



Inside this issue:

- ✍ Japan – Lecture outlines on RBAC and the Personal Information Attribute Authentication Act
- ✍ RBAC Taskforce - 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

~

RBAC and the Next Generation Electronic Commerce Promotion Council of Japan (ECOM) – Lecture Review

<Editor's note> I had the pleasure of meeting Mr. Miyohara at an HL7 meeting here in San Diego. He has attended several HL7 Security Technical meetings and has also presented information to the security technical committee. This lecture given at ECOM covers two organizations and their examination of similar attribute authentication in their relation to security in healthcare/medical information and finishes with an introduction to efforts being made in Japan's Medical Information Infrastructure. I have taken in context, small liberties using the English version of his lecture to further clarify Mr. Miyohara's perspectives.

“The Latest Trend of Attribute Authentication in the Medical Field” - Mr. Hideyuki Miyohara-Chair of Security Committee, Japanese Association of Healthcare Information Systems Industry (JAHIS)

A tangible example for examining attribute authentication (internationally) in the medical field would be if an injury or illness were to occur in a foreign country, an overseas medical institution may need access to medical information in the patient's home country. With an international attribute authentication in place, this access ability can occur and thus put in place proper care for the patient.

ISO/TC215 WG4 (Health Informatics in charge of security) is a representative standards organization examining standardization of security in the area of medical information.

Privilege Management and Access Control (PMAC) is a standard for enabling access controls based on authority management between domains with different policies (e.g. qualifications of doctors



Upcoming Meetings

- ✍ **INCITS CS1 Task Group CS1.1, Role-Based Access Control (RBAC)**
May 3, 2006
Gaithersburg, MD
- ✍ **ASTM Committees E31 May 2006 Meeting (in conjunction w/TEPR)**
May 22 - May 24 2006
Baltimore, MD
- ✍ **HL7 Working Group Meeting**
May 7 - 12, 2006
San Antonio, TX
- ✍ **OASIS Symposium**
9-12 May
San Francisco, CA
- ✍ **ONC (ONCHIT) American Health Information Community Meeting**
May 16, 2006
Washington, DC 20201
- ✍ **11th ACM SACMAT 06 Conference**
June 7-9, 2006
Lake Tahoe, CA

~

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

between Japan and the US). This is being examined by the working group of ISO Technical Committee 215. PMAC is classified into:

- ✍ Framework – Part 1,
- ✍ Modeling – Part 2, and
- ✍ Implementation – Part 3.

Parts 1 and 2 have already been released and Part 3 is currently being formulated.

The purpose of PMAC is to enable information exchange among domains with different security policies in the area of healthcare and to work as a bridge by concluding policy agreements. It also aims to map structural roles that are independently defined within domains into functional roles and to enable authority management in other domains.

Another standards organization, HL7 (HL7 Security Technical Committee) is also examining security-related standardization in the exchange of medical information. With regard to the examination of attribute authentication by the HL7 Security Technical Committee, Role Based Access Control or RBAC is being investigated as a standard for controlling access based on roles for controlling access in a domain of a medical information system. RBAC is a standard for controlling access by means of role-based authority management. This role-based authority management is being promoted by the National Institute of Standards and Technology (NIST) and is registered with the American National Standards Institute (ANSI). The RBAC draft standard of HL7 has adopted a scenario-driven type as a role definition method. It has been prepared in part based on actual role definition examples in hospitals for U.S. Veterans.

In the United States, the following efforts have been made toward domains with different policies the implementation of attribute authentication:



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

- ✍ Identity and access management,
- ✍ application of RBAC,
- ✍ permission tables, and
- ✍ use of the OASIS RBAC standard.

Identity and Access Management (IAM) contains the concepts of directory service, single sign-on and access control, while RBAC is being adopted within the concept of the privilege management infrastructure (PMI) of IAM. As for implementation based on the OASIS standard of PMI, basic and functional roles are defined in XACML (eXtensible Access Control Markup Language), which is a policy description language. In addition, access privileges and resource information are described in SPML (Service Provisioning Markup Language), which is a specification for exchanging provisioning information, and requests and responses are described in SAML (Security Assertion Markup Language), which is a security information description language. The U.S. researchers aim to construct efficient systems by adopting these OASIS standards and by making use of the products and tools of the vendors who support them.

In Japan, for the purpose of promoting a Healthcare Public Key Infrastructure (HPKI), the following efforts have been made:

- ✍ examination by the Investigative Committee on Medical Information Network Infrastructures,
- ✍ establishment of CPs (certification policies) and compliance audit rules by the Ministry of Health, Labour and Welfare,
- ✍ the separation of signatures for HPKI and other purposes (for certification and encryption), and
- ✍ development of nationally uniform rules for signature purposes, etc.



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

HPKI will be developed as part of social infrastructures in Japan in a manner consistent with international standards and in line with the New IT Reform Strategies. With HPKI, it is possible to simultaneously confirm both identity and attributes by examining a certificate, and to confirm both national qualifications (doctor's signature or signatures and seals are required for clinical record provision letters, in other words, letters of introduction) and managers of medical institutions (confirm if they are responsible for issuing electronic receipts).

It may be too early to establish nationally uniform rules for attribute authentication because of differences in role definitions of individual domains that cooperate regionally with one another. Per Mr. Miyohara, it is necessary to start with consensus building of a framework to construct national-level attribute authentication infrastructures, the mapping of structural and functional roles, and policy development in Japan for exchanging medical information.

RBAC Taskforce – Update

The first RBAC Constraint meeting was held on Wednesday, April 12th, 2006 with representatives from the RBAC Licensed, RBAC Non-Licensed.

The RBAC Taskforce will continue to meet once a month on the first Wednesday to discuss and prepare the addition of constraints to the current Permission Catalog and Roles. The next meeting is scheduled for May 3rd at 11:00am PT / 1:00pm CT / 2:00pm ET. The agenda will be distributed prior to the meeting.

If you have questions regarding the information discussed about the constraints process and/or would like to participate, please feel free to contact Suzanne Gonzales-Webb at suzanne.l.gonzales-webb@saic.com or 858-826-6621



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

HEALTH LEVEL SEVEN (HL7) SECURITY AND ACCOUNTABILITY TECHNICAL COMMITTEE

Draft Standard for Trial Use (DSTU) Ballot – UPDATE

A few comments remain on the documentation submitted for the January ballot and are in the process of reconciliation and/or removal request. The following list of materials were prepared and submitted to HL7 and voted affirmatively 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.

Role-Based Access Control 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.