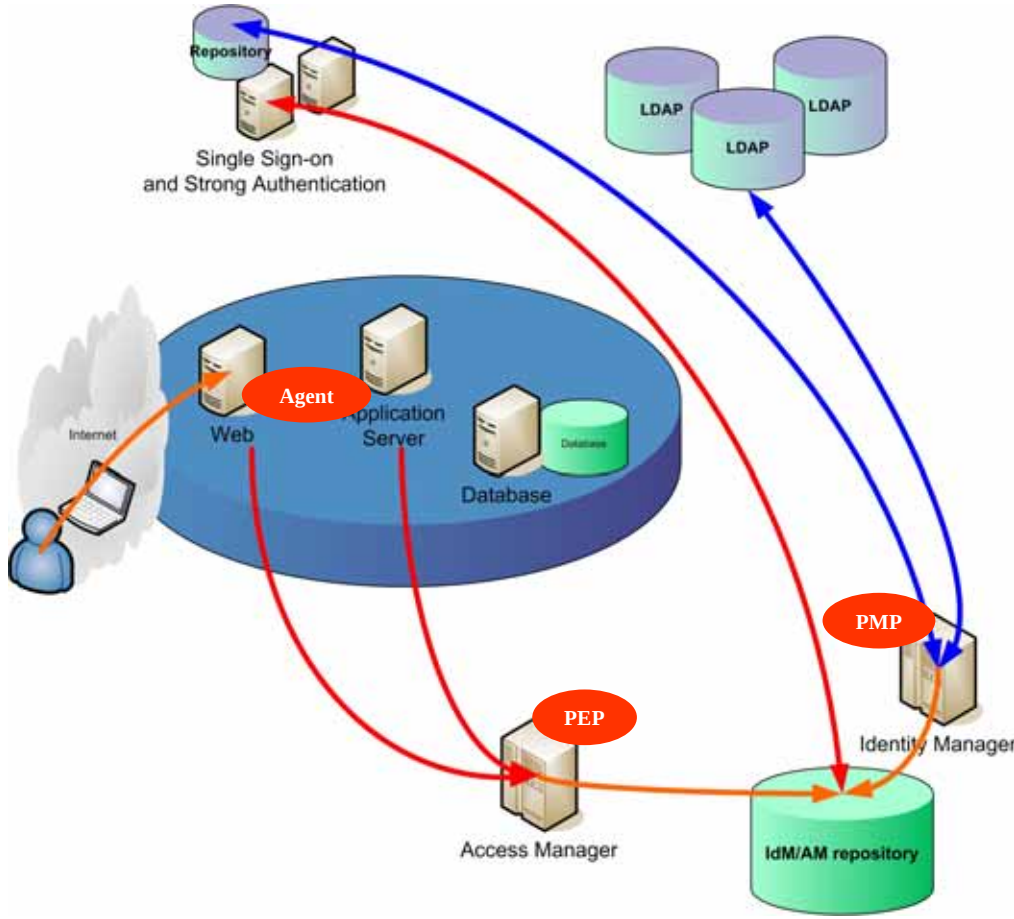
Tools exist to facilitate the mapping and ongoing management of roles & identities

Single Sign-on & Strong Authentication

- **Single sign-on allows access to all resources – strong authentication is required**

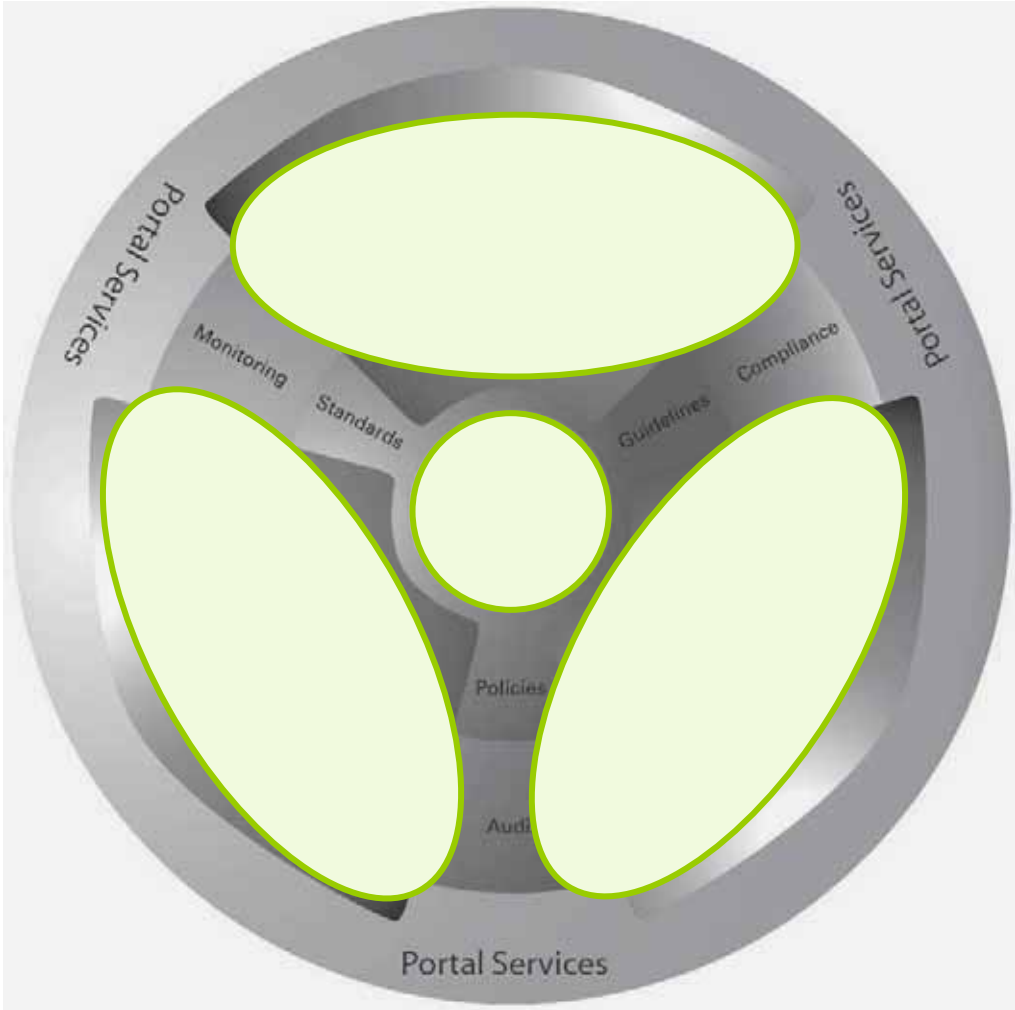
Identity & Access Management Systems

1. User connects to Web server
2. Web server has a connector or "**Agent**"
   - An interface to the Access Manager
   - 'plug-ins' or APIs
3. Access Manager is Policy Enforcement Point: "**PEP**"
   - High-volulme system to make decisions on access requests from the Web server
   - Must be high-availability
4. Identity Manager is the Policy Management Point: "**PMP**"
   - Central management of all identity information from various sources
   - Able to define processes and workflows to manage, maintain, and audit access to resources.



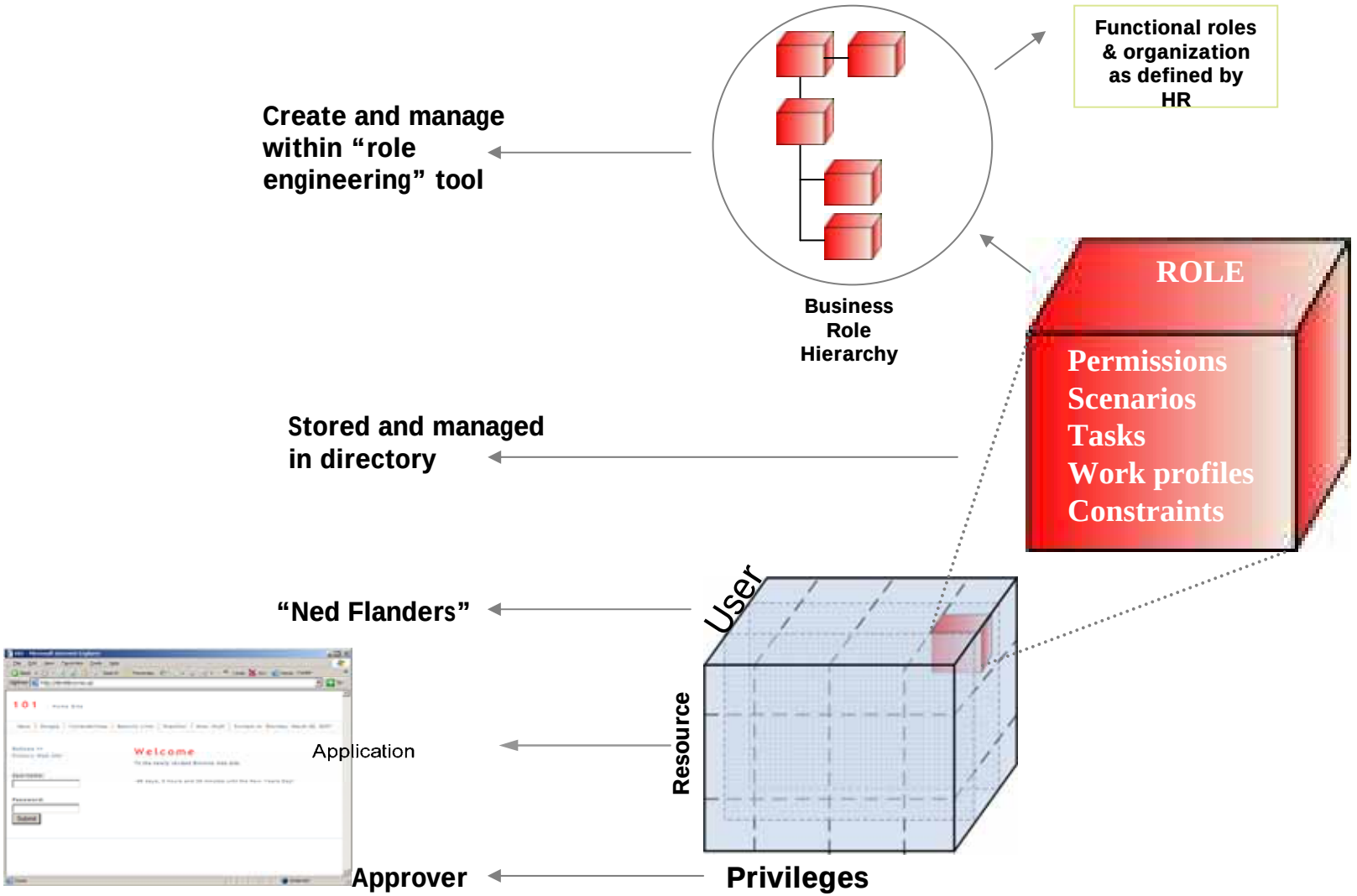
Identity Management Framework

- Directory services repository is the most critical component, and is the primary data store for user-ID and profile information.
- Provisioning provides a role-based approach to end-to-end user lifecycle management
- Authentication –leverage existing systems including Active Directory, Enterprise Single Sign-on, and RSA tokens.
- Access Management – leverage existing access manager infrastructure



Leverage existing technologies and processes

Role Based Access Control



Role Engineering – Process

- RBAC is widely supported and solves the Privilege management problem better than DAC or MAC, etc. but development of the Role Hierarchy is manual and utilities are few and not all are effective.

The role engineering process...

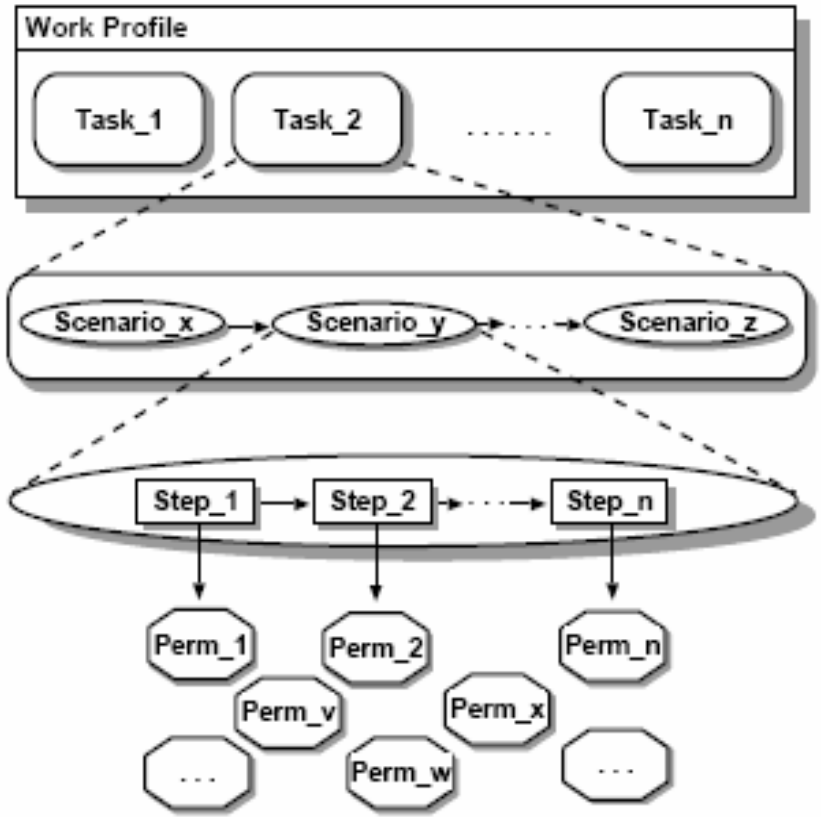
- Discovers Orphaned accounts, privileges, roles
- Merges overlapping roles
- Breaks apart overly broad roles: multiple jobs done by the same organization?
- Defines *Role* constraints that come from *permission* constraints
- Creates role hierarchies: junior roles with common bases

...and provides the benefits of...

- Cleanup and streamline privileges and group definitions
- Essential for ongoing privilege management
- Assists with & documents compliance with policies

Role Engineering – Creating Roles

- **Functional Decomposition**
  - Matter of pulling apart the existing processes and relationships between resources and users and their jobs
  - Understanding the interactions that constraints that exist on permissions
- **“Scenario-Driven”**
  - Models the usage of the system overall
  - Goal is to establish RBAC from concrete Role Hierarchies

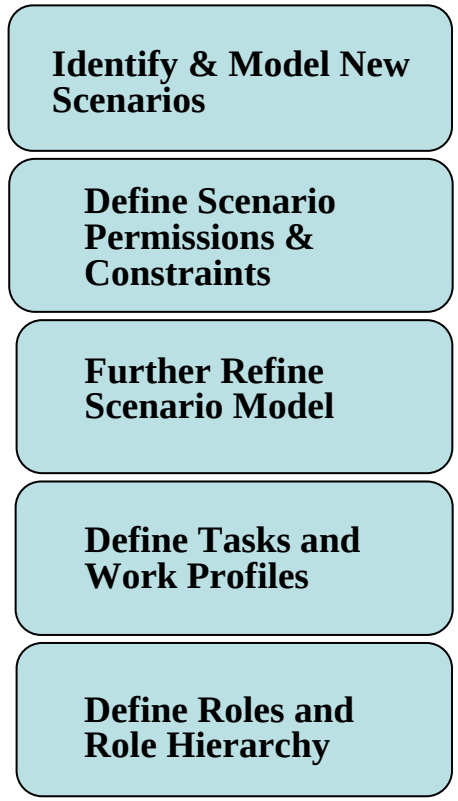


“bottom-up” approach

Role Engineering – Process

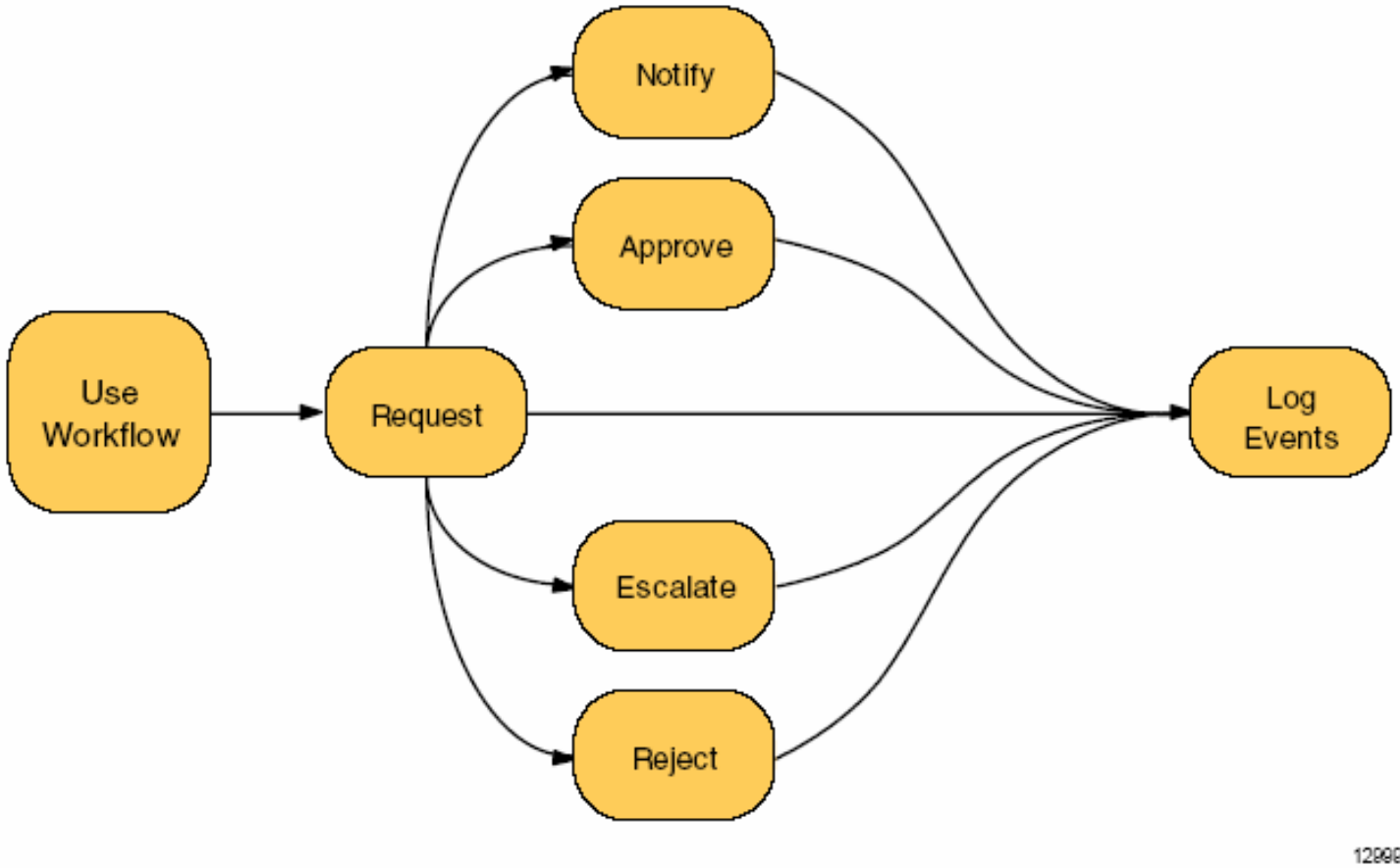
- Each IdM tool integrates a set of features to assist

- Bridgestream (SmartRoles)
  - Manages dynamic approval processes based on context and relationships
  - Does this by assuming the job of managing roles...all roles
  - Defines Approval Policies to control relationships
- Eurekify (Sage)
  - Can provide Query and Discovery functions – preliminary review of privilege landscape
  - Provides audit and compliance reporting on business roles
- xoRET
  - Initial Attempt at tool for scenario based role engineering
- Ultimately R.E. has so many human factors that there are key manual efforts required



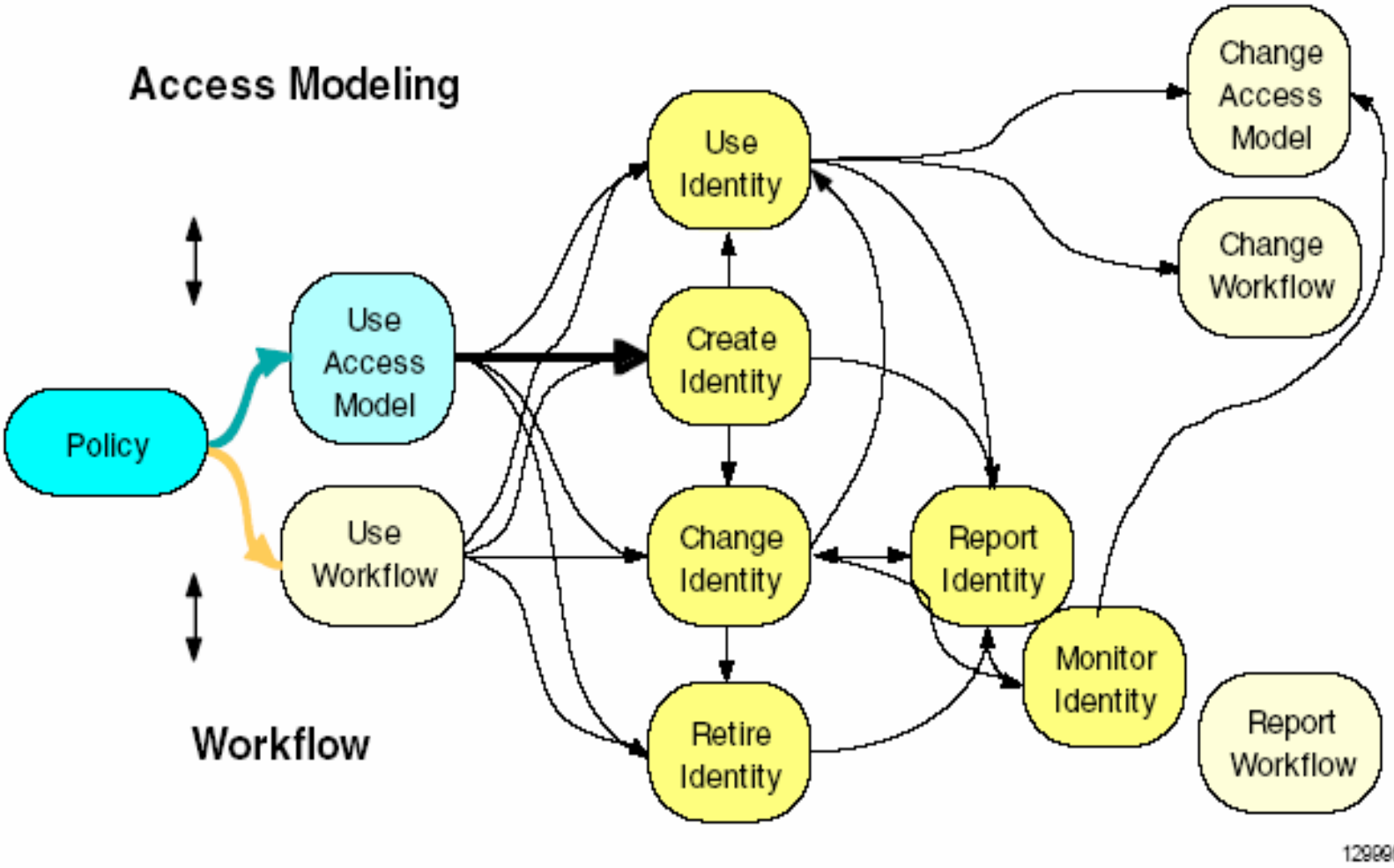
Logging & Monitoring is Critical

Figure 9. Use Workflow Subprocess



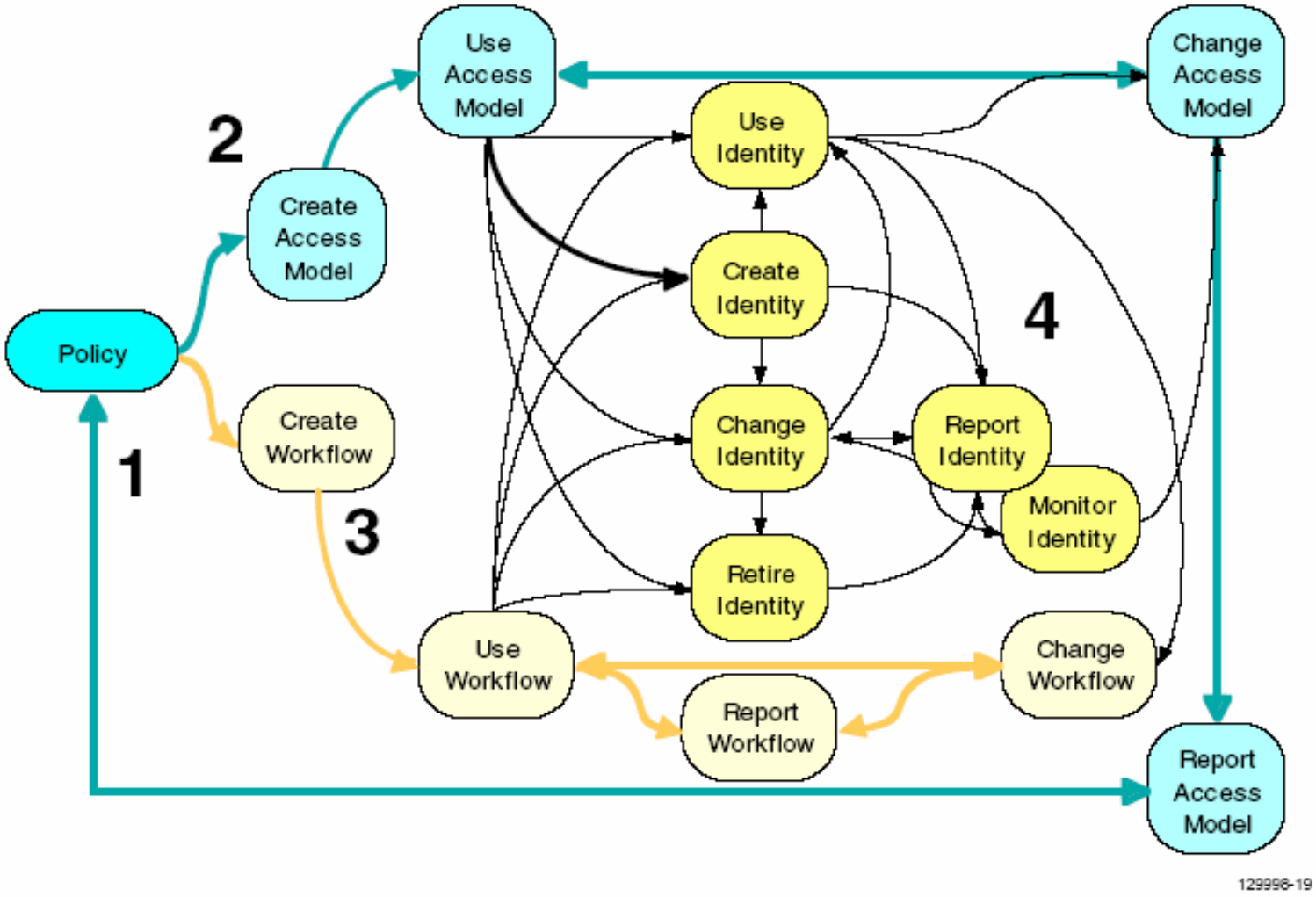
Source: Gartner (July 2005)

Figure 12. Identity Modeling Process



Source: Gartner (July 2005)

Figure 19. IAM as a Process

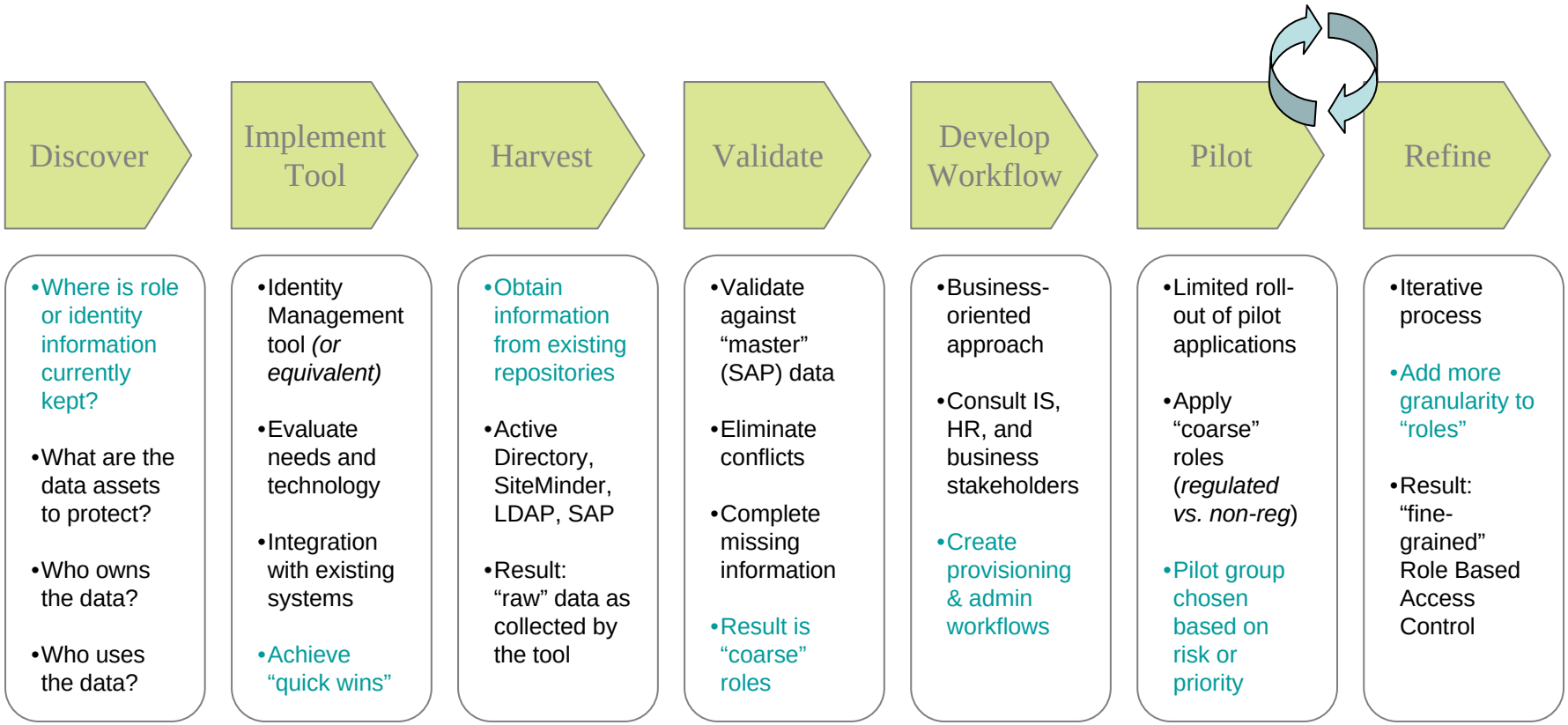


Source: Gartner (July 2005)

Agenda

1. Identity Management Overview
2. Concepts
3. **Approach**
4. Example Scenarios
5. Product Demonstrations

Applying a Methodology

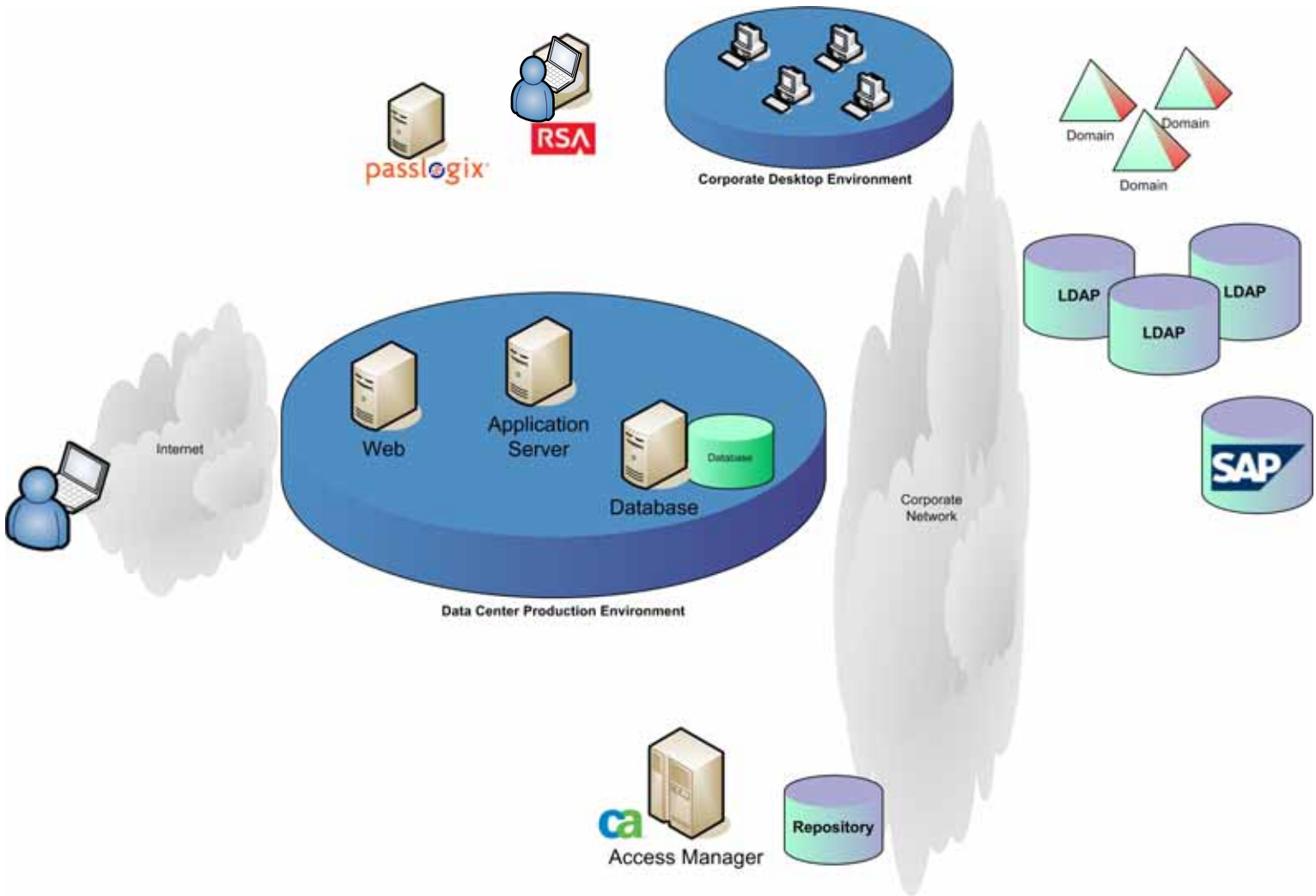


The actual process will not be linear…

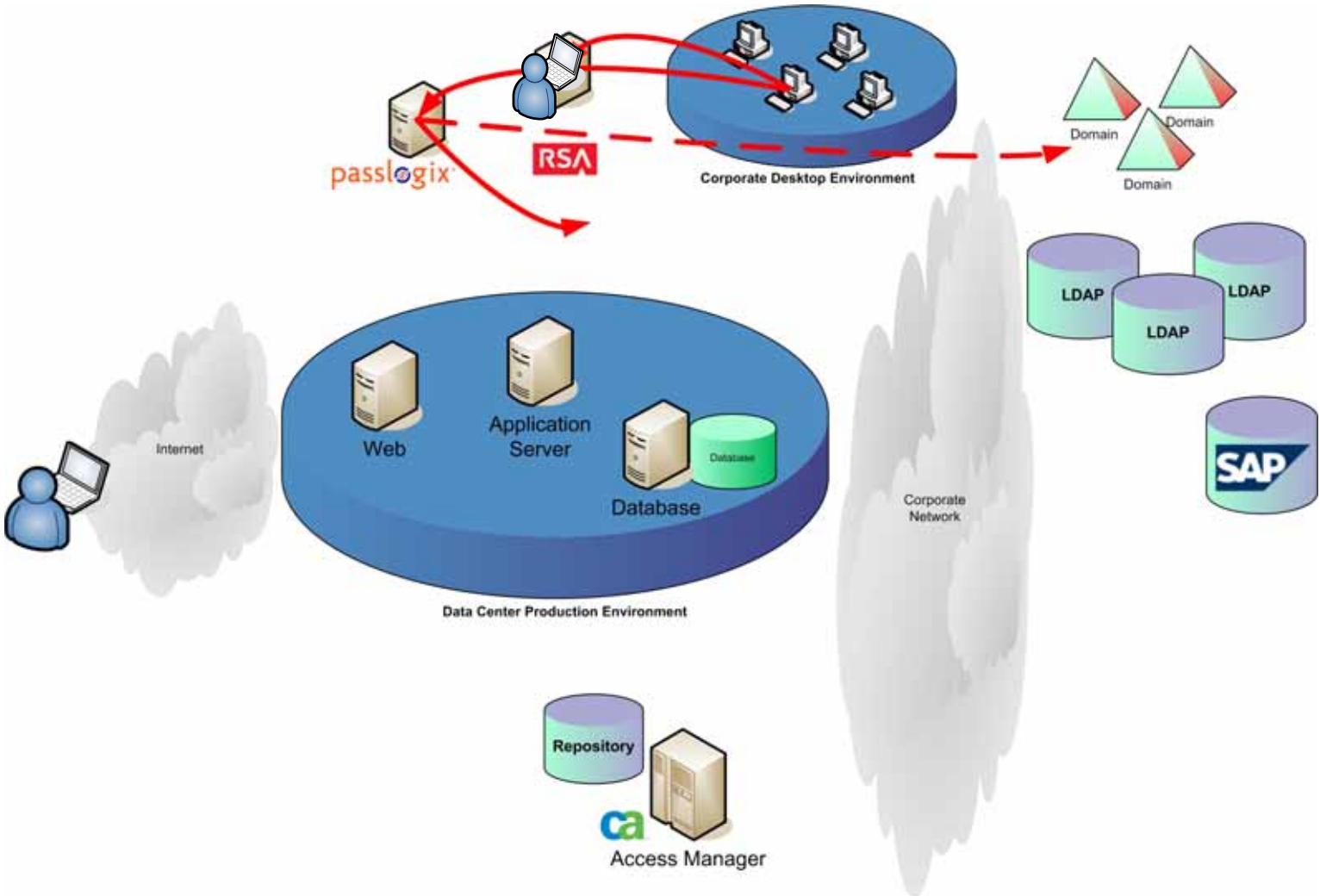
Agenda

1. Identity Management Overview
2. Concepts
3. Approach
4. **Example Scenarios**
5. Product Demonstrations

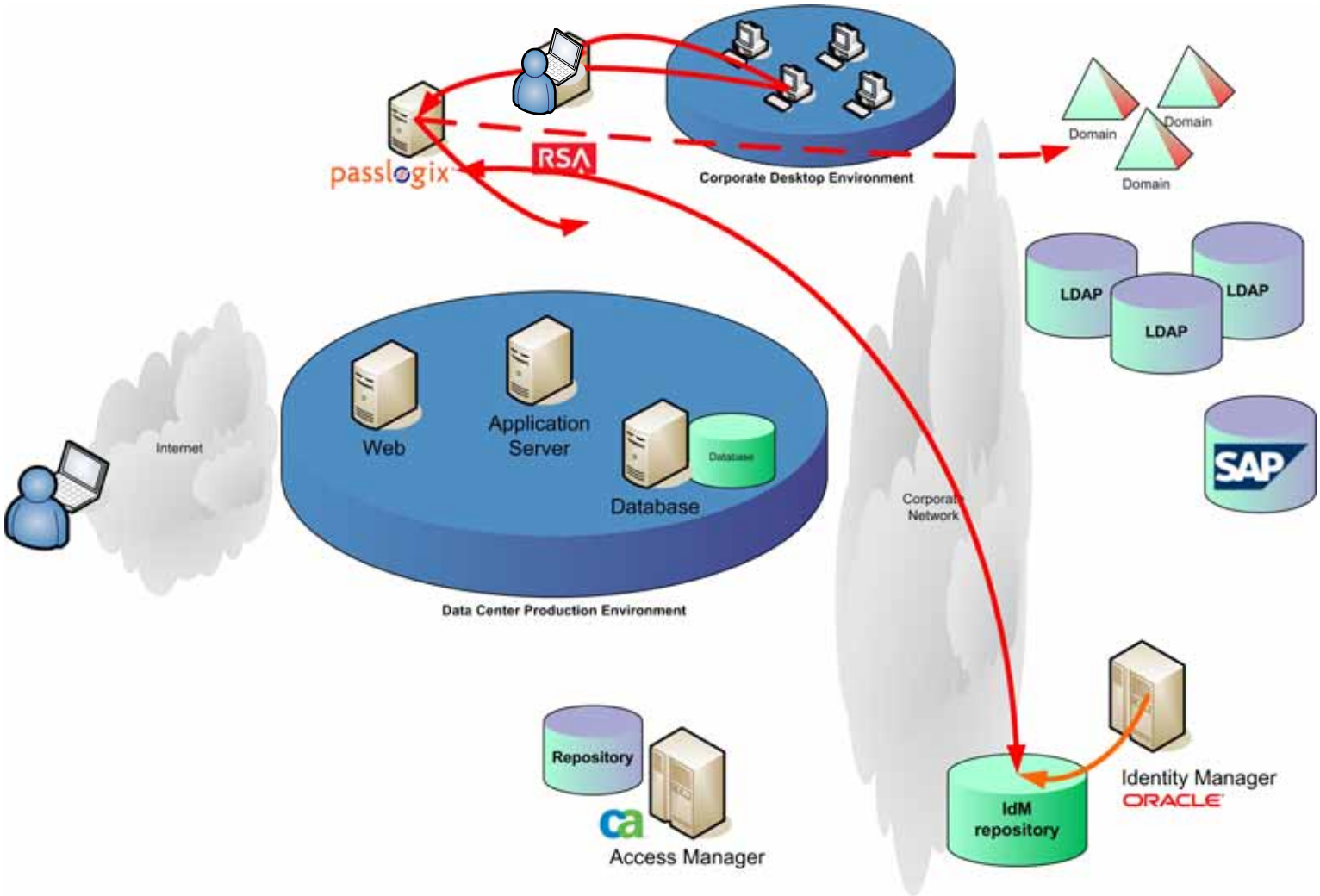
Typical Environments



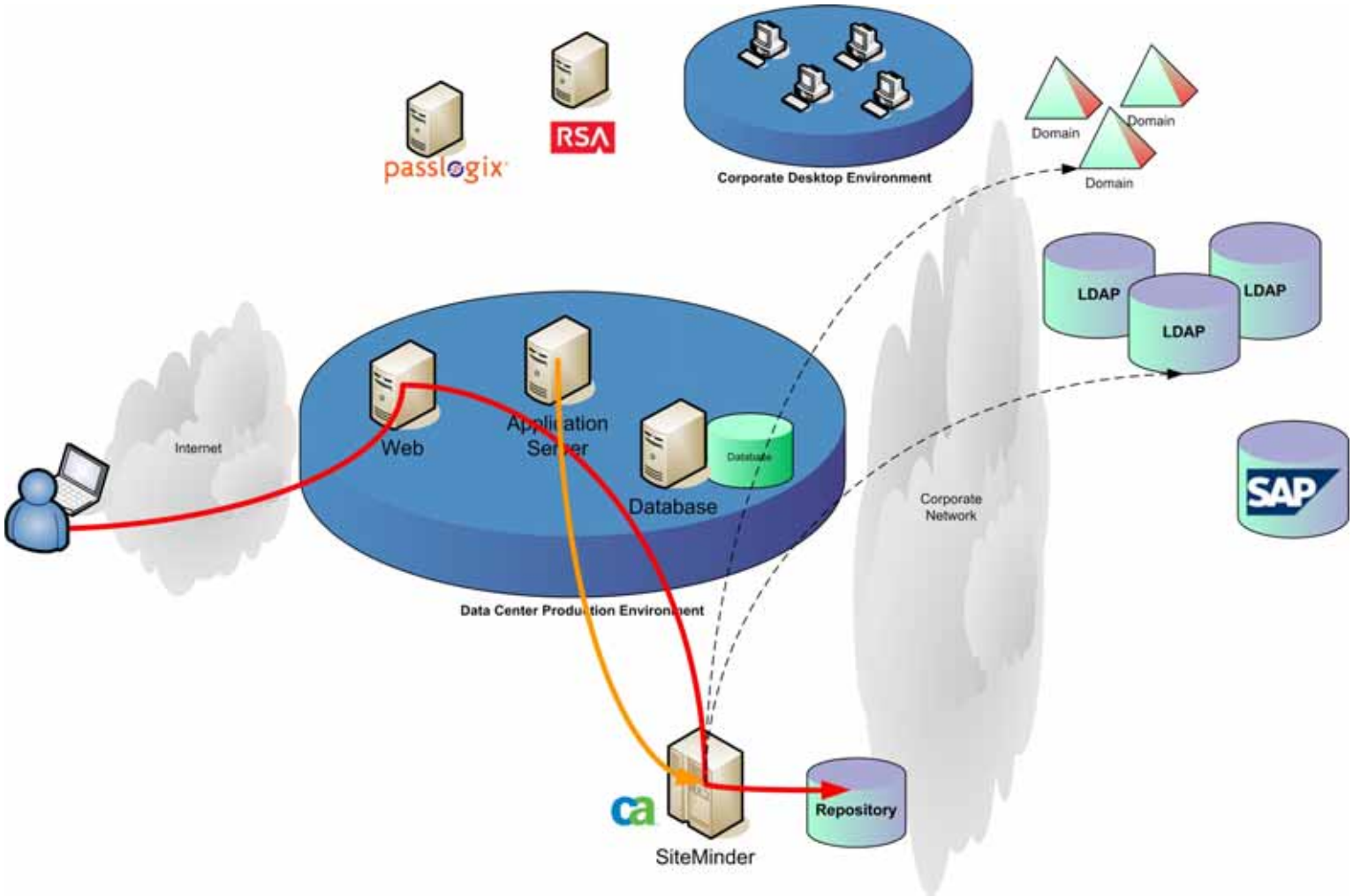
Enterprise Single Sign-on



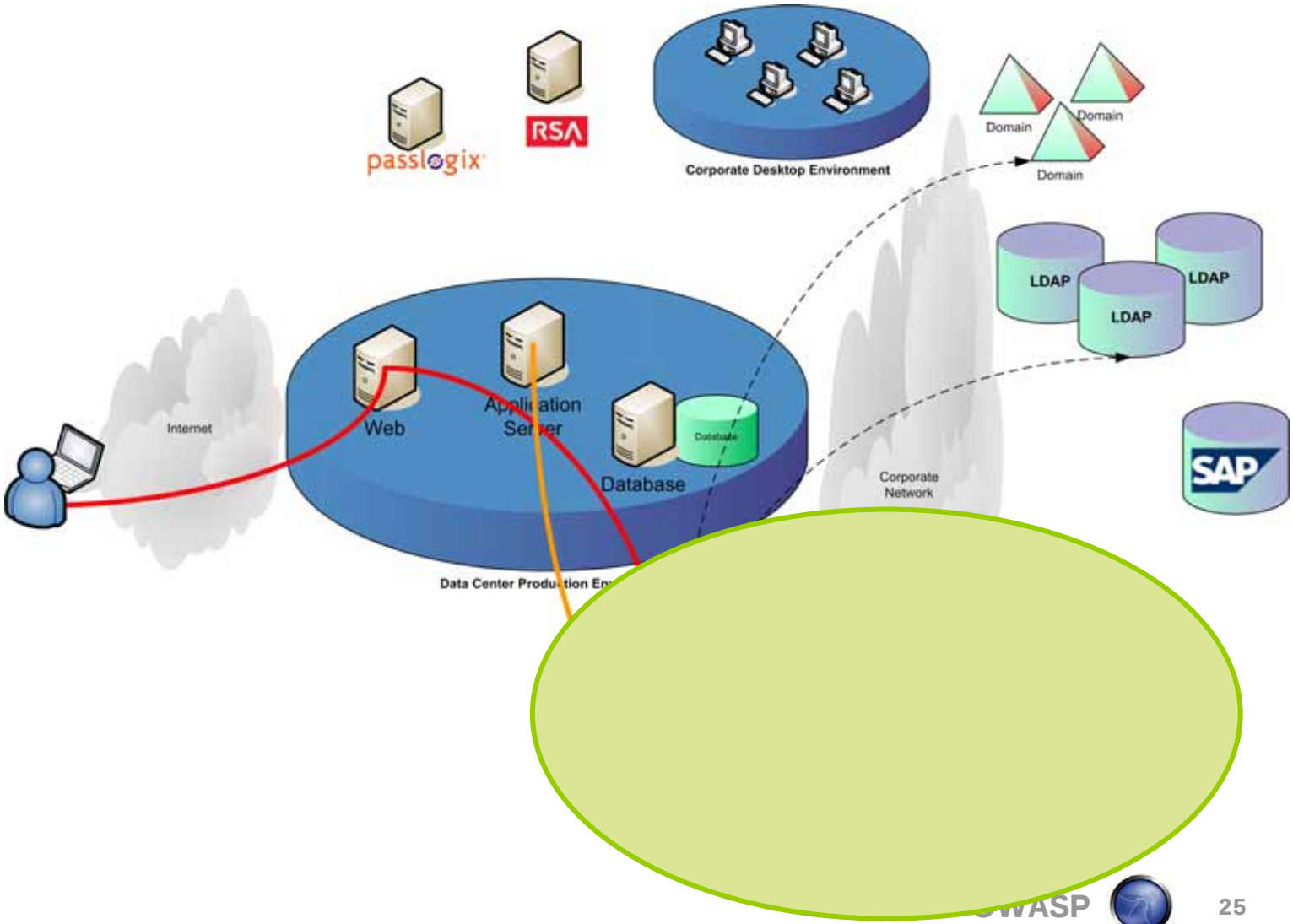
Enterprise Single Sign-on with IdM



Access Management

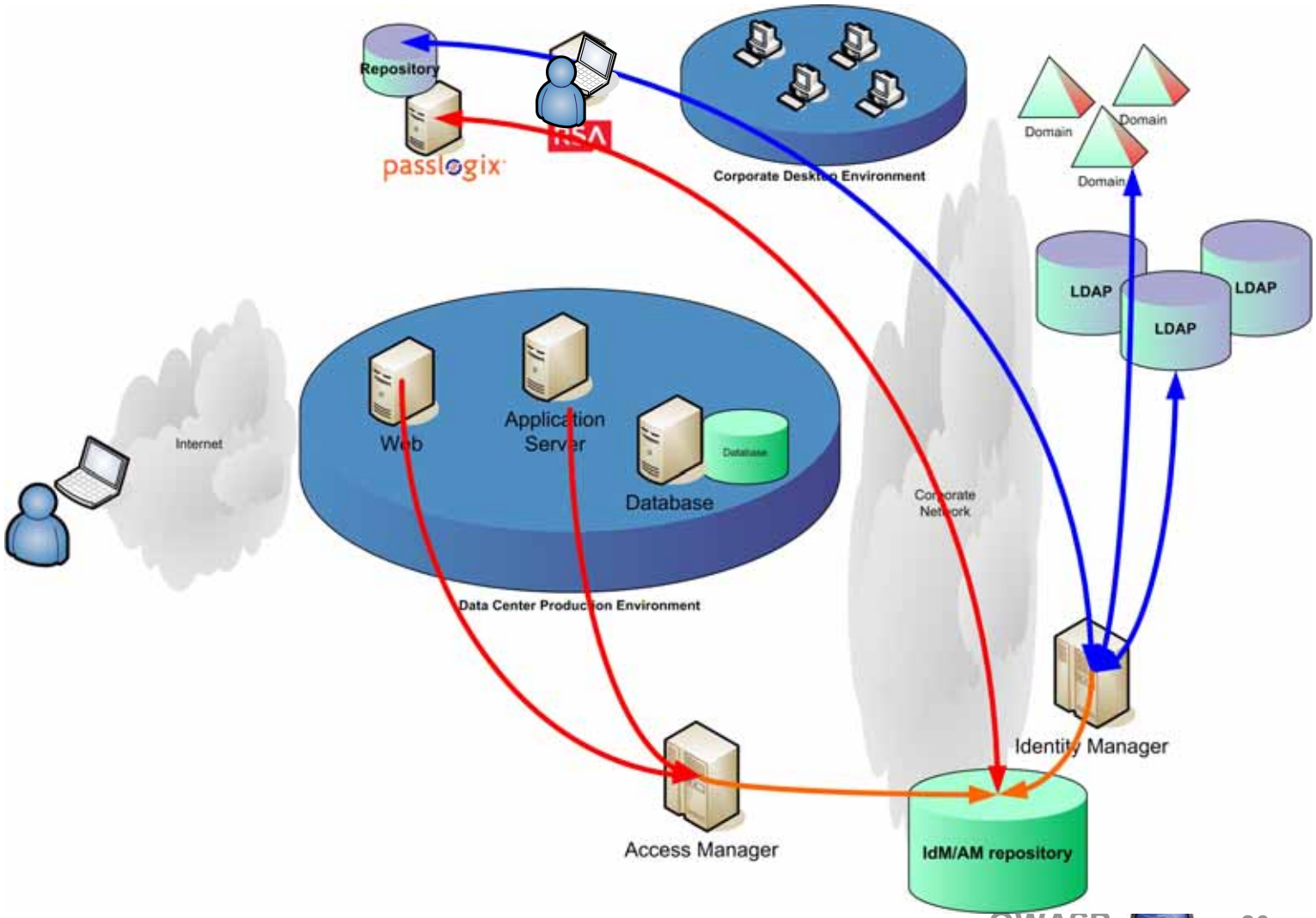


Access Management with IdM



Integrated Identity & Access Management

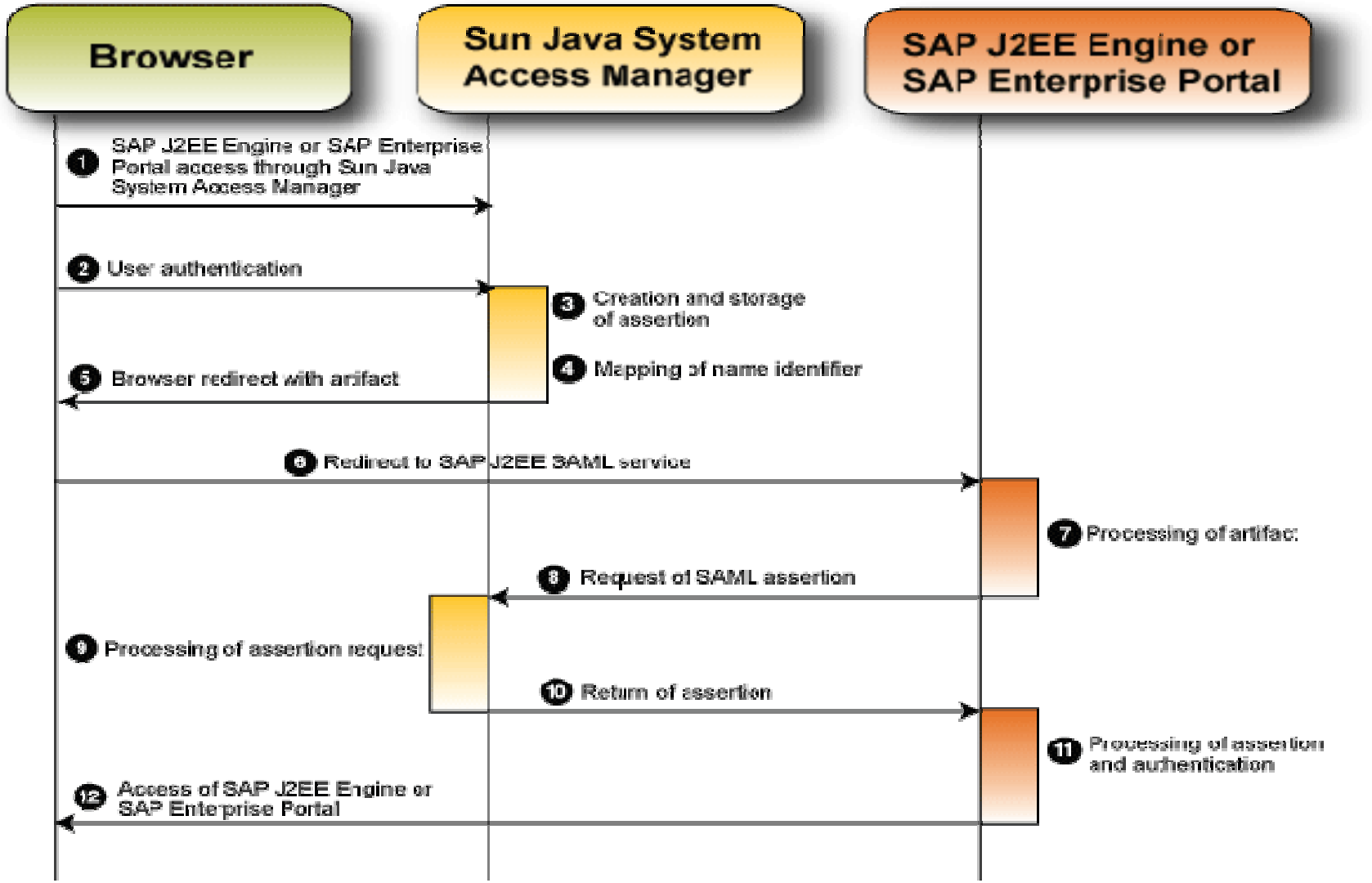
IdM Without Context



SAML

- Primary concern is Complexity
  - Built by committee – but so was IPSec
  - Motivated backers
  - Seasoned backers
- Synchronized clocks for validation
- Multitude of Trust relationships
  - A trusted third party resolves this but not mandatory

SAML Data Flow



Sun 2007
http://developers.sun.com/identity/reference/techart/sso.html

Options - What are the Choices

- Key Vendors in this area include (no ranking) ...
  - Sun
  - Oracle
  - Computer Associates
  - BMC Software
  - Novell
  - Passlogix
  - Imprivata
  - RSA
  - Many others...
- Competitive Analysis is being prepared now
  - Criteria being defined...
    - Federation
    - Audit capability
    - Encryption capability
    - Workflow flexibility

Agenda

1. Introductions and Objectives
2. Concepts
3. Approach to Identity & Access Management
4. Example Scenarios
5. **Product Demonstration…hopefully…**

Links as of June 1, 2007

- Sun
  - http://www.sun.com/download/index.jsp?cat=Identity%20Management&tab=3
- Oracle
  - http://www.oracle.com/technology/products/id_mgmt/index.html
- SXIP
  - http://www.sxip.com
  - http://identity20.com

- Derek Browne, CISSP, ISSAP
- derek.browne@emergis.com