Health Information ARCHITECTURE

Role-Based Access Control (RBAC) Newsletter

Volume 23 – January 2006

Inside this issue:

- RBAC Review
- Healthcare Scenario Roadmap – HL7 Update
- Health Level Seven (HL7) Security and Accountability Technical Committee – DSTU Ballot Briefing Update
- Upcoming Meetings

VHA / IHS RBAC TF Chair
Robert O'Hara, MD
Robert.Ohara@med.va.gov

VHA Deputy Chief Architect
RBAC Project Manager
Steve Wagner
Steve.Wagner@med.va.gov

VHA Security Architect
RBAC Architect
Mike Davis, CISSP
Mike.Davis@med.va.gov

VHA Security Architect
RBAC Architect
Ed Coyne, PhD
Ed.Coyne@med.va.gov

VHA Software Security Architect
Amy Page
Amy.Page@med.va.gov

RBAC Project Lead
Suzanne Webb
Suzanne.Gonzales-Webb@saic.com

≈

ROLE BASED ACCESS CONTROL (RBAC) REVIEW

Security - Authentication and Access Control

Security is the ability to control access and protect information from accidental or intentional disclosure to unauthorized persons and from alteration, destruction or loss.

Authentication is about whom the user is, the ability to prove or validate the identity of a user or a transaction.

Access control, also known as authorization, refers to what an identified user can do and what that identified user can access. Access control implements technical policies and procedures for electronic information systems that maintain business information. This ensures access is only allowed to those users--people or software programs--that have been granted those specific access rights. Access control not only can grant access rights but can also restrict individual access.

Role-based access control administers a set of controls determining how subjects and objects interact. It is the active entity that requests access to an object or the data within an object.

- The subject may be a program, a user or a process,
- The subject accesses information to accomplish a task,
- The object is a passive entity that contains information, and
- An object may be a computer, a database, a field in a database table, a file or a directory.

With role based access control, rather than attempting to map an organization's security policy to a relatively low-level set of technical controls (i.e. an access-control list), each user is assigned to one or more predefined roles, each of which has been assigned the various privileges needed to perform that role. In RBAC, a user is associated with a role, and roles are associated with permissions. A user has permission only if the user has an authorized role that is associated with that permission.[1]

Security is managed with RBAC at a level that corresponds closely to the organization's structure. Each user is assigned one or more roles, and each role is assigned one or more privileges that are permitted to users in that role. Security administration with RBAC consists of determining the operations that must be executed by

[1] Role-Based Access Control (RBAC); September 2003 - Uday O. Ali Pabrai

RBAC Newsletter Editor

ATTN: Suzanne Webb
RBAC Project Lead
10260 Campus Point MS-B1E
La Jolla, CA 92121

Or e-mail:

Suzanne.Gonzales-Webb@va.gov

people in particular jobs and assigning members of the workforce to the proper roles.

Non-Licensed Personnel - Update

The HL7 Working Group meeting is currently on and the Security Technical Meeting are responding to any comments made to the submitted January ballot.

The following list of materials were prepared and submitted to HL7 and voted upon as a Draft Standard for Trial use in the January 2006 Ballot.

- HL7 RBAC Healthcare Permission Catalog v2.2,
- HL7 Healthcare Scenario Roadmap v2.19,
- HL7 RBAC Healthcare Scenarios v2.0,
- HL7 RBAC Role Engineering Process v1.1, and
- HL7 RBAC Role Engineer Process Applied Example v1.1.

HEALTH LEVEL SEVEN (HL7) SECURITY AND ACCOUNTABILITY TECHNICAL COMMITTEE

Draft Standard for Trial Use (DSTU) Ballot – UPDATE

The cast votes posted as of January 10, 2006 were as follows:

Name	Lvl.	Aff.	Neg.	Abst.	NV	TotP.	Q.	A
RBAC*	D1	30	7	2	1	40	**97.50%**	**25**

***** Role based Access Control Healthcare Permission Catalog

UPCOMING MEETINGS

- **NIST and FISSEA Conference** – Training for a Cyber-Secure Future, March 20-21, 2006 Bethesda, Maryland
- **ASTM Committee E31 on Healthcare Informatics**, May 22-24, 2006 Baltimore, Maryland
- **HIMSS Annual Conference and Exhibition** February 12-16, 2006 San Diego, California
- **INCITS CS1 Task Group, Cyber Security** February 1-2, 2006 San Jose, California

The HL7 Jan 2006 Ballot Criteria includes the following:

The voter participant breakdowns for the votes were as follows:

	Aff.	Neg.	Abst.	NV
Affiliate	2	6	0	0
Consultant	0	0	1	0
General Int.	1	0	0	1
Payor	0	0	0	0
Pharmaceutical	0	0	0	0
Provider	18	1	0	0
Vendor	9	0	1	0
Totals	**30**	**7**	**2**	**1**
% of Votes	75.00%	17.50%	5.00%	2.50%
Quorum	**97.50%**			
Approval	**25**			

Participants voting on the RBAC Permission Catalog included persons representing such firms as: US Department of Veterans Affairs; Kaiser Permanente; HL7 Germany; Health Level Seven, Inc.; HL7 Canada; Alschuler Associates LLC; Oracle Corporation; U.S. Department of Defense, Military Health System; GE Healthcare Information Technologies Healthcare; Siemens Medical Solutions Health Services; Shafarman Consulting, and the Regenstrief Institute, Inc.

TALLY LEGEND:

- Lvl. = Ballot Level,
- Aff. = Affirmative Votes,
- Neg. = Negative Votes,
- Abst. = Abstaining,
- NV = No vote Returned,
- TotP. = Total Participants,
- Q. = Quorum, and
- A. = Affirmatives Required for Approval.

CALCULATING QUORUM

- Committee Ballots (includes DSTUs and Updates): 60% Quorum, 2/3rds Approval,
- Membership Ballots: 60% Quorum, 90% Approval,
- Informative Ballots: No Quorum requirements, 2/3rds Approval,

RBAC Newsletter Editor

ATTN: Suzanne Webb
RBAC Project Lead
10260 Campus Point MS-B1E
La Jolla, CA 92121

Or e-mail:

Suzanne.Gonzales-Webb@va.gov

- Quorum is achieved by total affirmatives, negatives and abstains, and
- Approval is achieved by total affirmatives and negatives.

Quorum and Approval values in this **color** mean that required values have been achieved.

***

RBAC is critically important to the security aspects of the VA and other healthcare organizations. There is a growing management and security demand for RBAC to be implemented in healthcare systems.

RBAC grants rights and permissions to roles rather than individual users. Users then acquire the rights and permissions by being assigned to appropriate roles. By grouping individuals with other individuals who have similar access rights, RBAC can provide significant security management efficiencies.

The latest RBAC Documentation additions and prior RBAC Newsletters can be found on the RBAC Website.