

# VHA RBAC TF Meeting

## RBAC Architecture

Mike Davis

VHA Security Architect

18 June 2003



# Contents

- Problem Description
- Service Oriented Architecture
- AAIP Security Framework
- Organizational and Functional Roles
- Application-Level Architecture

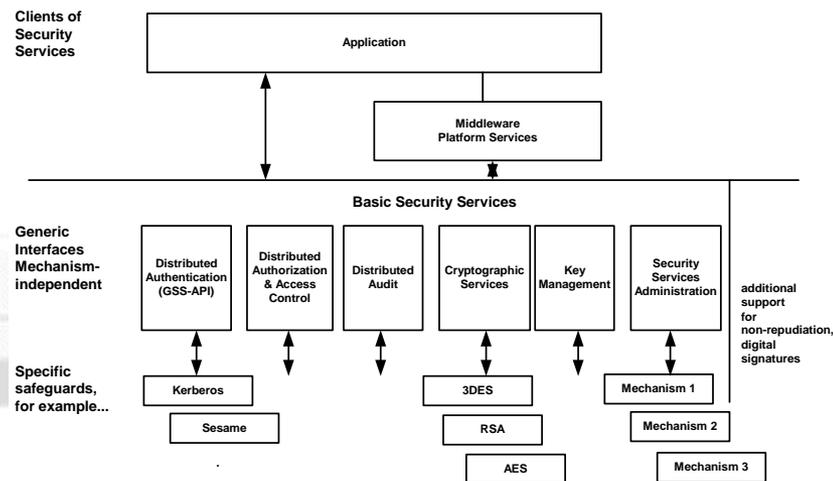
# RBAC Problem Description

- **Complexity**- Multiple different systems, protocols and implementations
- **Scaleability**-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
- **Assurance**-Certification, testing and maintaining assurance of security function over system life-cycle

# Security Approach

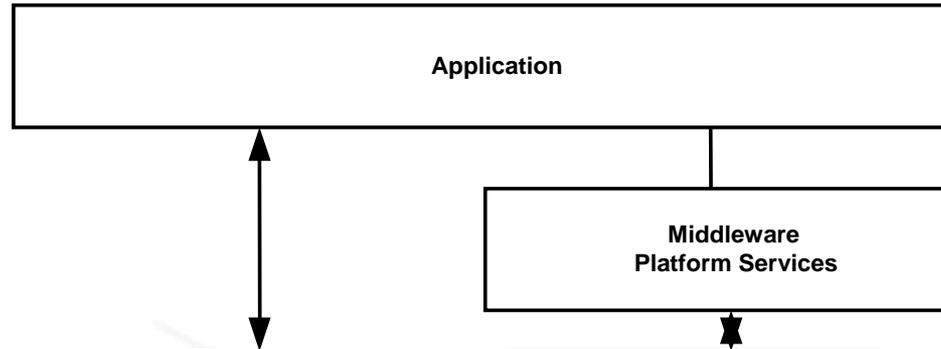
VA security systems need to evolve with IT strategic planning to achieve:

- “One VA” security
- Leveraging of scarce resources
- Security frameworks that function together
- Common security services across enterprise applications (SOA)
- Independent Security APIs
- Shared security information bases
- Decoupled security mechanisms
- Use of standards for interoperability



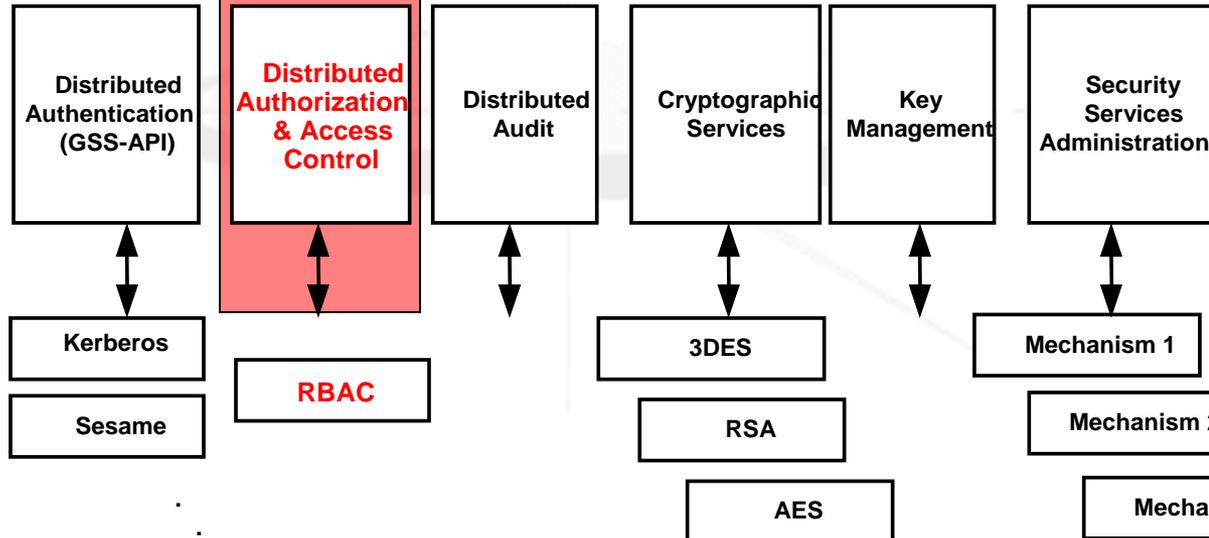
# Service Oriented Architecture

Clients of Security Services



## Basic Security Services

Generic Interfaces  
Mechanism-independent



Specific safeguards, for example...

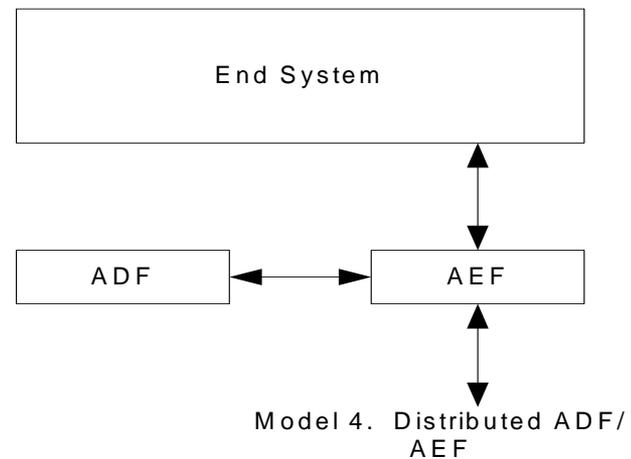
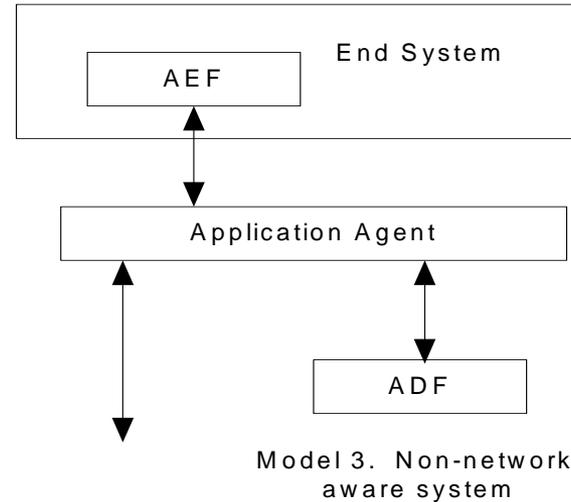
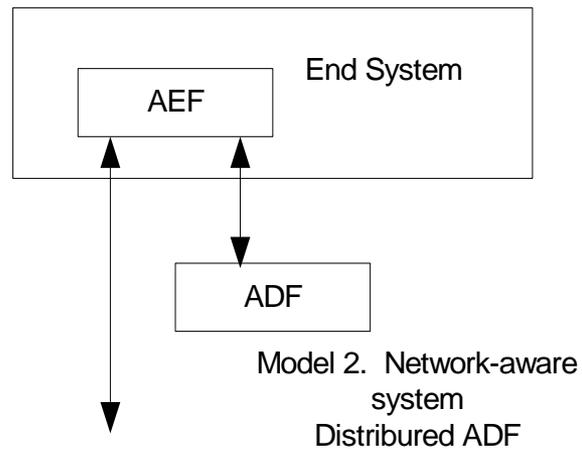
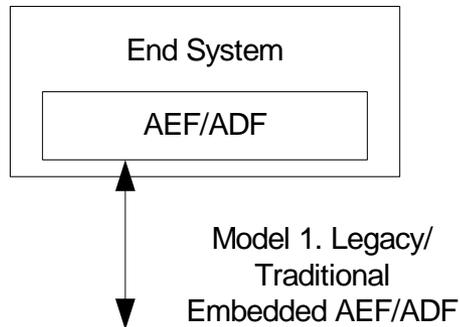
additional support for non-repudiation, digital signatures



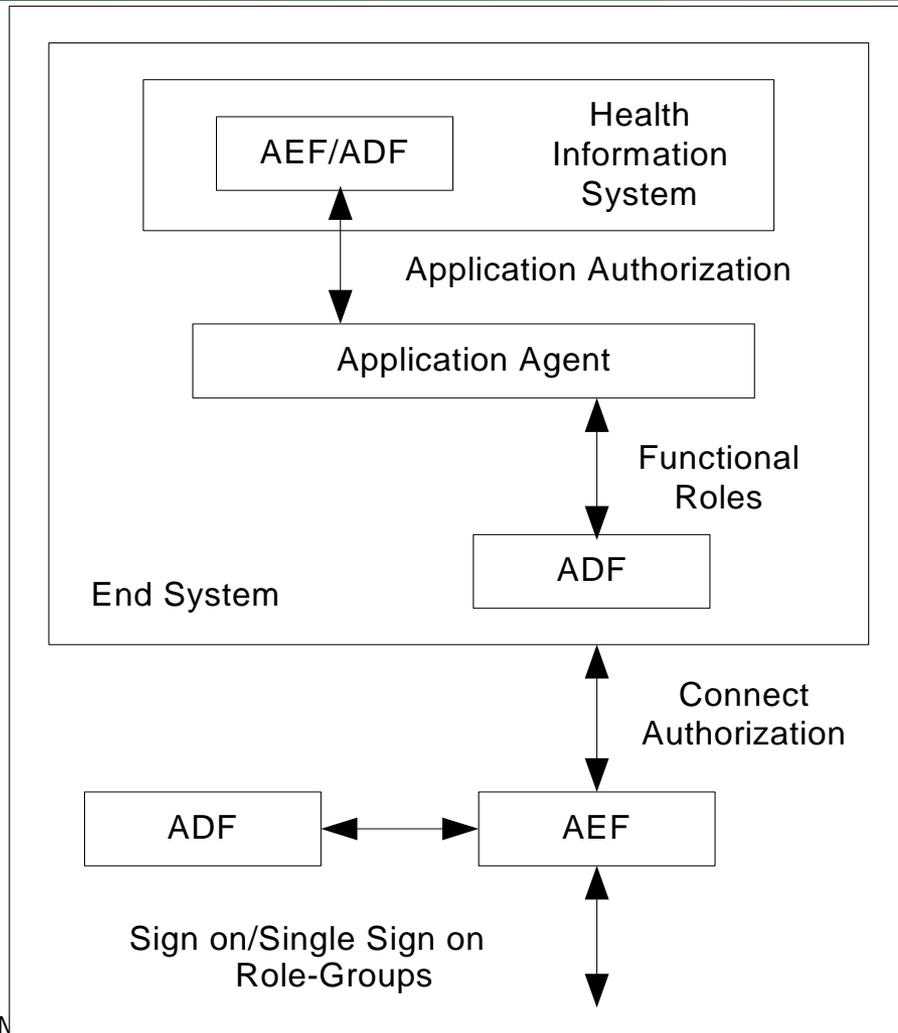
HEALTH INFORMATION

ARCHITECTURE

# Access Control Models



# Practical Access Control Architecture



# VHA Security SOA Evolution

- VHA Security FW 2000
- Security SOA specified as key component of VHA EA 2001
- Security requirements investigated, linked to VHA business needs, validated by VHA collaboration community
  - DACA WG CONOPS Sep 2001
  - STEP (Feb-Dec 2002) Final Report Jan 2003
  - VHA efforts merged with VA AAIP Jan 2003
  - Consolidated VHA AAIP requirements (constraints, functional and technical) May/June 2003
- **VHA RBAC TF June 2003 YOU ARE HERE!**

# AAIP Requirements

- Enterprise-wide distributed authentication
  - Medical Sign-on/Persistent clinical sessions
  - CCOW
  - Single Sign-on
  - Strong authentication (VA PKI) (wireless/remote users)
  - Enterprise-wide person identifiers
- **Enterprise-wide distributed authorization**
  - **RBAC and role engineering**
  - **Break-glass access**
  - **Federated authorizations**
  - **Distributed vs local access control**
- Health information system audit (Healthcare Standard)
- Security Management
  - Centralized user and system security management
  - Configuration management, provisioning, test and operations
  - Enterprise-wide Security Management Information Bases
- Assurance
  - Secure software development environments
  - Standard interfaces to security function
  - Certification

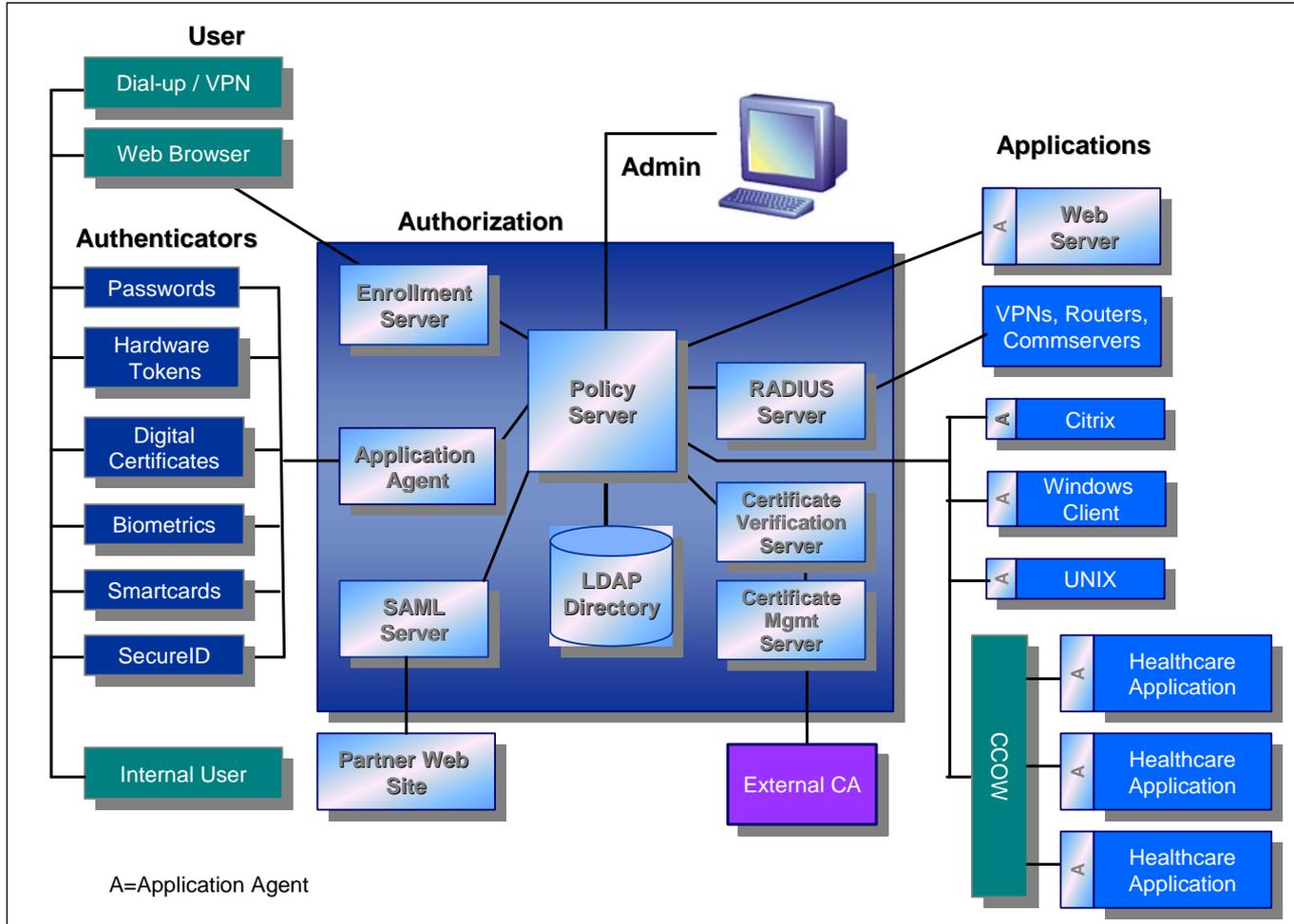
# Key AAIP Technology: RBAC

- “Only authorized personnel will be approved for access to VA information systems. ...approval must be specific to each individual’s roles and responsibilities in the performance of duties...” VA Handbook 6500
- Role-based access control (RBAC) is particularly useful in healthcare environments with user roles and access requirements such as separation of duties. ASTM 1986
- AAIP RBAC infrastructure must be in place before RBAC can be supported.
- Roles and permissions must be defined before RBAC can be used on an enterprise basis.

# VHA AAIP Framework

- Support for Self-Enrollment.
- Support for the full range of VHA health information system topologies
- **Place AA services at the Enterprise level**
- Support medical context application SSO.
- **Provide for Federated identity management**
- Provide Enterprise-wide user profiles and attributes.
- **Provide support to healthcare roles.**
- **Support application level authentication, authorization and delegation.**
- Provide central audit facility.
- Provide centralized security administration

# VHA AAIP Framework



# Organizational Roles: Workflow Access

- Defines Health Professional position in the organizational hierarchy (Static)
  - Medical director
  - Director of Clinic
  - Senior Physician
  - Resident Physician
  - Medical assistant
  - Medical student
  - Head Nurse
  - Nurse

# VA PKI

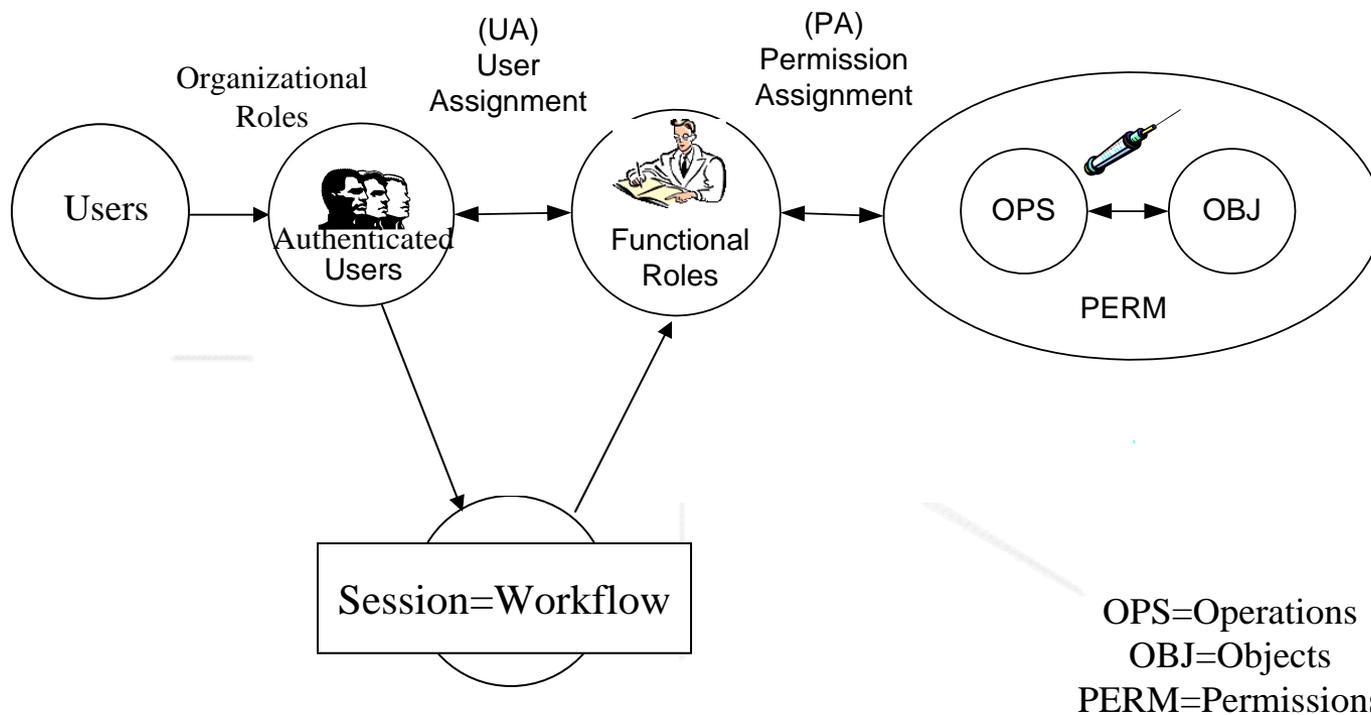
**Provide basic access control prior to allowing a user to connect to protected resources.**

- ASTM Privilege Management Infrastructure
  - ASTM 1986 Healthcare positions warranting access control
  - ASTM 2212 Healthcare PKI CP. Harmonized with Federal Bridge CP
- Allows VA PKI (X.509 v3 Cert) support for:
  - VPID as alternative ID (SubjAltName)
  - Assert Federal/ASTM CP
    - ASTM 1986 roles
    - Healthcare credentialing
- Allows AAIP to enforce basic “connect” access control (Network-level access control)

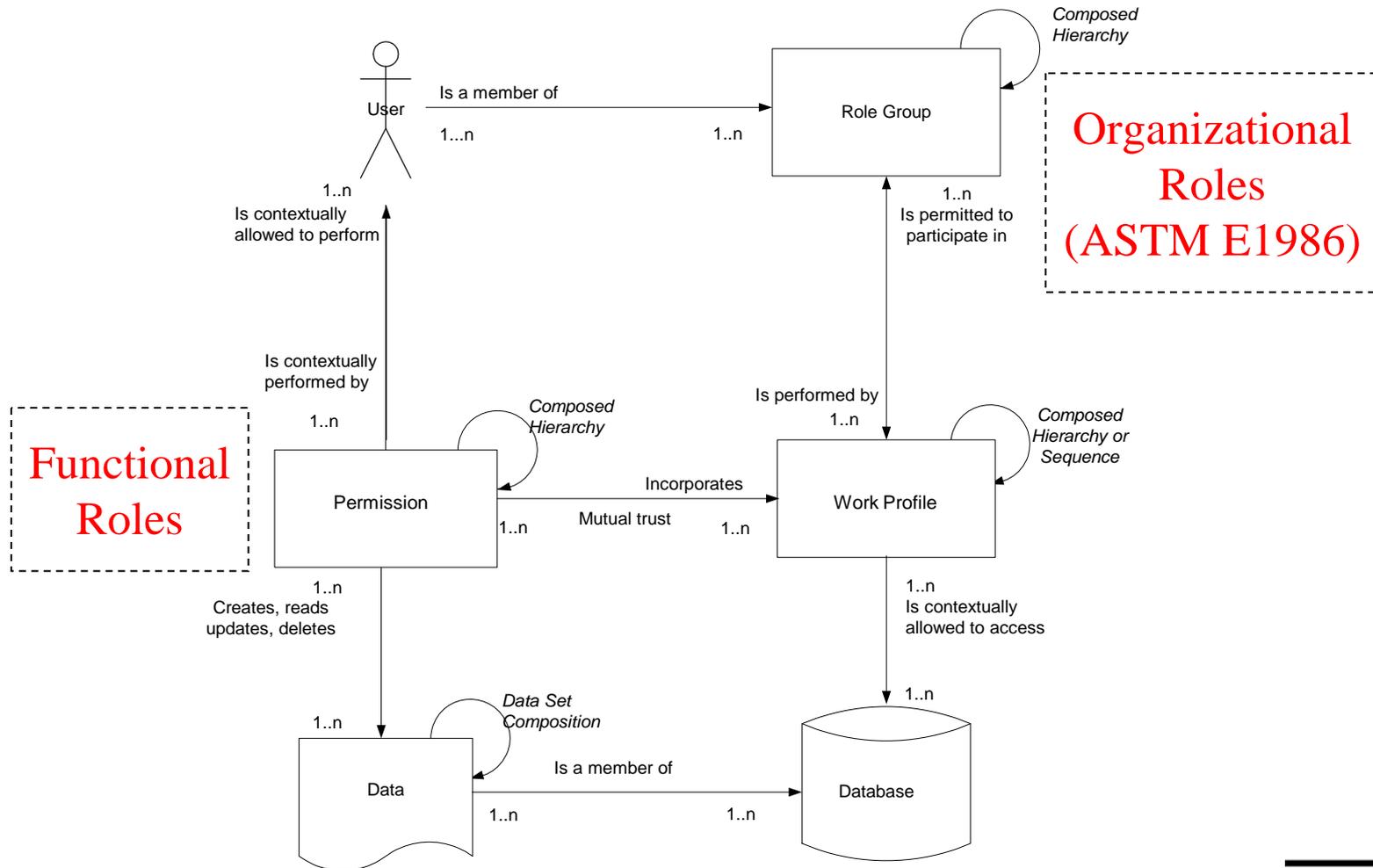
# Functional Roles: Application Access (Dynamic)

- Function-related role reflects the health professional position in the healthcare process.
  - Caring doctor
  - Member of diagnostic team
  - Member of therapeutic team
  - Consulting doctor
  - Referring doctor
  - Attending doctor
  - Family doctor
  - Attending Nurse

# NIST Role Standard (Mod)



# Connecting Role Types

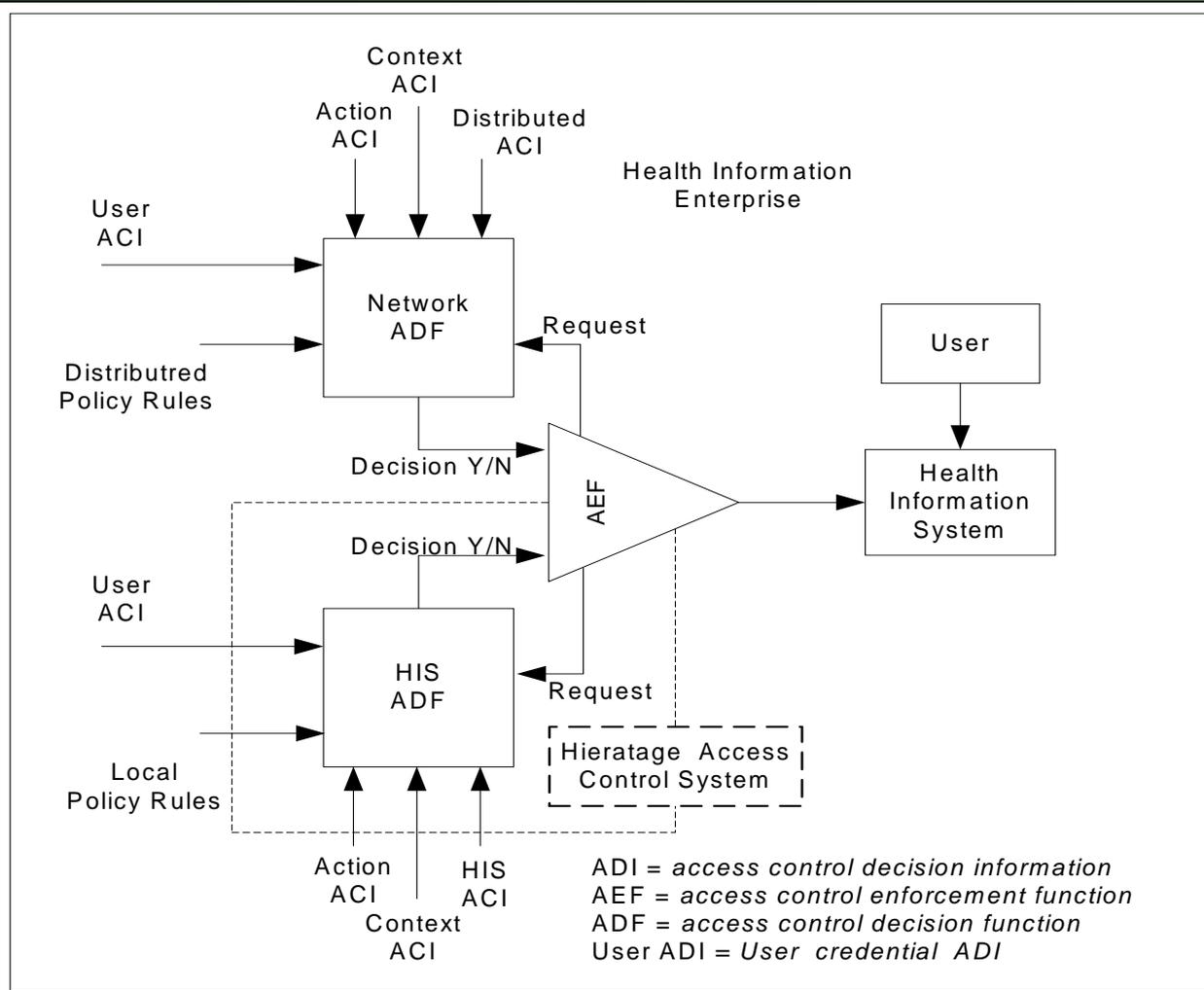


# Initially Affected VHA Projects

All HealthVet/VistA applications must be on board with AAIP Security. Current projects with near-term security requirements include:

- PATS (6/03)
- Patient Lookup (6/03)
- CPRS (9/03)
- CPRS HealthVet Desktop (9/03)
- Scheduling (10/03)
- HDR (11/03)
- Billing (4/04)
- VistA Imaging (4/04)
- My HealthVet

# Application Level Access Control Architecture



# Summary RBAC Standards Activity

- NIST
  - Draft RBAC Standard
- HL7
  - CCOW (AA middleware RBAC migration/PP)
  - Healthcare RBAC Standard <- Healthcare RBAC TF <- VHA RBAC TF
- ASTM
  - PMI and Identity Management Draft
  - PKI CP (E2212/E1986)
- OASIS
  - SAML/XACML