

VHA

HEALTH INFORMATION
ARCHITECTURE

User Authorization with Role-Based Access Control

RBAC

13 October 2004

Agenda

- Introduction
- Identity and Access Management (IAM)
- Privilege Management Infrastructure (PMI)
- Role Engineering and Provisioning
- Standards Activities

Identity and Access Management (IAM)



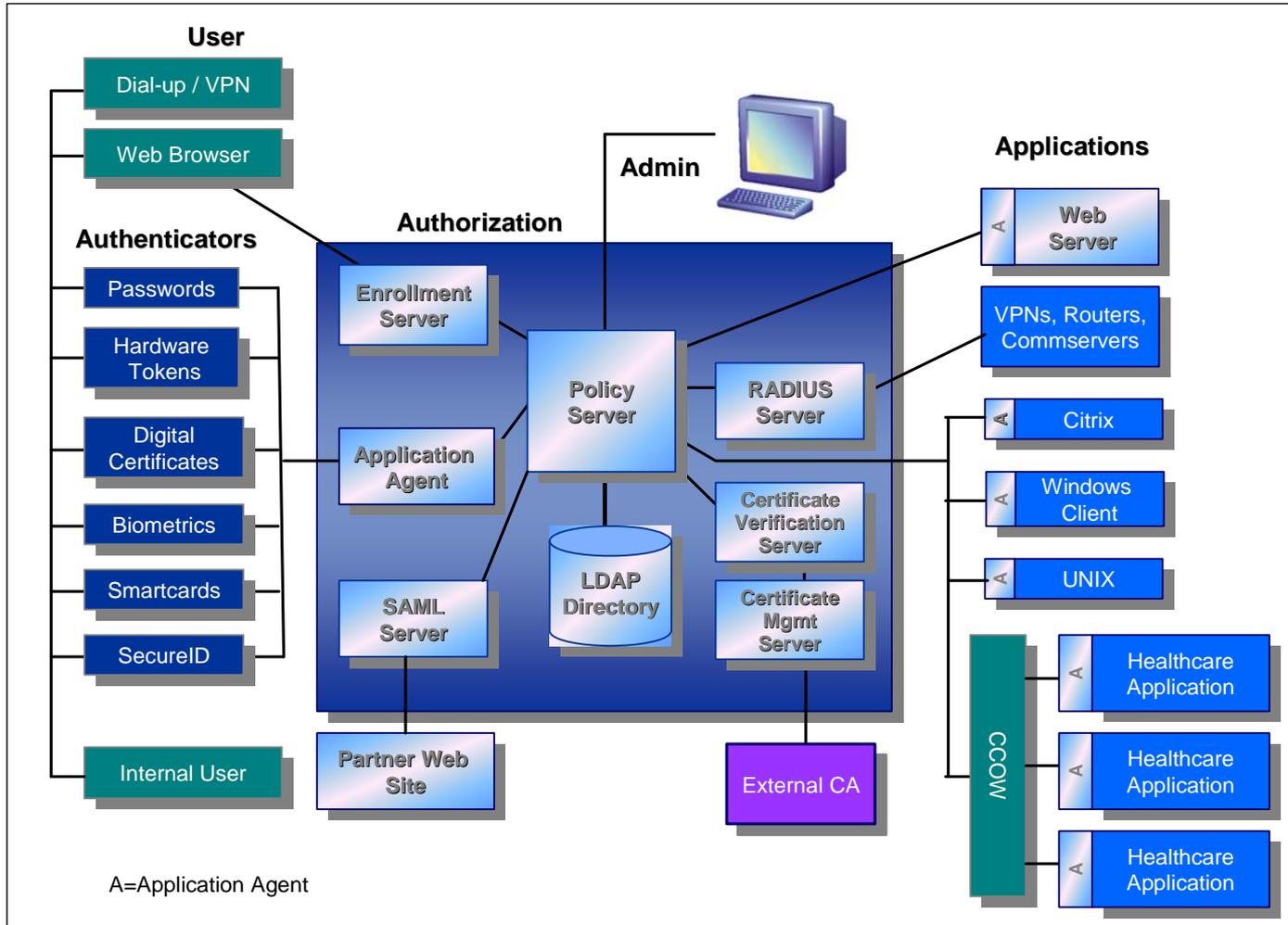
Security Problem Description

- **Complexity** - Multiple different systems, protocols and implementations
- **Scalability** - Hundreds of systems and tens of thousands of users, millions of Veterans
- **Adaptability** - New policies and practices not originally planned, new technologies
- **Interoperability** - Secure data exchange with business partners
- **Assurability** - Certification, testing and maintaining assurance of security function over system life-cycle

The Solution: IAM

- Identity and Access Management provides service-oriented architecture solutions for user authentication and authorization, including directories, single sign-on, and identity and access provisioning.
 - Part of a service-oriented security architecture
 - Provides common security infrastructure for identity and access management
 - Allows for sharing of security information
 - “Decouples” security mechanisms formerly tightly integrated with specific applications.
- Authentication component (e.g., PKI)
- Authorization component (e.g., PMI)
- Provisioning component (e.g., Role Engineering)

IAM Framework



IAM Benefits

- Solves security scalability problems through use of a service-oriented common infrastructure
- Simplifies authentication management
- Simplifies authorization management
- Reduces administrative costs
- Improves security
- Enhances business partner interoperability
- Enables new network-level security services
- Improves service to members/clients/patients

I AM Supports Full-Range of Healthcare Requirements

- Supports all health information system topologies (CCOW, Thin Client, Web, etc.).
- Places AA services at the Enterprise level.
- Supports medical sign-on, persistent sessions.
- Supports Enterprise and Federated SSO.
- Supports Emergency Access.
- Provides for Federated identity management.
- Provides Enterprise-wide user profiles and attributes.
- Provides support to healthcare roles.
- Supports application level authentication, authorization and delegation.
- Provides centralized security administration.
- Supports healthcare standards/interoperability.

Privilege Management Infrastructure (PMI)

Privilege Management Infrastructure (PMI)

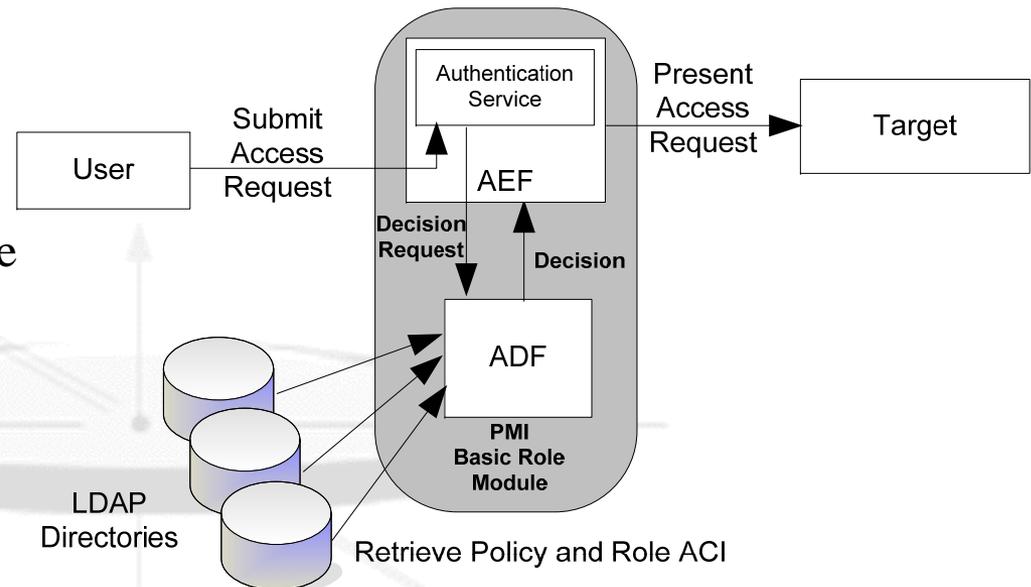
- Definition: The complete set of processes required to provide an authorization service. Part of an IAM solution.
 - **Access Control Decision Function (ADF)**
The system entity that evaluates applicable policy and renders an authorization decision
 - **Access Control Enforcement Function (AEF)**
The system entity that performs access control, by making decision requests and enforcing authorization decisions
 - **Policy** *A set of rules, an identifier for the rule combining algorithm and (optionally) a set of obligations.*

Note: The terms ADF and AEF are defined by ISO. They are synonymous with PDP (Policy Decision Point) and PEP (Policy Enforcement Point) used by OASIS.

PMI Basic Roles

Basic Roles place people in the organizational hierarchy as belonging to categories of healthcare personnel warranting differing levels of access control.

- Basic roles allow users to participate in the organization's workflow (e.g., tasks) but do not specify detailed permissions on specific information objects.
- Basic roles allow a user to "connect" to a resource but do not grant authorizations on protected objects.

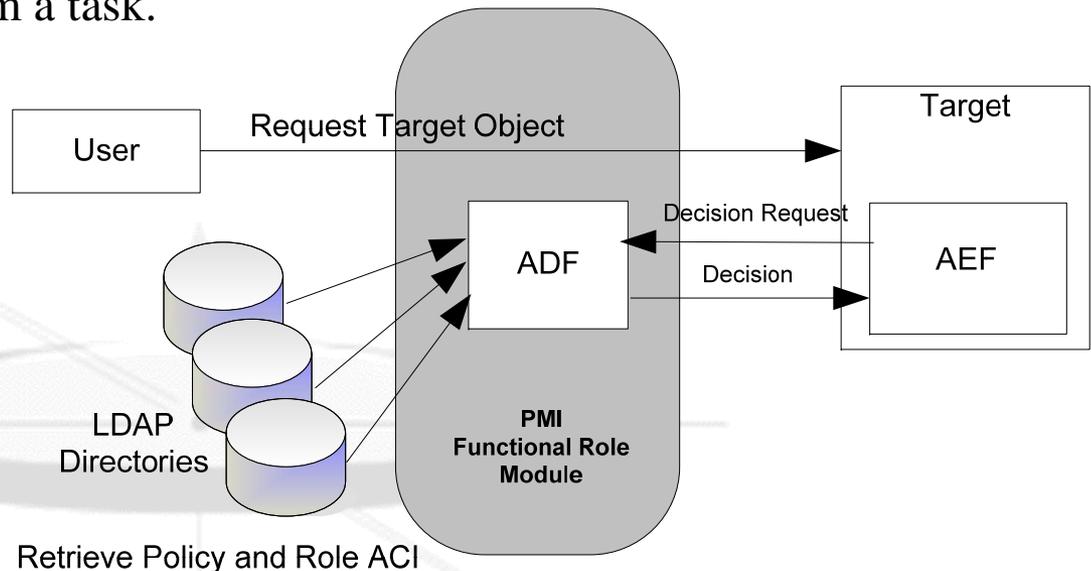


See ASTM E1986-98 for a listing of healthcare personnel that warrant differing levels of access control.

PMI Functional Roles

Functional Roles consist of all the permissions on health information system objects users need to perform a task.

- Functional role names associate groups of permissions to users.
- A user may be assigned one or more functional roles, and all of the permissions associated with a corresponding healthcare workflow.
- Permissions are used to set the system operations (create, read, update, delete, execute, etc.) for data and software applications.



PMI Language and Application Interface: XACML

XACML (eXtensible Access Control Markup Language) is both an access control language and a policy language.

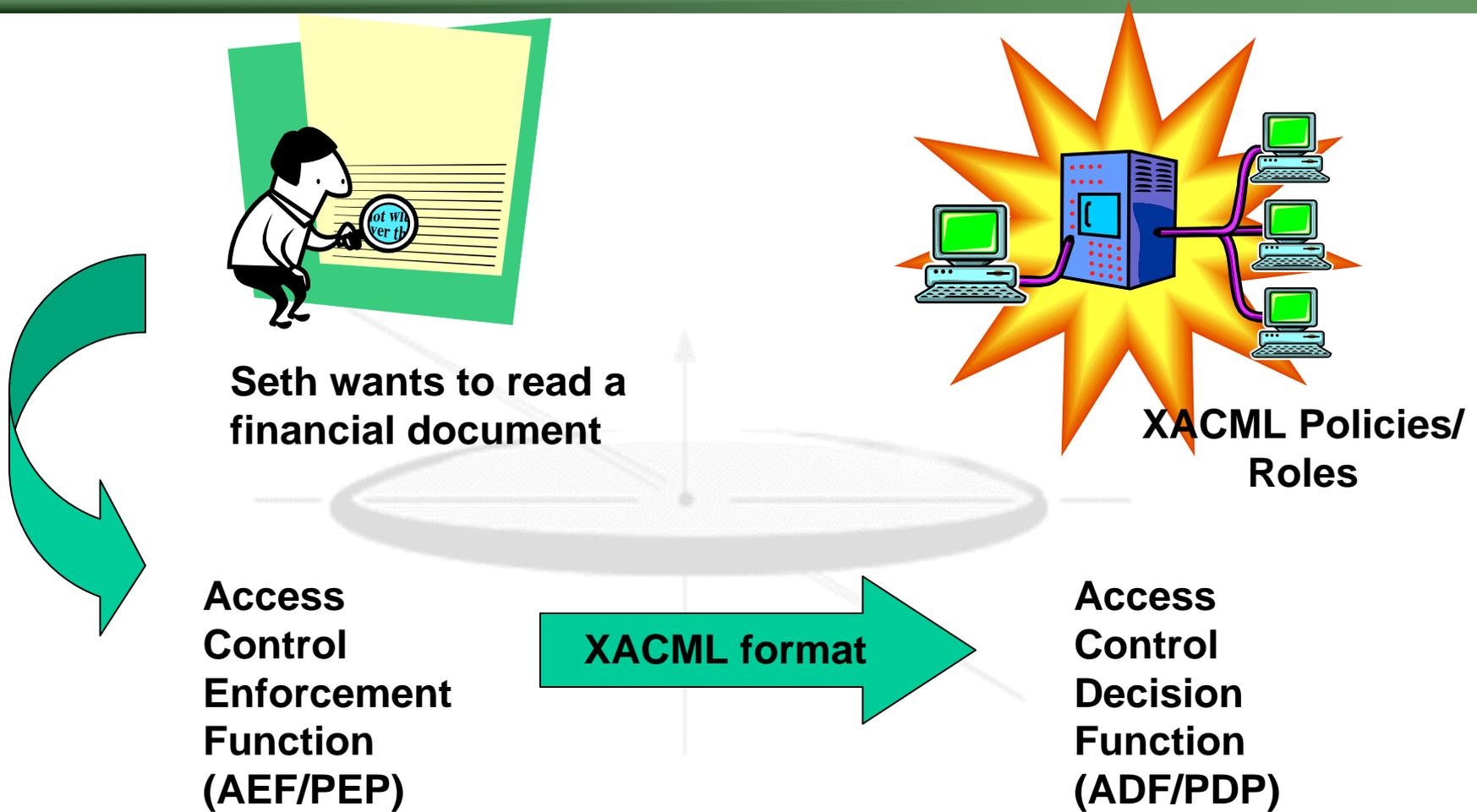
XACML is an OASIS standard and non-proprietary.

Programmers can use the OASIS standard to implement policy-based access control or use available third-party implementations.

VHA's Authentication and Authorization Infrastructure (AAI) Lab is using Sun's Java implementation of XACML. It is available for download at:

<http://sunxacml.sourceforge.net/>

Making an XACML Request



XACML Requests

XACML requests are defined in the schema:

<http://www.oasis-open.org/committees/download.php/919/cs-xacml-schema-context-01.xsd>

XACML requests are described in the document:

<http://www.oasis-open.org/committees/download.php/2406/oasis-xacml-1.0.pdf>

Each XACML Request must contain:

- 1 *Subject*: Attributes Associated with Requestor
- 2 *Resource*: Information About the Protected Resource
- 3 *Action*: Requested Action on the Resource

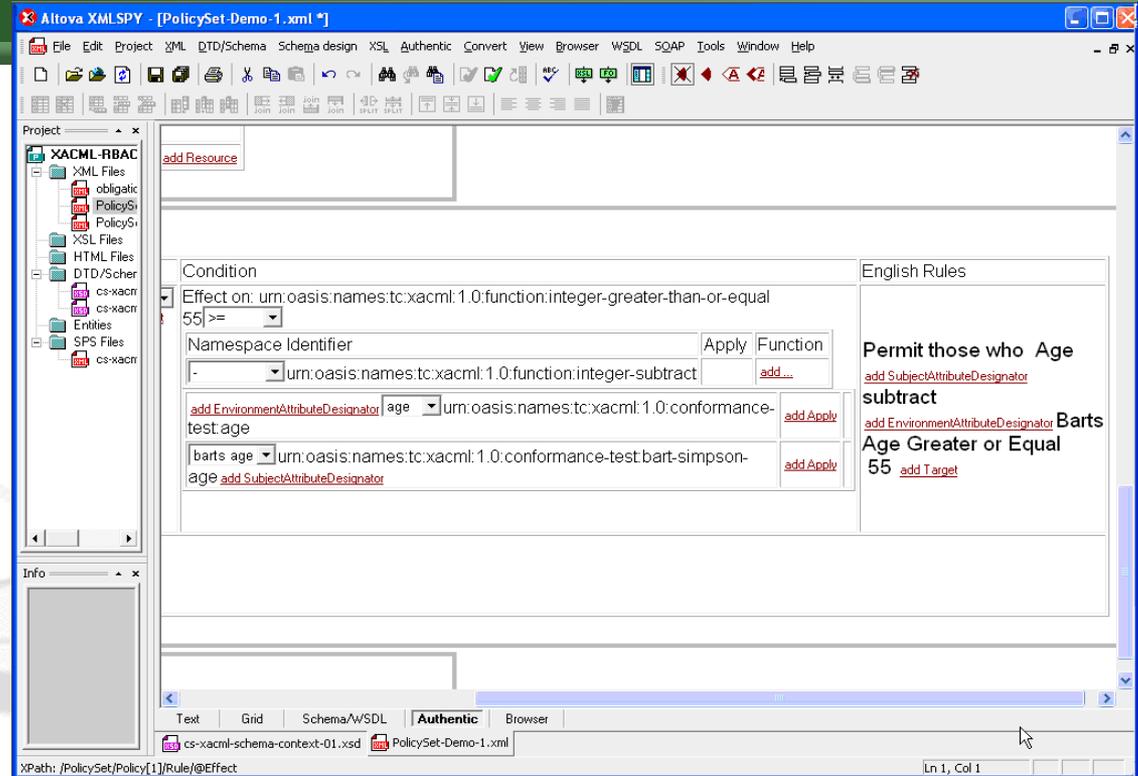
Suitability of XACML for RBAC

- Can use OASIS XML standard to create NIST/ANSI compliant standard permissions.
- Can use XACML/SAML for standard query/response
- Supports desired features:
 - X-Path, for accessing data within an XML document
 - Obligations, for imposing requirements on PEP
 - Conditions, for robust policy writing
- LDAP designed to support Attribute - Value data required in XML
- XML Used in European projects (e.g. Permis)

The PERMIS X.509 Role Based Privilege Management Infrastructure

D.W.Chadwick, O.Otenko, ISI, University of Salford, Salford, M5 4WT, *SACMAT'02*,
June 3-4, 2002, Monterey, California, USA.

Support Tools for RBAC in XML



How can we write and maintain the large volume of XACML policies required to support major healthcare organizations?

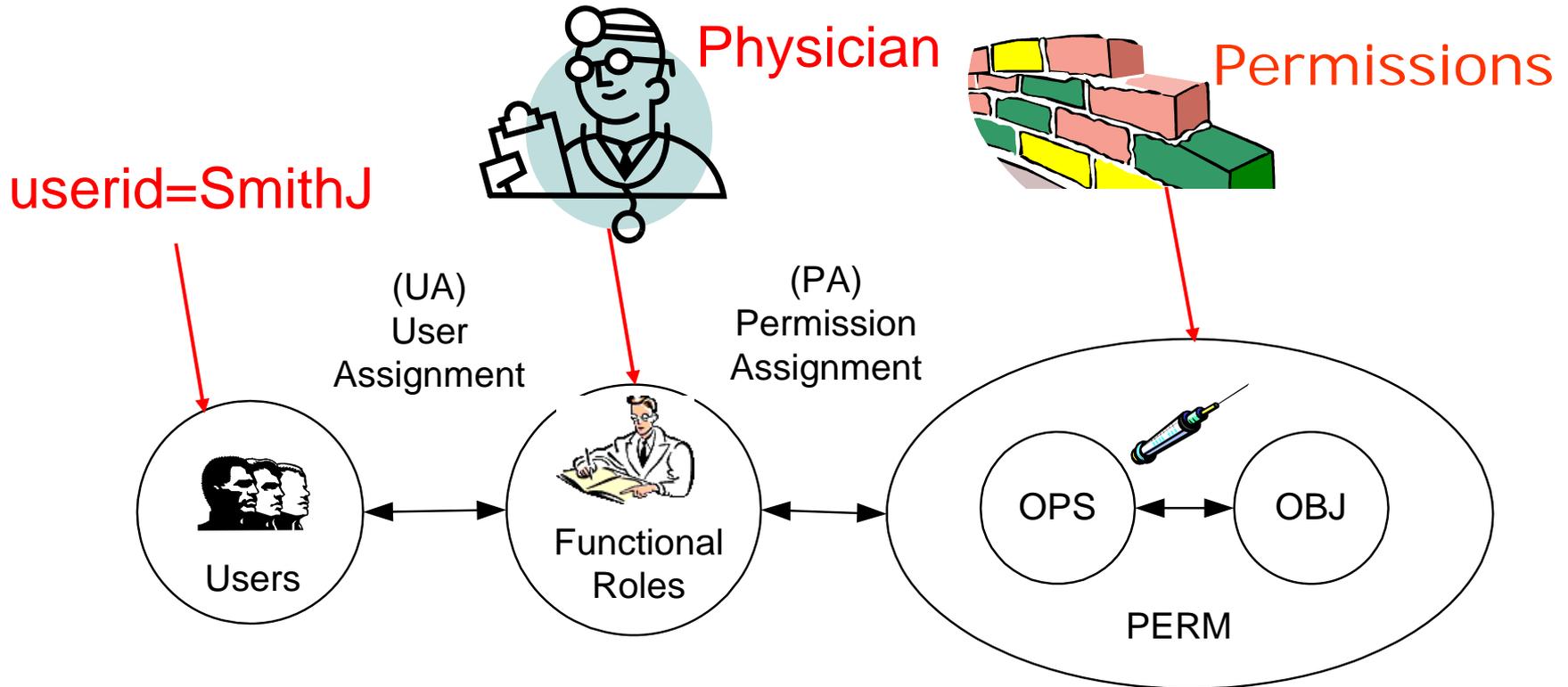
Role Engineering and Provisioning



Role-Based Access Control

- Role-Based Access Control (RBAC) is a type of policy based access control where entity access is granted based upon membership in a group (role) and where rights and privileges are bestowed upon the role rather than the entity directly.
- RBAC is useful in healthcare environments with user roles and access requirements, including separation of duties.
- Roles are collections of permissions which are ordered sets of operations on protected objects.

Permissions



OPS = Operations
OBJ = Objects
PERM = Permissions

Adapted from ANSI
INCITS 359-2004

Prerequisites

Roles are the Information Content for IAM/PMI.
They are the gas for the IAM engine.

- Roles and permissions must be defined before RBAC can be used within an enterprise PMI.
- Standard permission sets must be defined before inter-organization interchange can be supported.

HL7 Role Engineering Process

The VHA RBAC TF first developed a scenario-driven Role Engineering Process*, which has also been applied and proven its value. The process is currently being adopted within HL7 for creating a standard healthcare permission vocabulary worldwide.

Role Engineering Process:

1. Identify and Model Usage Scenarios
2. Derive Permissions
3. Identify Permission Constraints
4. Refine Scenario Model
5. Define Tasks and Work Profiles
6. Define RBAC Model

*Adapted from *A Scenario-driven Role Engineering Process for Functional RBAC Roles*, G. Neumann and M. Strembeck. June 2002.

In a Nutshell

- We model scenarios, tasks and steps to understand people's jobs.
- We create access rules for each part of a job and call them permissions.
- We organize blocks of permissions and call them roles.
- We manage security and privacy for protected resources (e.g. health information) with roles.
- We give people permissions (roles) they need to do their jobs (least privilege) and to access protected resources.
- We standardize permissions so we can share information among systems and partners.

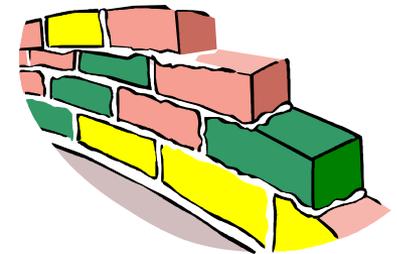
How It All Fits Together

ROLE = Physician



Dr. Joe Smith is an
Oncologist

PERMISSION = Write Medication Order

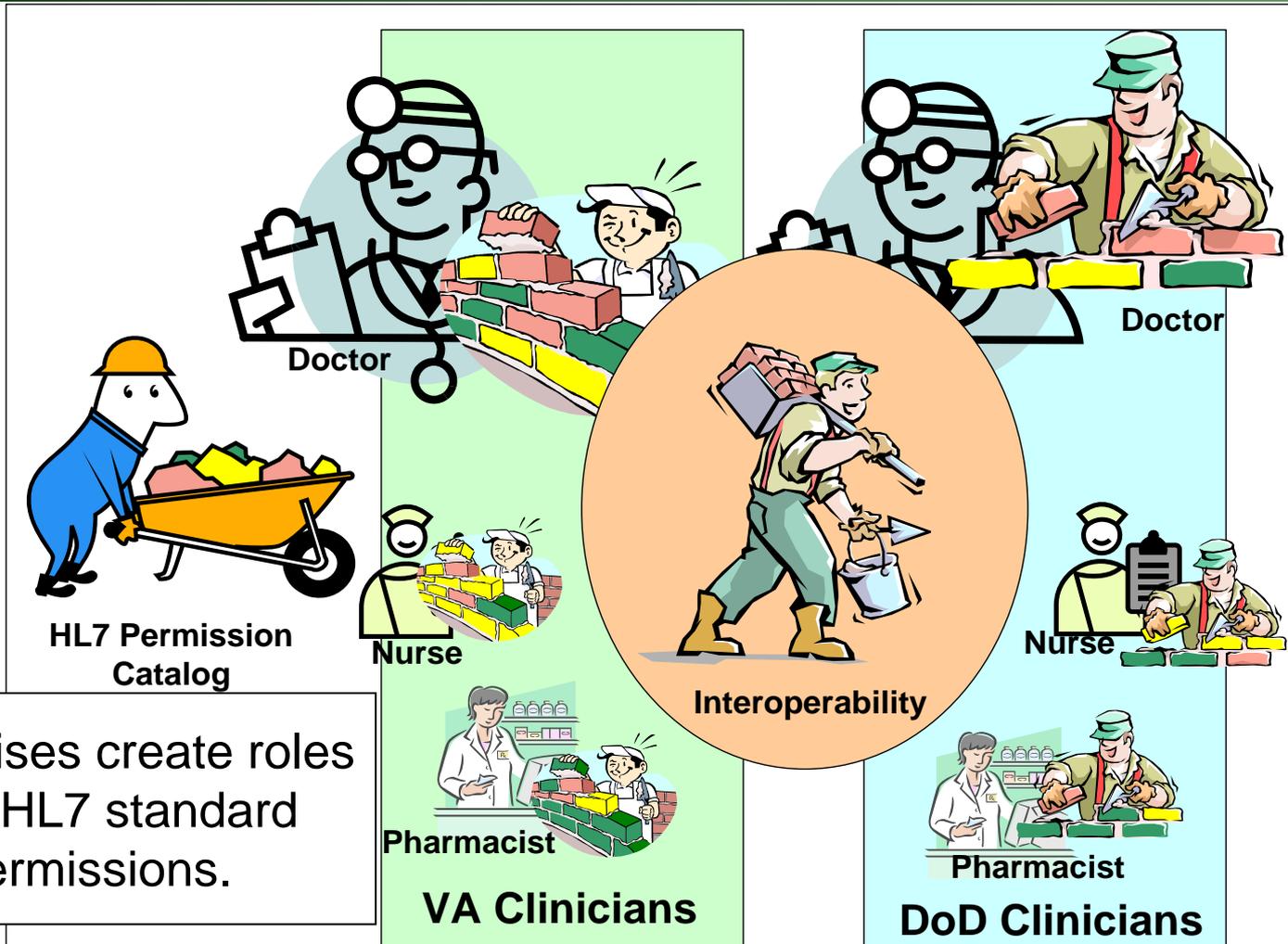


**BUSINESS RULE = Oncologists may Write
"Chemotherapy" Medication Orders**

CONSTRAINT = 1st year Oncology Residents
need Chemotherapy Medication Orders
co-signed by an Attending Physician



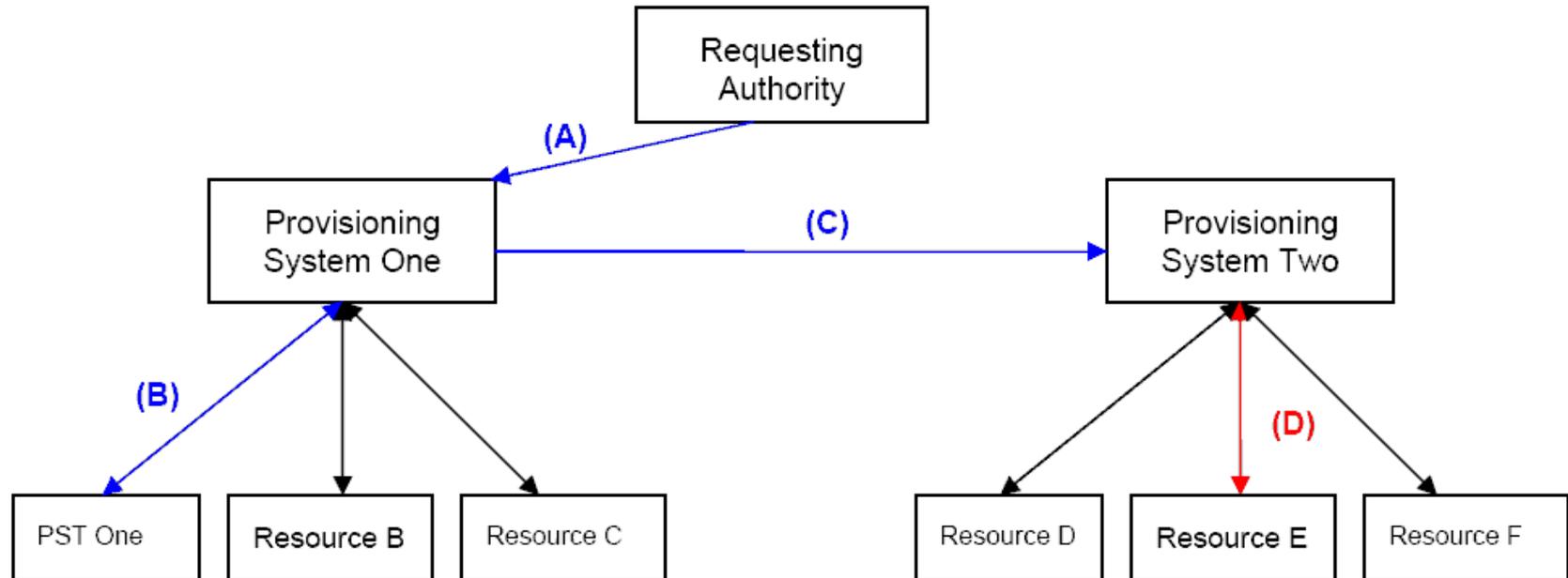
Roles are Built from Permissions



Enterprises create roles from HL7 standard permissions.

Service Provisioning Markup Language (SPML)

SPML XML-based framework for exchanging user, resource, and service provisioning information.



Provisioning Systems: Adapted from SPML OASIS Standard (Approved October, 2003)

Standards Activities



Role of HL7 for RBAC

1. Review and adopt standard role engineering process.
2. Standardize healthcare permission set.
3. Identify permission constraints.
4. Derive preliminary role hierarchy.
5. Define guidelines for developing RBAC models, e.g., for assigning role names and for engineering role-role constraints.
6. Coordinate with other SDOs, e.g., W3C, OASIS, ASTM, IHE to provide an implementation path.

Summary of HL7 Activities

- May 2004 HL7 WGM - Approval of the RBAC permission catalog standardization activities by HL7 Board of Directors as part of the HL7 family of standards.
 - Review, comment and approve healthcare role engineering process, then integrate it into the HDF.
 - Validate previously developed (within HL7 and in RBAC Task Forces) healthcare scenarios.
 - Develop and model additional healthcare scenarios.
 - Define role permissions and objects.
 - Integrate RBAC permission catalog with the HL7 RIM, RMIMs and DMIMs.
 - Define guidelines for developing RBAC models.

Summary of ASTM Activities

- May 2004 - ASTM E31 Committee acceptance of VHA recommended modifications to ASTM E-1986 list of licensed health care providers.
- Created Privilege Management Infrastructure Standard Work Group
 - Wide range of major industry leaders
 - Representation by healthcare industry and providers
- Continuity of Care Record

Summary of OASIS Activities

Creating emerging standards that are addressing issues associated with implementing PMI:

- eXtensible Access Control Markup Language (XACML), OASIS Standard 1.0
- LDAP profile for distribution of XACML policies, OASIS Working Draft
- XACML Profile for Role Based Access Control, OASIS Committee Draft 0.1
- Service Provisioning Markup Language (SPML), OASIS Standard 1.0

Summary of RBAC Related Standards

OASIS  <http://www.oasis-open.org>

- eXtensible Access Control Markup Language (XACML), OASIS Standard 1.0
- LDAP Profile for Distribution of XACML Policies, OASIS Working Draft
- XACML Profile for Role Based Access Control, OASIS Committee Draft 0.1
- Service Provisioning Markup Language (SPML), OASIS Standard 1.0
- UDDI Version 2, 19 July 2002
- Web Services Security v 1.0, March 2004
- Security Assertion Markup Language (SAML)



<http://csrc.nist.gov/rbac>
- ANSI INCITS 359-2004



<http://www.astm.org>

- Healthcare Privilege Management Infrastructure (E31 Committee Work Project)



<http://www.hl7.org>

- HL7 Healthcare Standard Permission Catalog (Security TC Work Project)



HEALTH INFORMATION

ARCHITECTURE

Standards

Contact Information

- Website

<http://www.va.gov/RBAC/>

- Points-of-Contact

Robert O'Hara, MD
VHA/IHS RBAC TF Chair
Robert.OHara@med.va.gov
(708) 202-8387 x22759

Mike Davis, CISSP
VHA Security Architect
Mike.Davis@med.va.gov
(760) 632-0294

Amy Page
VHA/IHS RBAC TF
Project Lead
Amy.Page@med.va.gov
(619) 741-7587

Dawn Rota, RN, BSN
VHA/IHS RBAC TF
Functional Analyst Lead
Dawn.Rota@med.va.gov
(858) 826-7496

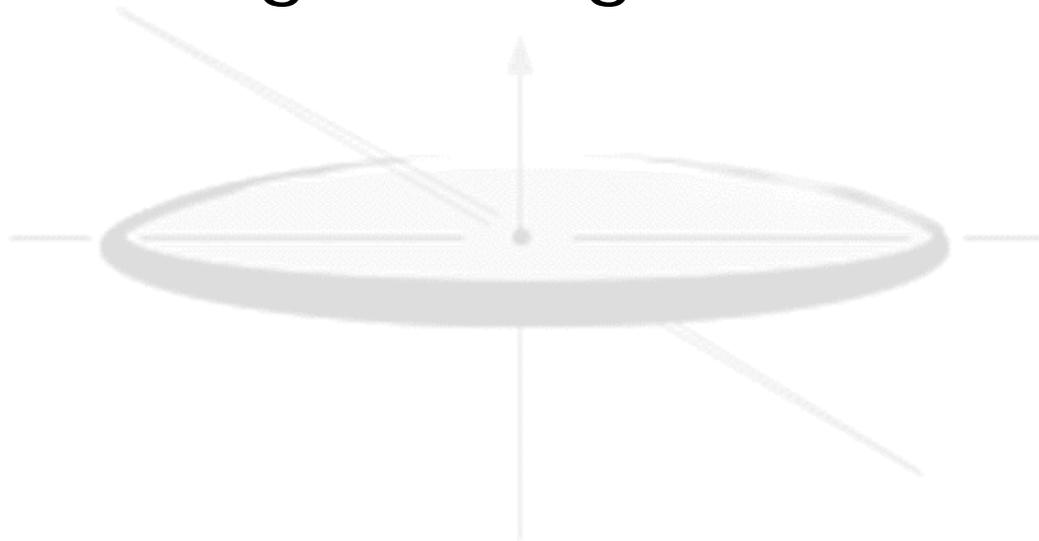
Q & A

Questions?

A large, light gray speech bubble graphic is positioned behind the word 'Questions?'. The bubble has a circular top and a tail pointing downwards and to the right. The word 'Questions?' is written in a bold, green, sans-serif font with a white outline and a slight drop shadow, making it stand out against the white background and the speech bubble.

Backup Slides

The slides that follow illustrate the detailed steps of the HL7 Role Engineering Process



1. Identify & Model Scenarios

- Example

Dr. Eric Emergency, an emergency room physician, sees a 45-year old male patient Adam Everyman, for chest pains. Myocardial infarction is suspected and the patient is admitted.

Dr. Emergency inquires if the patient Adam Everyman has any allergies, conducts a history and physical and **[documents his findings in the patient's chart]**.

To determine whether patient Adam Everyman has had a heart attack, Dr. Emergency **[orders a CPK]** to be collected immediately and then every 8 hours for the next 2 days. Dr. Emergency also **[orders a STAT Chest X-Ray]**.

STEP

SCENARIO

STEP

STEP

2. Derive Permissions from Scenarios

- For each scenario, the steps are identified and stored in the permission catalog as {operation, object} pairs.
STEP 1 ➔ Identify operations.
STEP 2 ➔ Find the associated object.
STEP 3 ➔ For each scenario step, record the associated (operation, object) pair in the permission catalogue.

2. Permissions - Example

| Step | Permission |
|---------------------------------------|-----------------------------|
| Perform ADT Functions (Admit Patient) | { C, Admission } |
| New Patient Allergy | { C, Allergy } |
| New History and Physical | { C, History and Physical } |
| New Progress Notes | { C, Progress Note } |
| New Laboratory Order (STAT CPK Panel) | { C, Laboratory Order } |
| New Laboratory Order (q8 CPK Panel) | { C, Laboratory Order } |
| New Radiology Order (STAT CXR) | { C, Radiology Order } |

3. Identify Permission Constraints

- Constraints to be enforced on permissions are identified and made explicit.

Constraints are:

- Restrictions that are enforced upon access permissions (e.g. Head Nurse, Chief of Staff).
- Include separation of duties, time-dependency, mutual exclusivity, cardinality or location.
- Distinguish healthcare policies that limit access to sensitive data (e.g. HIV, mental health, adoption).

4. Refine Scenario Model

STEP 1 ➡ The scenario is reviewed to see if some similar scenarios exist.

STEP 2 ➡ Similar scenarios are defined.

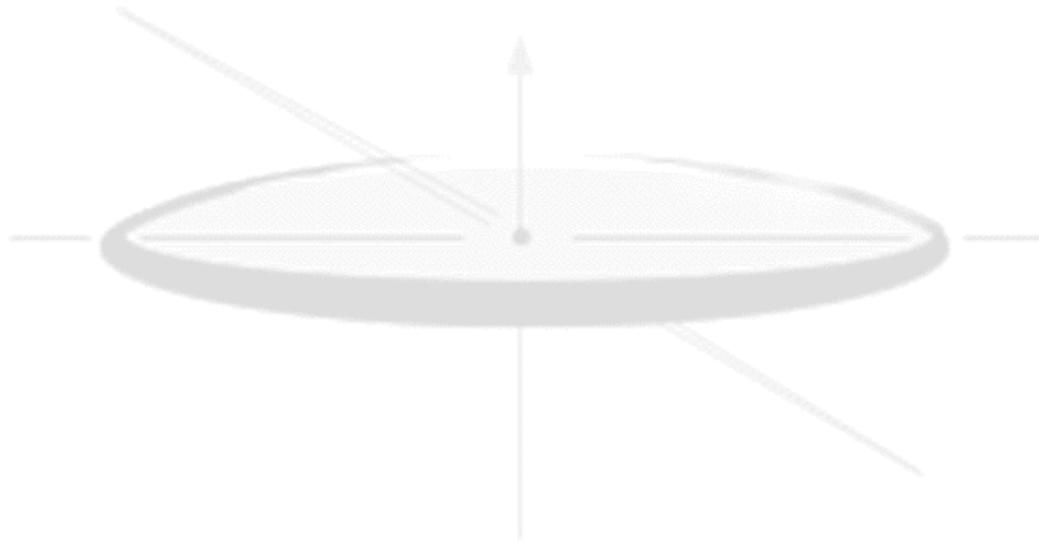
STEP 3 ➡ For each group of similar scenarios, determine if an abstract scenario can be defined.

STEP 4 ➡ The scenarios are grouped and a common abstract scenario is derived.

5. Define Tasks and Work Profiles

STEP 1 ➔ Identify scenarios that logically belonged together.

STEP 2 ➔ Group the scenarios into tasks.



6. Define RBAC Model

The role-hierarchy, permission catalog and constraint catalog define the RBAC model.

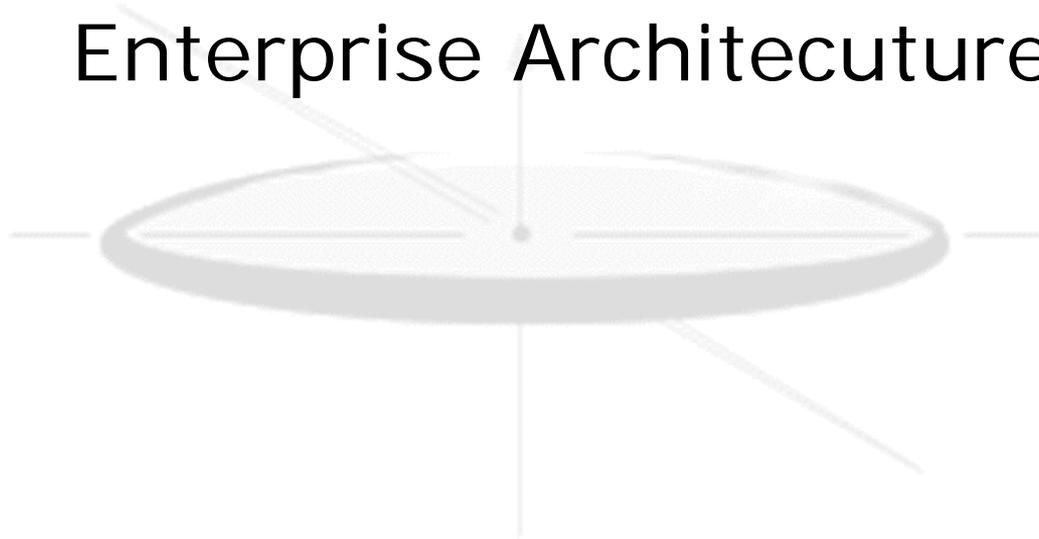
STEP 1 ➔ The work tasks and permission catalog are used to create a preliminary role-hierarchy.

STEP 2 ➔ Potentially redundant roles are identified and marked for review.

STEP 3 ➔ Redundant roles are removed, new roles and constraints are defined and role-hierarchies are merged or separated.

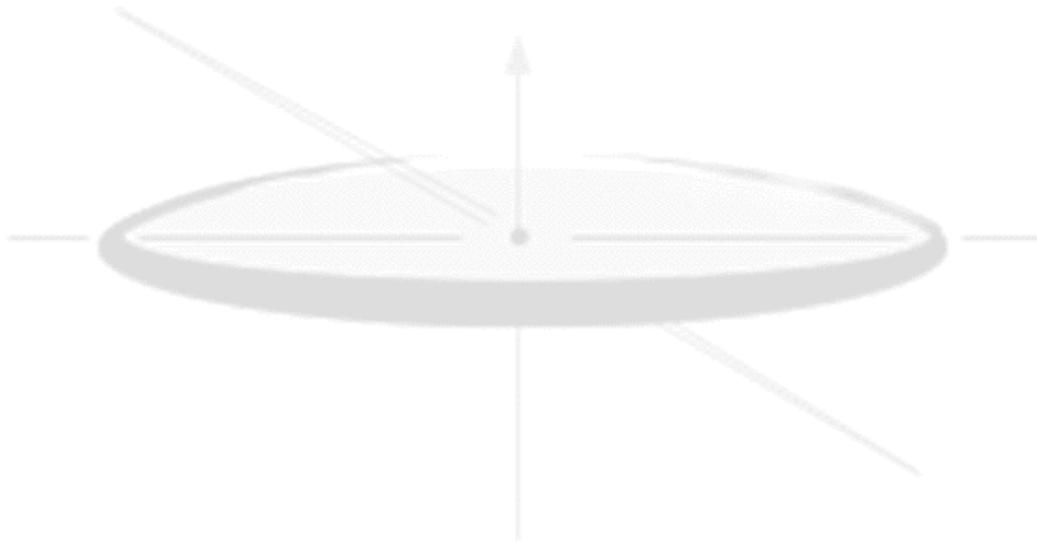
Backup Slides

The slide that follows illustrates an example of healthcare IAM infrastructure as contained in the VA Enterprise Architecture



Backup Slides

The slide that follows illustrate schema for an XACML request

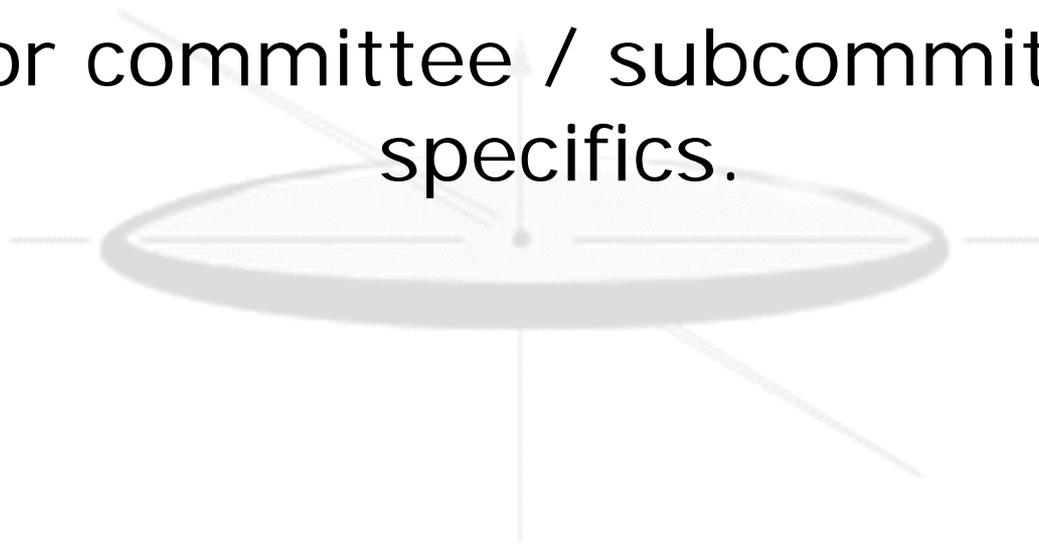


Actual XACML Request

```
<?xml version="1.0" encoding="UTF-8" ?>
- <Request xmlns="urn:oasis:names:tc:xacml:1.0:context" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="urn:oasis:names:tc:xacml:1.0:context cs-xacml-schema-context-01.xsd">
- <Subject>
  - <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id" DataType="urn:oasis:names:tc:xacml:
    1.0:data-type:rfc822Name">
    <AttributeValue>seth@users.example.com<1>AttributeValue>
    </Attribute>
  </Subject>
- <Resource>
  - <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
    DataType="http://www.w3.org/2001/XMLSchema#string">
    <AttributeValue>http://server.example.com/sensitive/financial-report<2>AttributeValue>
    </Attribute>
  </Resource>
- <Action>
  - <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
    DataType="http://www.w3.org/2001/XMLSchema#string">
    <AttributeValue>read<3>AttributeValue>
    </Attribute>
  </Action>
</Request>
```

Backup Slides

The slides that follow illustrates the VHA Role Engineering Task Force Organization. View the Notes Page for committee / subcommittee specifics.



VHA RBAC Organization

