

Designing Roles for Identity Management A Real World Guide

Patrick O’Kane
Unisys Corporation

Digital Id World, October 27, 2004

- > **Systems Integration.**
- > **Outsourcing.**
- > **Infrastructure.**
- > **Server Technology.**
- > **Consulting.**

UNISYS

Imagine it • Done •

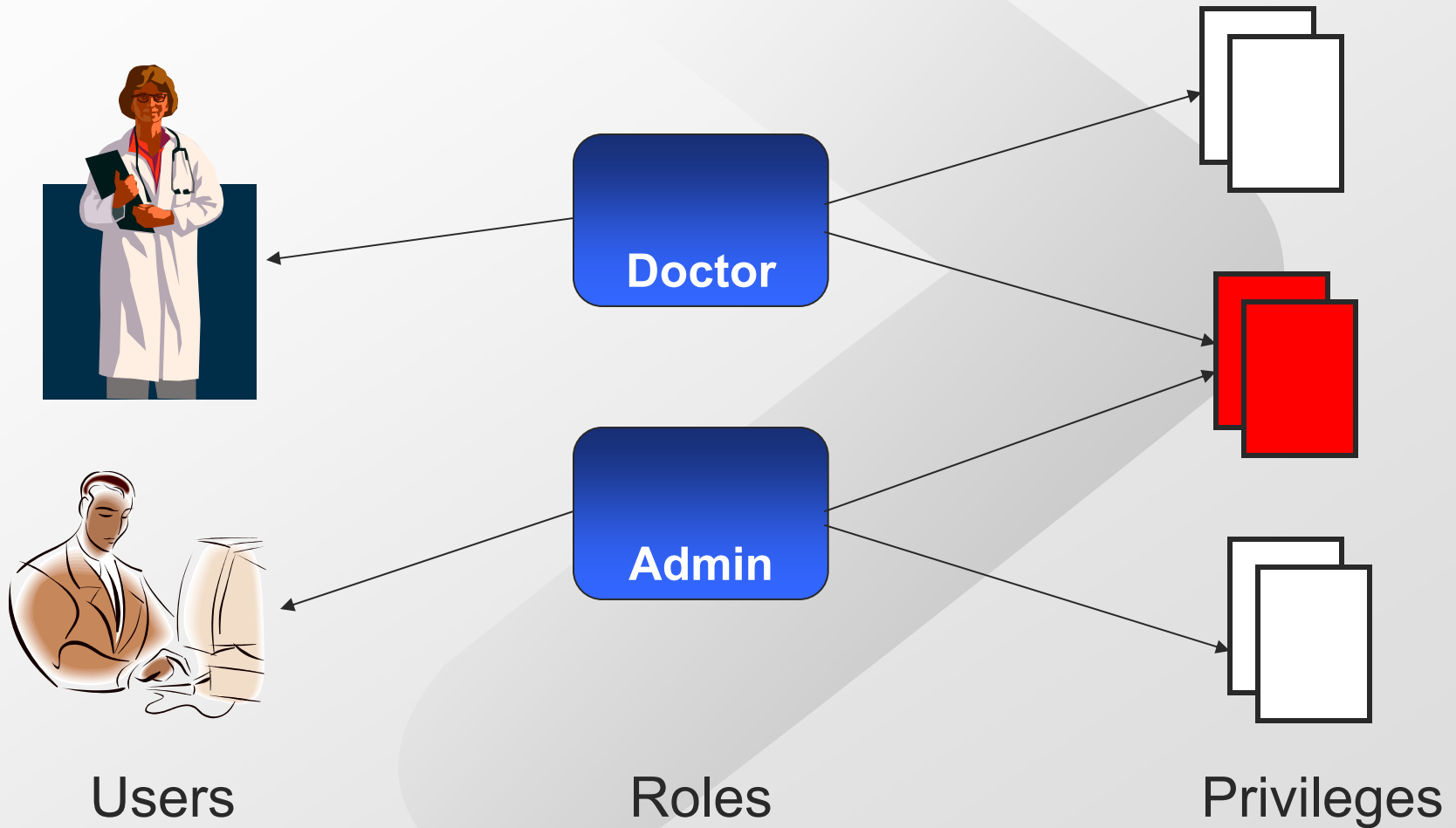
Agenda

- > **The RBAC concept within Identity Management**
- > **The state of RBAC today**
- > **Designing Roles**
- > **Top-down role design**
- > **Bottom-up role design**
 - Eurekaify Sage Role Mining Demo
- > **Best practice summary**

The RBAC Concept

- > RBAC = **Role** Based Access Control
- > **Components: Privileges, Users, Roles**
 - Separation of duty, constraints (time of day, remote vs. local)
- > **Privileges are abstracted for modeling**
 - Ultimately mapped to real systems and resources
 - Range from transaction security to physical assets
- > **Privileges are grouped in roles**
 - Roles may be further organized into hierarchies to reduce redundancy
 - Roles are integrated into systems that support RBAC
- > **Users are associated with roles not privileges**

The RBAC Concept



RBAC Today

> The RBAC challenge

- Concept to reality – RBAC is challenging to implement
- Role design is the first step

> Regulatory compliance re-accelerating the move to RBAC

- **Prove** access and management controls

> RBAC vs. RBAP

- Access control using roles
- Access provisioning using roles

> Broad vendor support for RBAC

- Microsoft, IBM Tivoli, CA/Netegrity, Courion ...

> Rules vs. Roles

- Complementary concepts but roles are the design base

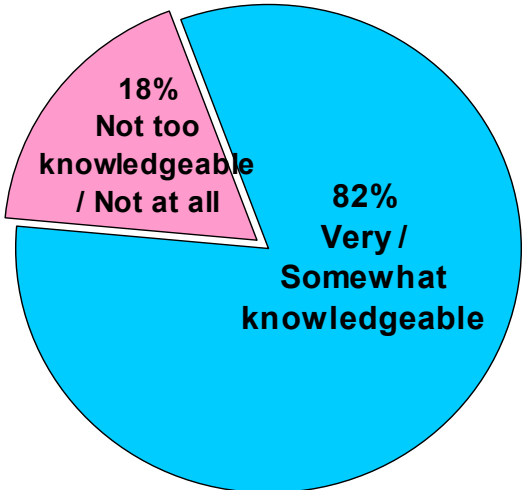
> Federated identity roles

- Role based federated access
- Privacy enhanced anonymous access

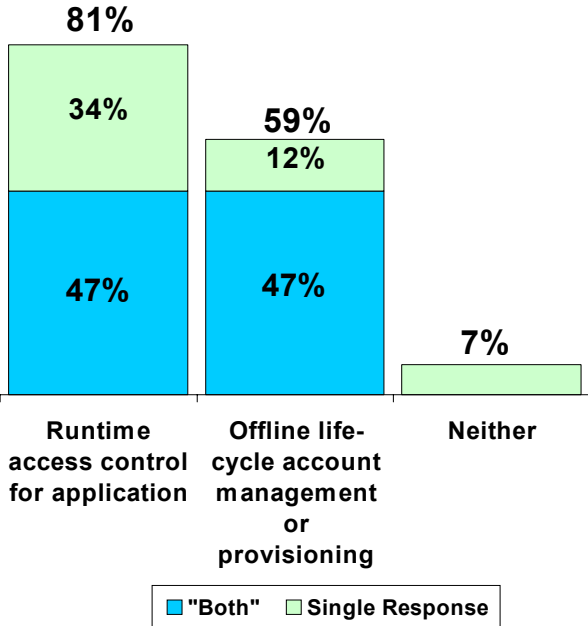
Unisys IAM Survey Results - RBAC

Uses of Role-Based Access Control

Knowledge of RBAC



Ways to Consider Using RBAC



RBAC Today - Resources

> NIST RBAC (csrc.nist.gov/rbac)

- ANSI Standard as of Feb-04
 - INCITS 359-2004

> The NAC (netapps.org)

- Success with roles and externalized authorization

Role Design Approaches

> Top-down design: Idealized approach

- Business model (not IT requirements) focus the approach
- Zero based analysis
- Mapping roles to access privileges

> Bottom-up design: Real world approach

- Current state based analysis
- Which users actually have what privileges
- Identify common user-privilege groupings that are candidate roles

> Best Practice – Hybrid Approach

- Governance, business model, and technology
- Accelerate and validate top-down model with bottom-up results
- Plan for long term management

Role Design Process - First steps

> Design and build a role repository

- Role model – use ANSI RBAC as a starting point
- Manageable repository
 - LDAP or RDBMS
- Plan for long term management

> Privileges abstraction

- Business model driven
- Document systems mapping

> Identity mapping strategy

- Consider adopting and extending unique IDs

> Identity data warehouse

- Consider combining: users, roles and permissions

Building An Identity Data Warehouse

- > **Inventory target systems and resources**
 - May be partitioned by business unit
- > **Define a normalized identity**
 - Relevant attributes, location, manager, job code etc.
- > **Define a privilege template or schema**
- > **Abstract system resource access into privileges**
 - May vary from high level (email) to transaction level (SAP)
- > **Link all identities and target privileges**
 - One unique identity per user
- > **Best Practice**
 - Leverage existing technology to facilitate the process

Role design workflow

- > **Model your security roles first**
 - Administrators tend to collect excessive privileges
- > **Model high-level enterprise organizational roles**
- > **Model high-level business unit roles**
 - Can be done in parallel
- > **Model functional level roles in phases**
 - Take the divide and conquer approach
 - Separation of duty is very important
 - Business model driven
- > **Consider hierarchy modeling: payroll clerk is an employee**

Top-down design

- > **Typically guided by organizational structure**
 - Roles are derived from organization and job function
 - Business need is the driver: **what** and **why** then **who**
 - May start to break down at the cross-functional boundary
 - Separation of duty is important
- > **Interview and analysis driven process**
 - Organizational barriers may slow process
 - Business analysts are key
- > **Best Practice**
 - Model against current standards if possible
 - Separate cross-functional analysis from line of business

Bottom-up Design

> Still guided by organizational structure

- Actual access patterns – **what** and **who** then **why**
- Roles typically map to job function
- Cross-functional roles are likely to emerge

> Technology driven process

- Technology accelerates the process
 - Role mining from existing identity data

> Best Practice

- Leverage other Identity components
 - Meta directory, provisioning
- Use an identity data warehouse

Role Mining

> Analogous to data mining for business intelligence

- Existing patterns of access are identified

> Leverage an identity data warehouse

- Initially user-privilege mappings
- May import existing roles

> Use data mining technology to extract roles

- Role candidates derived from actual user-privilege mappings
- Business analyst and role engineer work together
- Sage Discovery and Audit from Eurekaify

The Role Mining Process

- **Export warehouse data to a role management system like Eureka Sage Discovery and Audit**
- **Distribute functional level analysis task to business entity teams as required**
- **Store extracted roles in the identity warehouse or role repository**
- **Set a target so you know when you are done**
 - Avoid over-refinement
 - Expand scope or merge to reduce number of roles
- **Best Practice**
 - Do a privileges survey and clean-up first
 - Use the analysis techniques for ongoing maintenance

Eurekify Sage Role Mining Demo

> Bank Scenario

- Corporate, Branch, Developer

> Resources

- Mainframe, NOS, Unix

> Permissions audit

- collectors, collectables

> Role mining

- Candidate roles

> Maintenance

- Audit card

Summary

- **Role definition for RBAC is challenging but can be done when approached in phases and accelerated using technology**
- **A role based approach enhances security**
- **Role based access and provisioning can facilitate regulatory compliance**
- **Use a hybrid approach to get the best results**
 - Bottom-up analysis can validate and enhance a top-down model
 - Accelerate the role management process
- **Maintain an independent role repository**
- **Leverage your role mining technology for permissions analysis particularly in a regulatory environment**
 - Excess or inappropriate privileges exist in your legacy environment

Designing Roles for Identity Management A Real World Guide

Questions

Patrick.O'Kane@Unisys.com

- > Systems Integration.
- > Outsourcing.
- > Infrastructure.
- > Server Technology.
- > Consulting.

UNISYS

Imagine it • Done •