

Interpretation of the Healthcare Scenario Roadmap

1 Introduction

The Healthcare Scenario Roadmap was developed to scope the extent of effort required by the role engineering team. The model consolidates several important role-engineering concepts and provides a concise way to define the role engineering effort in a way useful for knowledgeable healthcare persons.

This paper is an interpretation of the roadmap in terms of other models.

2 Role Engineering Models

The RBAC TF will use role-engineering models to assist it in carrying out its activities. Models illustrate relationships between components of an abstract role system to the components of the role engineering process. Two models significant to interpreting the roles engineering roadmap are the Scenario Model and the Role Engineering Model.

2.1 Work Profiles, Tasks, Scenarios and Steps

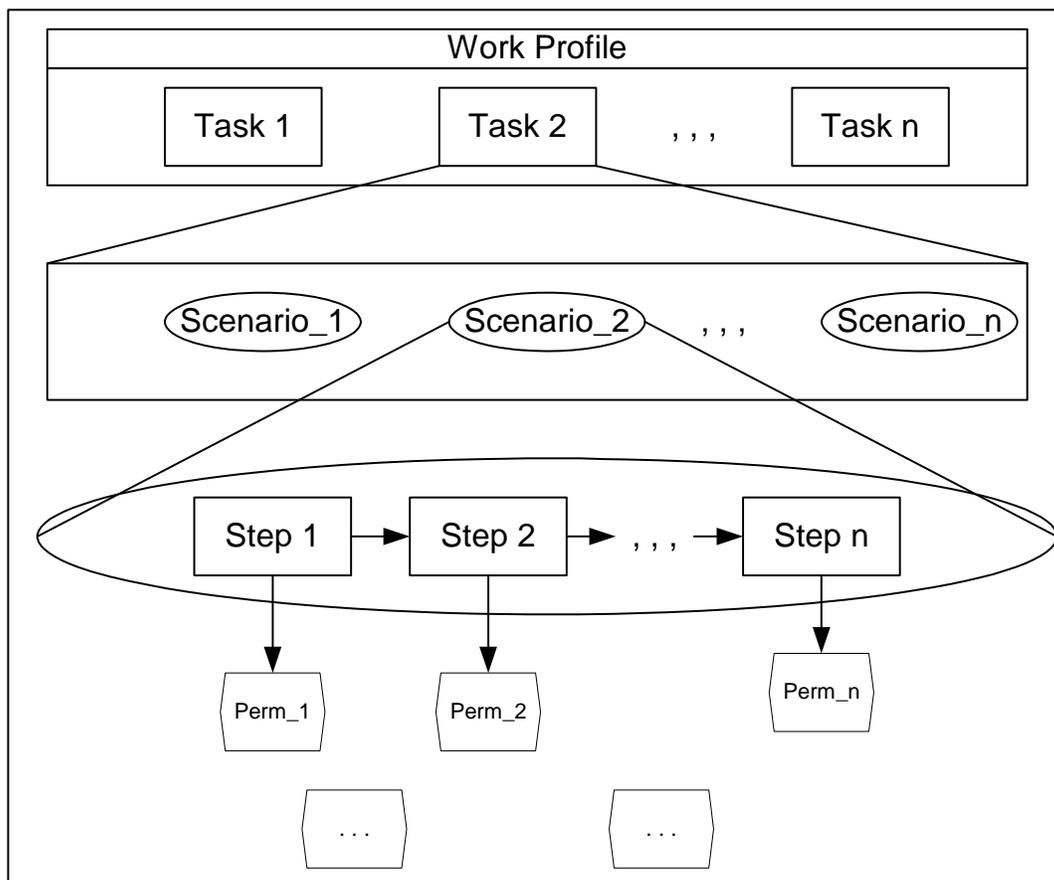


Figure 1: Scenario Model [Neumann/Strembeck]

The Scenario Model, as shown in Figure 1, illustrates the hierarchy of work profile, task, scenario, and step. Permissions are defined relative to steps described in the role engineering process.

2.2 RBAC TF Role Engineering Model

Figure 2 illustrates the core unified RBAC TF Role Engineering Model. It consolidates the permission→work profile relationship, the core RBAC Model, and the HL7 RIM.

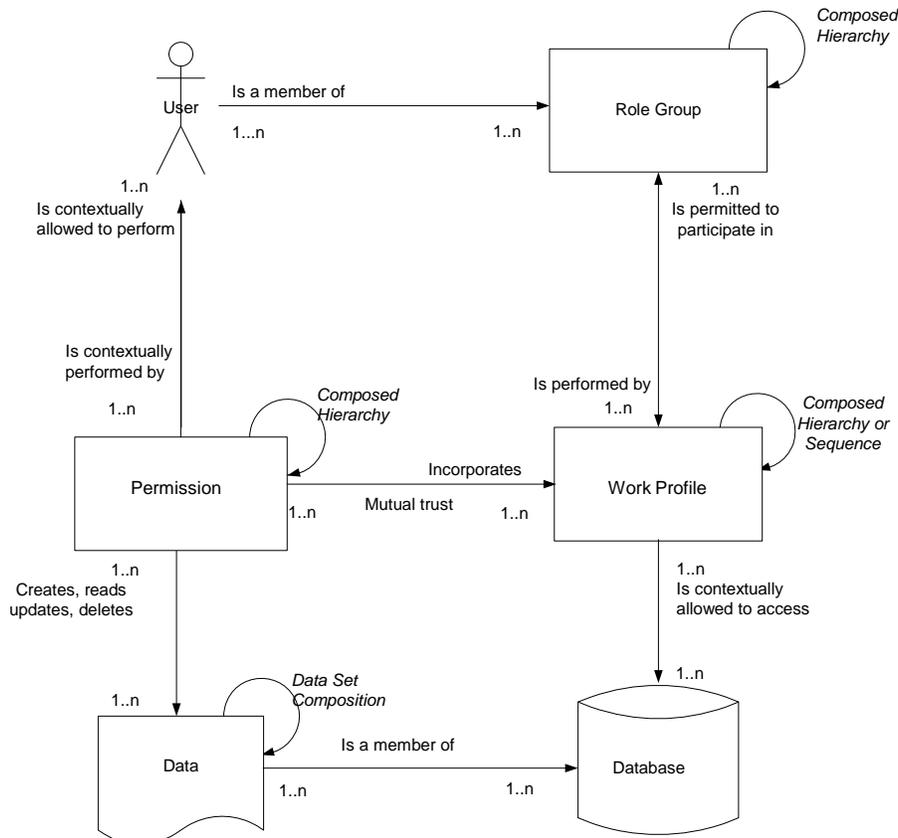


Figure 2: RBAC TF Role Engineering Model (Courtesy Siemens Medical Solutions)

Users are members of role groups permitted to participate in work profiles that contextually allow access to specific enterprise information objects/databases.. From the user point of view, he has been granted the permissions (according to the principle of least privilege) that allow performing operations (e.g., create, read, update, delete, and execute) on protected information objects associated with the work profile scenarios.

3 Interpretation

Figure 3 represents a portion of the Healthcare Scenario Roadmap. It consists of columns consisting of named healthcare persons and rows consisting of aggregate activities. The cells containing an 'x' identify which roles generally perform each activity. It is desired to use this model to identify and define scenarios used in the role engineering process.

Figure 3: Healthcare Scenario Roadmap Example

	Audiologist	Dental Hygienist/Registered Dental Hygienist (RDH)	Dentist (DDS or DMD)	Dietitian (RD)	Non-western Medicine Providers	Certified Acupuncturist (CA)	Licensed Massage Therapist (LMT)/Registered Massage	Nurse	Clinical Nurse Specialist (CNS)	Clinical Registered Nurse Anesthetist (CRNA)	Licensed Vocational Nurse (LVN)/Licensed Practical Nurs	Nurse Midwife (NM)	Nurse Practitioner (NP)	Registered Nurse (RN)
Legend:														
x = performs														
o = does not perform														
? = unknown														
Order Entry														
New/Change/Discontinue Laboratory Order	o	o	x	x	o	o	o		x	x	x	x	x	x
New/Change/Discontinue Radiology Order	o	o	x	x	o	o	o		x	x	x	x	x	x
New/Renew/Change/Discontinue/Refill Outpatient Rx Order	o	o	x	o	o	o	o		x	x	x	x	x	x
New/Change/Discontinue Inpatient Medication Order	o	o	x	o	o	o	o		x	x	x	x	x	x
New/Change/Discontinue Diet Order	o	o	x	x	o	o	o		x	x	x	x	x	x
New/Change/Discontinue Consult Order	x	o	x	x	o	o	o		x	x	x	x	x	x
New/Change/Discontinue Nursing Order	o	o	x	o	o	o	o		x	x	x	x	x	x
New/Change/Discontinue Standing Order(s) PRN	o	o	x	x	o	o	o		x	x	x	x	x	x
New/Change/Discontinue Verbal and Telephone Order	o	o	x	x	o	o	o		x	x	x	x	x	x
New/Change/Discontinue Supply Order (e.g. ostomy, diabetic)	o	o	x	x	o	o	o		x	x	x	x	x	x
New/Change/Discontinue Prosthetic Order (e.g. wheelchair, crutches)	o	o	x	x	o	o	o		x	x	x	x	x	x
Sign Order(s)	o	o	x	x	o	o	o		x	x	o	x	x	x

3.1 Roadmap Columns

The role engineering process has specified the existence of two distinct role types, basic and functional roles.

Basic roles, also called static roles, can be viewed as a precursor role that gives a person access to a "session" or "connection". Basic roles allow a user possessing that role to participate in a work profile. The RBAC TF has chosen to use ASTM 1986 Healthcare

Personnel that Warrant Differing Levels of Access Control as the definition of basic role names.

Interpretation: The entities placed in the columns of the roadmap are basic role names.

Functional roles reflect the essential business functions that need to be performed. They are closely related to Work Profiles in the Scenario model. Functional roles define what an actor can do once connected to a protected resource. The roadmap does not define functional roles, however, analysis of the roadmap-derived scenarios will lead to defined permissions that can be assigned to create functional roles.

3.2 Roadmap Rows

The aggregate activities in the rows of the Roadmap have been suggested by knowledgeable healthcare personnel possessing the basic roles listed in the columns of the roadmap. The elements in the rows reflect aggregate activities performed by the corresponding basic role. An “x” in the intersection means that the activity is performed; an “o” means that it is not.

Interpretation: The combination of all activities for which an “x” exists for a given basic role defines a work profile for that role.

3.3 Tasks and Scenarios

A task is work profile activity for (potentially) several actors consisting of one or more scenarios. Scenarios are composed of one or more steps that are performed by a single actor. A task with a single scenario is effectively collapsed into a scenario. Ultimately, work profiles comprise tasks that basic roles are allowed to participate in, while collections of permissions define functional roles. The HL7 Security TC is involved in defining standards for healthcare permissions, leaving it to individual enterprises to define for themselves which users or enterprise roles are to be granted which permissions.

The rows of the Roadmap that are highlighted contain defined activities and associated lists of subordinate activities. For example, the first activity is “Order Entry” with a list of specific subordinate activities involving different types of orders. The Order Entry activity also includes signature and co-signature activity. A description of Order Entry involving both signature and co-signature could potentially involve more than one actor. The Order Entry activity may, therefore, be modeled as least two scenarios, one involving activities on a specific order and signature and one involving the co-signature. Alternatively, the activity could be modeled as one scenario performed by one actor without a co-signature. Since Order Entry consists of one or more scenarios, then it is a task as defined in Figure 1. In particular, each highlighted row of the roadmap may be viewed in this manner as activities consisting of one or more scenarios.

Interpretation: The highlighted horizontal activities of the roadmap are tasks.

Note that if the subordinate activities can be described by a single scenario by a single actor, then the highlighted horizontal tasks collapse to a scenario and the subordinate activities become steps. Role engineering efforts focus on writing scenarios for defined roadmap tasks

Interpretation: The subordinate task activities represent, in part or as a whole, components of scenarios performed by a single actor.

Interpretation: The “x” activities of the roadmap represent “least” privilege” abstract permissions for the corresponding objects of the rows.

3.4 Object Levels

Permissions consist of actions on protected objects; however, objects may exist at different conceptual levels. To define permissions in a standard way, we must have some concept of what these conceptual levels are, and what level a specific group of permissions refers to.

For example, individual data elements could be viewed as a kind of fundamental component from which all others are created. Individual data elements would exist at the lowest and simplest conceptual level of our hierarchy. Collections of data elements may then be organized to define tables in a database. Database tables viewed as pure objects (ignoring their data element structure) define another hierarchical level a step more abstract than data elements. If we continue, then we can again abstract objects consisting of named aggregations of data elements and tables, forming yet another abstraction layer in an object hierarchy. As with database tables, named aggregations are treated as complete objects without reference to their internal aggregate data structure of tables and data elements.

If we extend in our imagination this object view to Figure 1, then the levels of the role-engineering process define a progressively more abstract description of a well defined object hierarchy. Furthermore, each of these levels may be associated with certain appropriate actions. These action-objects pairs become an associated permission defined at each level of the role-engineering hierarchy.

To illustrate this concept, at the highest level of Table 1 we see permissions defined by participation in a work profile. This particular association has previously been defined as a “Basic Role” in the role-engineering process.

We would like to define an appropriate level for HL7 defined “permissions”. This should not be too low or too high in the hierarchy. If permissions are defined too low, e.g., at the data element or table level, then we are effectively defining a universal healthcare schema

to which all organizations must comply. Considering that many such schemas have already been developed, it would be presumptuous to assert a new one that would be incompatible with everything currently in existence. If we go too high, then we are back to Basic roles. What is needed is a hierarchical level to which existing enterprise system implementations and data definitions can easily map. The lowest hierarchical level for which this appears practical is the “aggregate” level of Table 1. Since the aggregate describes a “conceptual” healthcare object or function (e.g., a prescription) without reference to its structural components, then system owners, architects, and vendors are all able to describe such objects concretely in reference to their own more proprietary objects. Since aggregates are viewed as the objects subordinate to steps of the role-engineering process, then they will also logically be defined by this process.

Accordingly, HL7 permissions can be clearly defined as operations on objects known as “aggregates” in a way that provides a clear mapping to objects that already exist in healthcare, at the lowest universally consistent level and consistent with the adopted role-engineering process.

Permission	
Action	Role Engineering Object
Participate	Work Profile
Execute	Task
Execute	Scenario
Perform	Step
Create, Read, Update, Delete ¹	Aggregation
Execute	Function
Create, Read, Update, Delete	Data Table
Create, Read, Update, Delete	Data Element

Table 1. Permissions as Action-Object Pairs at Different Levels of HL7’s Role-Engineering Hierarchy

Interpretation: The use of the Roadmap for HL7 functional role engineering is concerned with defining permissions for aggregations and functions.

4 Actions

The foregoing analysis suggests the following actions for the HL7 role-engineering process applied to adoption of the Healthcare Roadmap:

¹ Many healthcare organizations do not “delete” objects, instead adding a new object that replaces the older one. In this case “deleted” may be effectively implemented as “Addend”.

- Each highlighted activity of the roadmap must be described by corresponding scenarios.
- Subordinate activities which are simply different instances of more general activity need only be described once, if no other distinction is present.
- One or more scenarios must be written for each highlighted activity until all subordinate activities are accounted for.
- It is not required to write scenarios for each actor if the only result is duplications of abstract permissions. If unique permissions result, then a scenario would be necessary.
- Scenarios are defined by Steps. Scenarios must therefore have one or more Steps.
- Steps may be described as a series of actions. If the action is on a protected aggregations or functions, then the step defines an abstract permission. Abstract permissions are collected for the permission catalogue. No further decomposition of the aggregation is necessary.
- For consistency and standardization purposes, each aggregation must include an authoritative definition of the aggregation as part of the role engineering process. The definition may reference an existing standard or description in an accepted healthcare terminology from an authoritative source.
- An initial level of completeness of the roadmap consists of a review of ASTM E1986 Data Elements Warranting Differing Levels of Access Control. This list will be used to verify Roadmap completeness and to suggest additional abstract objects that should be included in the Roadmap.
- The HL7 EHR has defined a set of functions for healthcare organizations. These functions will also be harmonized with the scenarios of the role-engineering process and the Data Elements of ASTM E1986.