



## Inside this issue:

- HL7 - RBAC Ballot Update
- HL7 Project Initiation for Constraints
- HITSP and HL7 Vocabulary Conformance Brief
- RBAC and Privacy Abstract
- RBAC Taskforce – Meeting Update
- Upcoming Meetings

### VHA/IHS RBAC TF Chair

Robert O'Hara, MD  
[Robert.OHara@med.va.gov](mailto:Robert.OHara@med.va.gov)

### VHA Deputy Chief Architect

RBAC Project Manager  
Steve Wagner  
[Steve.Wagner@med.va.gov](mailto:Steve.Wagner@med.va.gov)

### VHA Security Architect

RBAC Architect  
Mike Davis, CISSP  
[Mike.Davis@med.va.gov](mailto:Mike.Davis@med.va.gov)

### VHA Security Architect

RBAC Architect  
Ed Coyne, PhD  
[Ed.Coyne@med.va.gov](mailto:Ed.Coyne@med.va.gov)

### RBAC Project Lead

Suzanne Webb  
[Suzanne.Gonzales-Webb@saic.com](mailto:Suzanne.Gonzales-Webb@saic.com)

## HEALTH LEVEL SEVEN (HL7) WORKING GROUP MEETING

September 2007 - Atlanta, Georgia

### *Role Based Access Control – HL7 Ballot Update*

All remaining negative ballot items have been resolved or withdrawn. The reconciliation package and updates to the HL7 Permission Catalog have been updated and submitted. With this passing of the HL7 RBAC Ballot, it allows the Security Technical Committee to move forward with enhancements to the current vocabulary and further refinements to the accepted process as noted below.

**Recap:** Resolution of the Role Based Access control – HL7 Ballot continued during the Working Group meeting held in Atlanta, Georgia. The HL7 Security Technical Committee (TC) identified negative ballot items as good candidates for future work, but were not in the intended scope of current ballot. The Security TC then determined it was not persuaded to add new permission use cases to the current ballot. The identified non-persuasive items will be candidates for future extensions to the permission vocabulary. Discussions continue in order to resolve the substantive negatives still holding up the ballot. Other resolutions agreed upon at the HL7 September meeting have been updated to the current HL7 RBAC Permission catalog. The latest version of the Permission Catalog will be posted on the RBAC Website.

The September Out-of-Cycle Ballot was completed in September 2007. Negative comments and votes were evaluated. Within the current RBAC ballot resolution spreadsheet, all negative voters have been notified of the dispositions of their votes and have been notified of their right to appeal. Contact has been made with voters who have agreed verbally to withdraw their negative votes and this information has also been posted on the RBAC ballot resolution spreadsheet. The remaining voters have been contacted for further open discussion to resolve remaining issues.

### *HL7 Project Initiation for Constraints*

As part of the continuing work with RBAC, the Security Technical committee will include coordination with the ISO PMAC<sup>1</sup> policy standard to include constraints. The Security TC will also be focusing on closing the identified HITSP<sup>2</sup> and other standard organizational gaps in communication of privacy policies.

<sup>1</sup> ISO PMAC - International Organization for Standardization Privilege Management and Access Control

<sup>2</sup> HITSP – Health Information Technology Standards Panel



## Upcoming Meetings

- **Open Standards Int'l Conference**  
November 28-29  
Beijing, China
- **International e-Health Conference**  
December 2 - 5, 2007  
Regensburg, Germany
- **4th Nationwide Health Info Network forum: Trial Implementations (NHIN forum)**  
December 11-12, 2007  
Long Beach, CA
- **HL7 Working Group**  
January 13-18, 2008  
San Antonio, TX
- **INCITS CS1 Mtg #12**  
January 23-24, 2008  
San Jose, CA
- **2nd International Conference on Pervasive Computing Technologies for Healthcare 2008**  
30 Jan - 1 Feb 2008  
Tampere, Finland
- **INCITS CS1 Mtg #13 (ITI-INCITS HQ)**  
February 27-28, 2008  
Washington, DC

## RBAC Newsletter

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

Or e-mail:

Suzanne.Gonzales-Webb@va.gov

Using the definition from Neumann and Strembeck, constraints are restrictions (conditions or obligations) that are enforced upon access permissions. In RBAC, a constraint may restrict for example, a user to continue to have an *action* on the data they are accessing. This could include contextual properties such as separation of duties, time-dependency, mutual exclusivity, cardinality, location, etc.

For the complex healthcare environments, constraints provide the higher flexibility required in RBAC implementation.

One has to ask first in dealing with constraints with respect to access control, which parts of these unmanageable quantities of context information are relevant for a specific authorization decision, and how the corresponding information may be elicited and defined on the modeling level. In the Constraint document posted on the RBAC website, we suggest a process for the specification of context constraints. This process is based as an extension to the scenario-driven role engineering process for RBAC roles presented in Neumann and Strembeck.<sup>3</sup>

In Role-Based Access Control, users (i.e., individuals or authorization services, etc.) are given a set of permissions (the ability to have an action such as create, read, write, etc.) on an object (a laboratory order, patient history, etc.). In a healthcare environment arena however, increased flexibility in RBAC is needed as the duties and functions of identified structural roles such as a physician, nurse or pharmacist<sup>4</sup> in relation to accessing an information system can vary on the time of day, their location (i.e., clinic, ward) and when the additional temporary duties are assigned (i.e., supervisory or administrative). These conditional changes or constraints modify the level of access control an individual user may have. One possibility to deal with this dynamically changing context is to rapidly modify permission assignment relations according to the changes in the (healthcare) environment. This central idea supports constraints on almost all parts of an RBAC model (e.g., permissions, roles, or assignment relations) to achieve a high flexibility.<sup>5</sup>

<sup>3</sup> M. Strembeck and G. Neumann, An Integrated Approach to Engineer and Enforce Context Constraints in RBAC Environments; Received November 2003; revised March 2004, April 2004 and May 2004; accepted May 2004

<sup>4</sup> Structural roles are categories of healthcare personnel warranting differing levels of access control. Structural roles allow a user to 'connect' to a resource, but do not grant authorization. Structural roles define what specific healthcare workflow users are allowed to participate in, while functional roles define authorizations granted to an entity to allow access (i.e., to protected health information).

<sup>5</sup> Ibid, M. Strembeck and G. Neumann



## Upcoming Meetings

- **INFOSEC World Conference**  
March 10-12, 2008  
Orlando, FL
- **The 5th Annual World Health Care Congress**  
April 21 – 23, 2008  
Washington, DC
- **HL7 Working Group**  
May 4-9, 2008  
Phoenix, AZ
- **TEPR 2008**  
May 17 – 21, 2008  
Ft. Lauderdale, FL
- **17th Annual WEDI National Conference**  
May 19 – 22, 2008  
Baltimore, MD
- **IEEE Security & Privacy Symposium**  
May 21-24, 2008  
Berkeley/Oakland, CA
- **13<sup>th</sup> ACM SACMAT**  
June 11-13, 2008  
Estes Park, CO

## RBAC Newsletter

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

Or e-mail:

Suzanne.Gonzales-Webb@va.gov

## *HITSP and HL7 Vocabulary Conformance Brief*

It was also noted in the meeting minutes of the HL7 Security TC meeting that HITSP uses the IHE DSG<sup>6</sup> profile, which coincides with the HL7 Security Technical Committee's advice that Structured Documents use the XML digital signature specification as-is. The Access control construct within HITSP references the HL7 RBAC permission vocabulary. Mike Davis will drive evaluation of the HL7 RBAC vocabulary relative to HITSP use cases.

## *RBAC and Privacy Abstract*

The abstract titled: *Privacy-aware Role Based Access Control* was presented at SACMAT'07 conference held in Sophia Antipolis, France, on June 20-22, 2007. The abstract was written by authors: Qun Ni and Professor, Elisa Bertino of Purdue University, Jorge Lobo from IBM and Alberto Trombetta of Insubria University, Italy.

In this abstract, the group of authors introduces a family of models they name as P-RBAC that extends the current familiar RBAC model in order to support fully and express privacy policies, while also taking account features such as purposes and obligations.

## **Introduction**

There has been a noticeable separation of security and privacy in the recent few years. Privacy today is a key issue in information technology and has received increasing attention from consumers, companies, researchers and legislators. Legislative acts such as HIPAA<sup>7</sup> and GLBA<sup>8</sup> have required enterprises to protect the privacy of their customers. The goal of the work reported in this paper is to extend the classical RBAC model in order to support privacy-aware access control and privacy policies. In the authors' model, privacy policies are expressed as permission assignments which differ from permissions in classical RBAC because of the presence of additional components representing privacy related information. Also introduced is the development of conflict analysis algorithms to detect conflicts among the permission assignments to avoid problems that have occurred with rules involving enterprise privacy authorization language.

<sup>6</sup> Integrating the Healthcare Enterprise Document Digital Signature

<sup>7</sup> HIPAA – Health Insurance Portability and Accountability Act

<sup>8</sup> GLBA – Gramm Leach Bliley Act for financial institutions, require enterprises to protect the privacy of their customers



## **Role-Based Access Control (RBAC) Newsletter**

### **RBAC Taskforce – Meeting Update**

The RBAC Taskforce meeting calls are held on the **SECOND** Wednesday of every month at 1300CT / 1100PST / 1200MT / 1400EST; a meeting reminder is sent to current participants. If you would like to participate in the Task Force please contact Suzanne Gonzales-Webb for more information.

Role-Based Access Control is critically important to the security aspects of the Veterans Health Administration and to other organizations. There is a growing management and security demand for RBAC to be implemented.

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.

≈

**The RBAC Newsletter is now published quarterly instead of monthly. Please be on the lookout for the next issue due January/February 2008!**

### **RBAC Newsletter**

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

Or e-mail:

[Suzanne.Gonzales-Webb@va.gov](mailto:Suzanne.Gonzales-Webb@va.gov)

≈