

Source	DMAG-UPC (A member of HL7 Spain)
Title	DMAG contribution to the HL7 Security and Privacy Ontology
Status	Input Contribution
Authors	Jaime Delgado (jaime.delgado@ac.upc.edu) Eva Rodríguez (evan@ac.upc.edu) Víctor Rodríguez (victorr@ac.upc.edu)
Date	2010/12/23

1 Introduction

The Distributed Multimedia Applications Group (DMAG) of the Universitat Politècnica de Catalunya (UPC) proposes in this document the use of a standard ontology, the Media Value Chain Ontology (MVCO) standardised by ISO/IEC JTC1/SC29 WG11 (MPEG) as ISO/IEC IS 21000-19, to represent the HL7 Role Based Access Control (RBAC), and more specifically the Permission Catalog.

Section 2 of this document presents the DMAG research group, focusing on the work that this group has done on ontologies, as well as its experience in standardization and in research projects.

Section 3 presents the proposed alignment of MVCO with the HL7 RBAC model. It shows that the RBAC model defined in the HL7 Security and Privacy Ontology is equivalent to the permission model defined in MVCO. Therefore, it could be advantageous for the HL7 Security Group to make explicit that the security and privacy ontology is compatible with a standard one. This document also provides some examples, in section 4, to illustrate the usage of the MVCO in HL7 RBAC scenarios.

As the HL7 Security and Privacy Ontology is in a review stage, section 5 provides some comments for this ontology.

Finally, section 6 proposes the use of standard Reference Software to build HL7 ontology-based applications. Moreover, it points out the use of DRM tools, based on MPEG-21 standard technologies, as an alternative to RBAC.

2 Background

2.1 DMAG

The DMAG [1] is a research group of the Computer Architecture Department at the UPC [2] in Barcelona (Spain) and a member of HL7 Spain since 2010. DMAG research and development activities deal with the management and distribution of multimedia content in a secure way, metadata search and interoperability, and all aspects of security, privacy, access control, and digital management of rights. DMAG members have long experience in standardisation, as editors of several standards in working groups of ISO/IEC, EWOS, CEN/ISSS, ETSI and ITU-T. From the standardisation activities, it is worth mentioning here the last work done on the Media Value Chain Ontology [3], Intellectual Property Management and Protection [4], Rights Expression Languages [5] profiles, Multimedia Application Formats [6], Query Formats [7], etc.

It is also important to note that the DMAG has been also providing reference software and experiments for the different standards in which DMAG members have been involved.

The DMAG has long experience in European research projects, such as the AXMEDIS Integrated Project, the European Networks of Excellence VISNET and VISNET-II, MOBIHEALTH, an old key European take-up action in the area of mobile applications for healthcare, etc., as well as in National research and industry projects.

Finally, the DMAG has an active participation in the creation of Ontologies for different aspects of the content value chain, including user roles, rights and actions, domains, etc. The most relevant activities are:

- *Media Value Chain Ontology (MVCO)* is an ontology for formalizing the representation of the Media Value Chain in the context of MPEG-21. It is Part 19 of MPEG-21.
- *Represent Rights Ontology (RRDOnto)* provides a model for describing the Intellectual Property Value Chain in the context of the Digital Media Project, which is the predecessor of MVCO.
- *Intellectual Property Rights Ontology (IPROnto)* is an ontology that describes intellectual property rights based on different initiatives in the field and our own contributions. It was initially developed as an answer to the Call for Proposals for a MPEG-21 Rights Expression Language and Rights Data Dictionary standard
- *Open Digital Rights Language Ontologies (ODRLOntos)* are two ontologies representing semantically the ODRL 1.1 Expression Language (EX) and Data Dictionary (DD). Its definition was useful in the analysis and bridging of the different Rights Expression Languages.

2.2 MPEG-21 Media Value Chain Ontology

ISO/IEC IS 21000-19 [3] standardises a Media Value Chain Ontology (MVCO), which formalizes the representation of the Media Value Chain. It represents in a standard way the Intellectual Property (IP) along the Value Chain, by means of different kinds of Intellectual Property entities, Actions and User roles. In this context, there are different types of objects, also called *IP Entities* (Work, Adaptation, Manifestation, Instance, Copy, Product), and different *actions* that are performed on them (CreateWork, MakeAdaptation, MakeManifestation, MakeInstance, MakeCopy, Produce, Distribute, EndUserAction), and different users that can perform these actions according to their *roles* (Creator, Adaptor, Instantiator, Producer, Distributor, EndUser).

MVCO defines the relationships among Users, IP Entities and Actions as depicted in Figure 1. In this figure, the round boxes represent classes, and the arrows object properties (heading from domain class to range class).

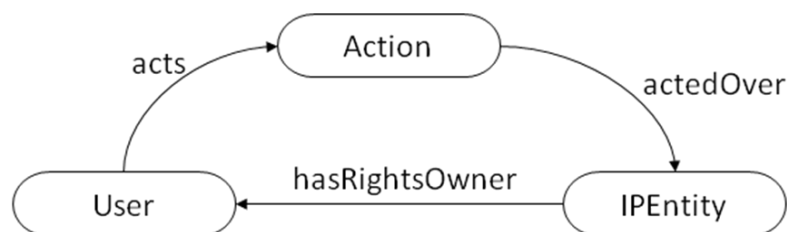


Figure 1. MVCO model – Relationships among User, Action and IPEntity.

In the MVCO ontology, permissions represent the transfers of rights. A *Permission* relates an *IP Entity* with the transmitted right, the original and the new rights owners. A *Permission* may require the prior fulfilment of conditions, and these conditions are represented as Facts. These

Facts are general statements with a binary truth value, describing any constraint related to the context or the users. Figure 2 shows the Permission model in MVCO.

The MVCO specification describes some other classes not relevant for the HL7 context, but, in any case, it remains a simple ontology with relatively few classes and properties.

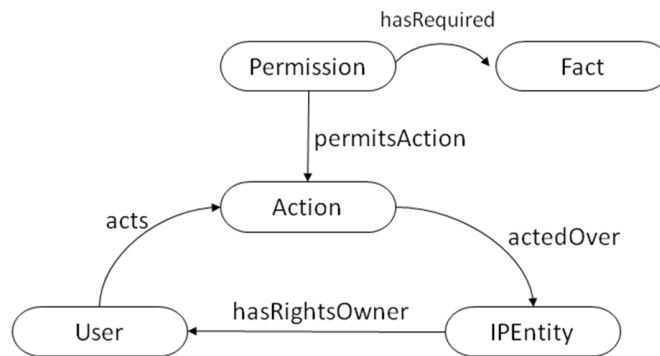


Figure 2. MVCO Permission model

3 HL7 Security and Privacy Ontology versus MPEG-21 MVCO

HL7 security working group is defining an ontology that “will cover the security and privacy domains as they pertain to healthcare IT”. They have initially focused on the Role Based Access Control (RBAC), more specifically, as specified in the HL7 RBAC Permission Catalog [8] [9]. Figure 3 shows our view of the current Security and Privacy Ontology model, only taking into account the entities defined in the HL7 RBAC. We use the MVCO style of representation.

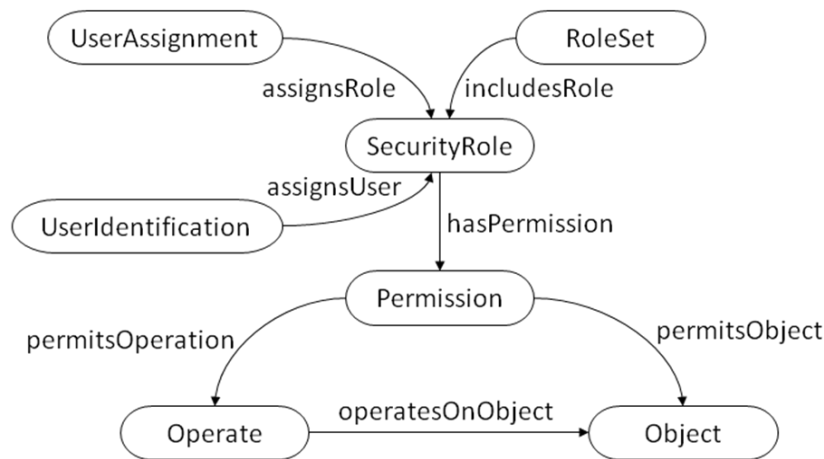


Figure 3. HL7 RBAC Ontology Model

This model is equivalent to the one standardised by MPEG in part 19 of the MPEG-21 standard. Figure 4 shows the MPEG-21 MVCO model equivalent to the HL7 Security and Privacy Ontology, i. e., a way for MVCO to express the HL7 RBAC Security and Privacy Ontology.

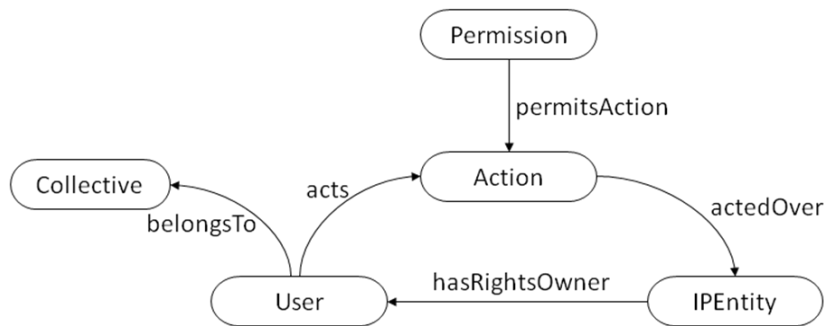


Figure 4. MVCO Model equivalent to the HL7 Ontology

4 Examples of MVCO use for HL7

This section describes which class individuals are present in the MVCO ontology for specific permissions and roles in an HL7 RBAC scenario. We have chosen the “POE-003 New Radiology Order” from the “Scenario SOE-001 Physician with Order Entry Privileges” described in the RBAC Healthcare scenarios document [10].

Scenario SOE-001. Physician with Order Entry Privileges

“Mr. Patient was placed in a clinic examination room for a Diabetic Consultation

...

The Physician asked Mr. Patient about any problems or concerns

...

The Physician did an examination of Mr. Patient, and entered the results of the examination into the EHR. Upon his earlier review of the EHR, he noted that Mr. Patient had not had a recent electrical cardiogram (ECG), so he ordered an ECG <<POE-003 New Radiology Order>> for Mr. Patient for review at a subsequent visit.” (Extracted from [10])

OWL individuals in the MVCO represent real Users, Roles, IP Entities, Actions and Permissions. In the scenario under consideration, Bob, a Physician ordering an electrical cardiogram is represented by the ontology with five class individuals: Bob, the Physician, the new Radiology Order, the action Create, and the permission NewRadiologyOrder1. Figure 5 represents the five individuals and the relations (object properties) by means of arrows. In that diagram, each box represents an individual, whose name is given first, followed by the main class it belongs to (in fixed width font). Arrows represent object properties linking the individuals.

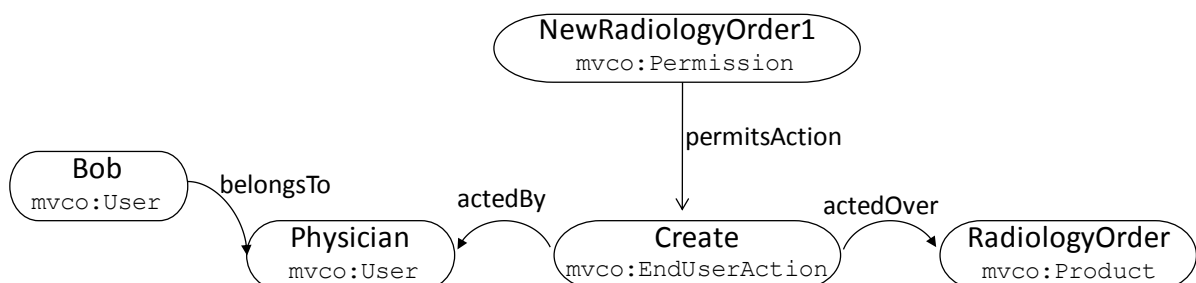


Figure 5. Class individuals in the MVCO ontology for the New Radiology Order POE.

5 Comments to the HL7 Security and Privacy Ontology

Based on what we have stated in sections 3 and 4, DMAG comments to the current version of the HL7 Security and Privacy Ontology for initial peer review (“Posted 11/15/2010”) are the following:

- The Security and Privacy ontology might be split in two, since it includes elements for security (with policies and permissions, etc.) and elements for record objects together.
- The ontology file could be more self-descriptive, including a definition for each of the classes. While currently some classes do have such a comment, we believe that all of them should have it, although it is probably already planned. Also, the way of giving the definition (currently through `dc:description`) is not, to our understanding, the most common practice. We think that `dc:description` should be left for annotating the ontology itself, while for documenting the classes and properties `rdfs:comment` should be preferred. Additionally, a version statement for each class would prove useful if more ontology editions are to be issued.
- Having a good collection of individual examples is pivotal for understanding the model. More individual examples might be added to the DemoLocalSecurityAndPrivacy Ontology (as the one we propose, depicted in Figure 6), where again, each box represents an individual, whose name is given first, followed by the main class it belongs to (in fixed width font).

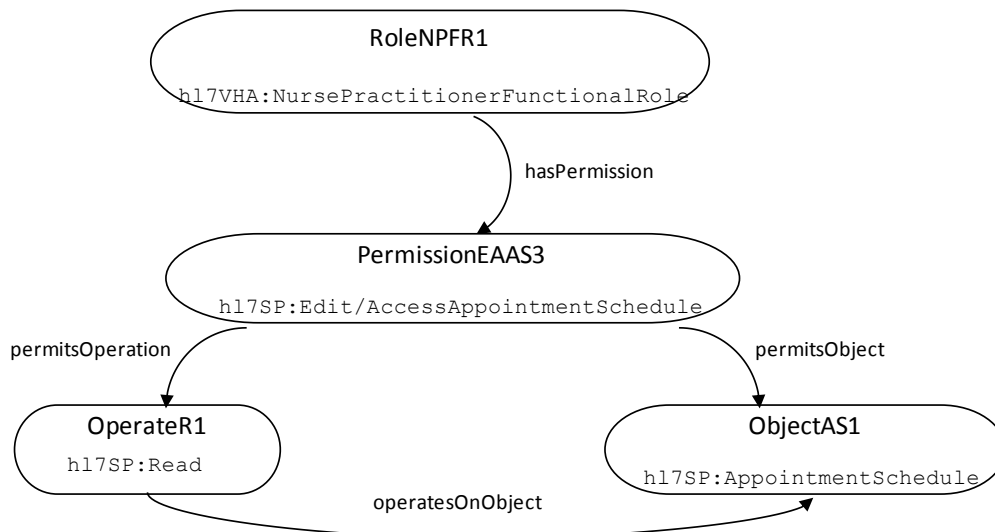


Figure 6. Class individuals in the HL7 Security and Privacy and VHA ontologies.

- The Functional Roles defined in the VeteransHealthAdministration (VHA) ontology might be defined in the same way. This ontology defines the *NursePractitionerFunctionalRole* and *RegisteredNurseFunctionalRole* as subclasses of *NurseFunctionalRole*. It also defines *MD/AllopathFunctionalRole*, but not as a subclass of *PhysicianRole*, which is not defined in the ontology. Then, the *MD/AllopathFunctionalRole* might be defined as subclass of *PhysicianRole*, as depicted in Figure 7.

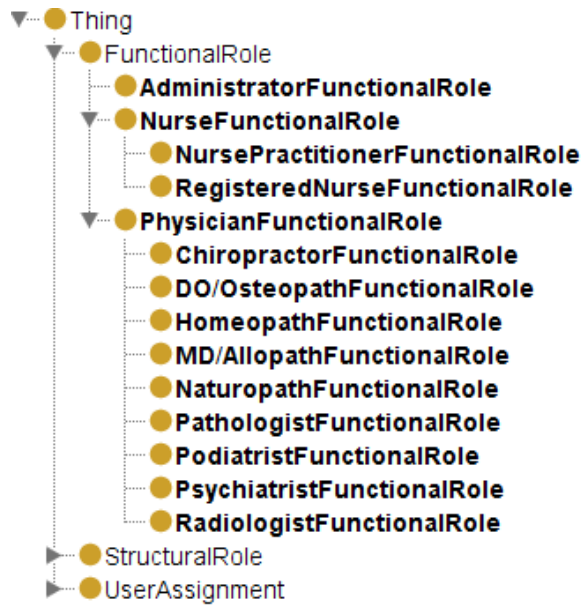


Figure 7. Functional Roles – VeteransHealthAdministration ontology.

- The VeteransHealthAdministration ontology associates Permissions to Roles through the object property *hasPermission*. At the moment, it only defines the permissions for the *MD/AllopathFunctionalRole*, which has all the permissions (i. e., order entry, perform and review documentation, and scheduling). Probably, it is planned to define the rest of the relations as specified in the HL7 HealthCare Scenario Roadmap v2.20 [11]. If not, we think that it might be useful to specify, at least, how these associations should be defined for Roles to which not all the permissions are granted, unlike the *MD/AllopathFunctionalRole*.

In any case, the assignment of permissions to roles remains somewhat unclear. In the example provided (*DemoLocalSecurityAndPrivacy.owl*), the assignment *_AssignDoctorWelbytoAllopathStructuralRole* (individual of *UserAssignment*) is related to Dr. Welby (individual of *UserIdentification*) through an object property (*assignUser*), but the assignment is not related to any role, existing only a simple restriction (saying only that *_AssignDoctorWelbytoAllopathStructuralRole* can be related to one or more individuals of *MD/AllopathFunctionalRole*). We believe that this relationship should be explicitly expressed, being the *UserAssignment* equally related to a *UserIdentification* individual and a *SecurityRole* individual. Figure 8 shows the existing relationship in black colour, and the proposed elements in gray.

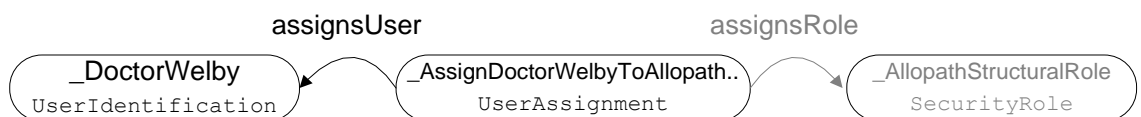


Figure 8. Proposal for assignment of Doctor Welby to a SecurityRole

- The schema in Figure 8 assumes the principle that relationships must always be expressed as object properties relating individuals to individuals, and never be given as restrictions imposed on the object properties. This leads to having to declare individuals like *_AllopathStructuralRole* (the box in the right in Figure 8 represents this individual, of the class *MD/AllopathStructuralRole*). The same principle can be applied to the assignment of permissions to roles, which is currently expressed

through mere object properties, and which perhaps should relate actual roles to actual permissions. We believe that it would be handier if each of the currently defined subclasses of `Permission` (e.g. `NewConsultOrder`) were defined as an individual of the `Permission` class.

6 Future contributions

6.1 Tools

In practice, HL7 ontology-based applications will have to provide a user interface to introduce or retrieve information. While the development of these tools is beyond scope, some basic tools handling HL7 ontology data may be drafted and exhibited as HL7 Tools and Resources for demonstration purposes or as a development aid, in a similar way to ISO “Reference Software”. Moreover, semantic authorisation tools developed for the MVCO can be also used for the HL7 Security and Privacy ontology for authorisation purposes. We have already developed some basic tools with this purpose.

6.2 DRM

The HL7 Security Work Group proposes in document “Role Based Access Control (RBAC) Healthcare Permission Catalog, version 4.10” [8], that implementers may use Digital Rights Management (DRM) as an alternative to RBAC. A possible choice pointed out in this document is the usage of MPEG-21 standard technologies.

The MPEG-21 standard provides technologies for the representation of digital objects. Part 2 of the MPEG-21 standard (ISO/IEC 21000-2) [12], entitled Digital Item Declaration, specifies a model for defining Digital Items, which are formed by the digital content (reference or embedded), plus its related metadata describing the content, e.g. how it has been protected, governed, processed, etc. Thus, in HL7, ISO/IEC 21000-2 could be used for the representation of clinical documents and electronic or patient health records. We are working in a proposal for representing protected EHRs with MPEG-21.

Part 4 of the MPEG-21 standard (ISO/IEC 21000-4) [4], entitled Intellectual Property Management and Protection (IPMP) Components, defines a model for the protection of Digital Items at any level of granularity, from a complete Digital Item to a specific asset. It also specifies a standard ways for describing IPMP tools and for retrieving them from remote locations. Finally, it defines how protection and governance information can be associated to protected Digital Items. Then, ISO/IEC 21000-4 can be useful for protecting clinical documents and electronic or patient health records at any level of granularity, for describing the protection tools used, and finally for associating this information to the protected document.

Part 19 of the MPEG-21 standard, described in section 2.2, can be used to specify the permissions and roles defined in the HL7 RBAC, as presented in section 3. The permissions can be later associated to digital objects (e.g. clinical documents) by means of MPEG-21 IPMP Components technology.

Part 15 of the MPEG-21 standard (ISO/IEC 21000-15) [13], Event Reporting, provides standard mechanisms for sharing information about events, related to Digital Items, amongst peers and users of the MPEG-21 Multimedia Framework. These technologies could be useful to report the events occurred within or between HL7 EHR systems.

6.3 MPEG-21 alignment

HL7 Security Work Group also proposes in [8] a possible future alignment with the MPEG-21 Rights Data Dictionary (ISO/IEC 21000-6). However, we have proposed the usage of the MPEG-21 Multimedia Value Chain Ontology (ISO/IEC 21000-19) to represent the HL7 RBAC. This standard ontology defines a permission model compatible with the HL7 RBAC, as demonstrated in section 3. Therefore, it is a better alternative than the MPEG-21 RDD, since MVCO defines a standard permission model suitable for HL7 RBAC, and it can be extended to support all the operations defined in the HL7 RBAC Permission model. Regarding this second issue, we think that it is better to extend an existing standard with new terms, than trying to modify existing definitions.

7 References

- [1] DMAG, <http://dmag.ac.upc.edu/>.
- [2] UPC, <http://www.upc.edu/>.
- [3] ISO/IEC, ISO/IEC 21000-19:2010 – Information Technology – Multimedia Framework (MPEG-21) – Part 19: Media Value Chain Ontology.
- [4] ISO/IEC, ISO/IEC 21000-4: 2006 – Information Technology – Multimedia Framework (MPEG-21) – Part 4: Intellectual Property Management and Protection Components.
- [5] ISO/IEC, ISO/IEC 21000-5:2004 – Information Technology – Multimedia Framework (MPEG-21) – Part 5: Rights Expression Language.
- [6] ISO/IEC, ISO/IEC 23000-7:2008 – Information Technology – Multimedia application format (MPEG-A) – Part 7: Open access application format.
- [7] ISO/IEC, ISO/IEC 15938-12:2008 – Information Technology – Multimedia content description interface (MPEG-7) – MPEG Query format.
- [8] HL7 Security Technical Committee, *“Role Based Access Control (RBAC) Healthcare Permission Catalog Version 4.10”*, January 2010.
- [9] HL7 Security Technical Committee, *“HL7 Role-based Access Control (RBAC) Role Engineering Process Version 1.1”*, November 2005.
- [10] HL7 Security Technical Committee, *“Role Based Access Control (RBAC) Healthcare Scenarios Version 2.0”*, November 2005.
- [11] HL7 Security Technical Committee, *“HL7 Healthcare Scenario Roadmap v2.20_Licensed_Providers”*.
- [12] ISO/IEC, ISO/IEC 21000-2:2005 – Information Technology – Multimedia Framework (MPEG-21) – Part 2: Digital Item Declaration (2nd Edition).
- [13] ISO/IEC, ISO/IEC 21000-15:2006 – Information Technology – Multimedia Framework (MPEG-21) – Part 15: Event Reporting.