Role Based Access Control (RBAC)

Questionnaire from WG15 to other TC57 WGs

1. Introduction

The objective of this questionnaire is to collect input from other Working Groups pertaining to the RBAC requirements in their domain based on a common definition.

RBAC is an *Access Control* technology to restrict *resource* access to authorized users. In the following, users are called *subjects*. This addresses the fact that a *subject* may be a person or an automated agent. A *resource* may be a function or a set of data, e.g. a data model, control, file, program or device. *Permissions* to access a *resource* in order to perform certain operations are assigned to *roles*. A *role* defines a certain authority level within a system or organization. *Subjects* are assigned to particular *roles*. Based on this assignment, they are authorized to perform certain operations on the *resource* restricted by the *permissions*. The assignment does always apply in the context of a *session*.

Because of the fact that *subjects* are not assigned to *permissions* directly, administration is easier and less error-prone. The administration of a RBAC-based system comprises definition, change or revocation of appropriate *role*-assignments to *subjects.*

The subsequent bullets list the relationships between the entities of the RBAC-Model:

- A *subject* may have multiple *roles*.
- A *role* may have multiple *subjects*.
- A *role* may have multiple *permissions*.
- A *permission* may be assigned to multiple roles.

The following figure depicts the RBAC-Model in general:

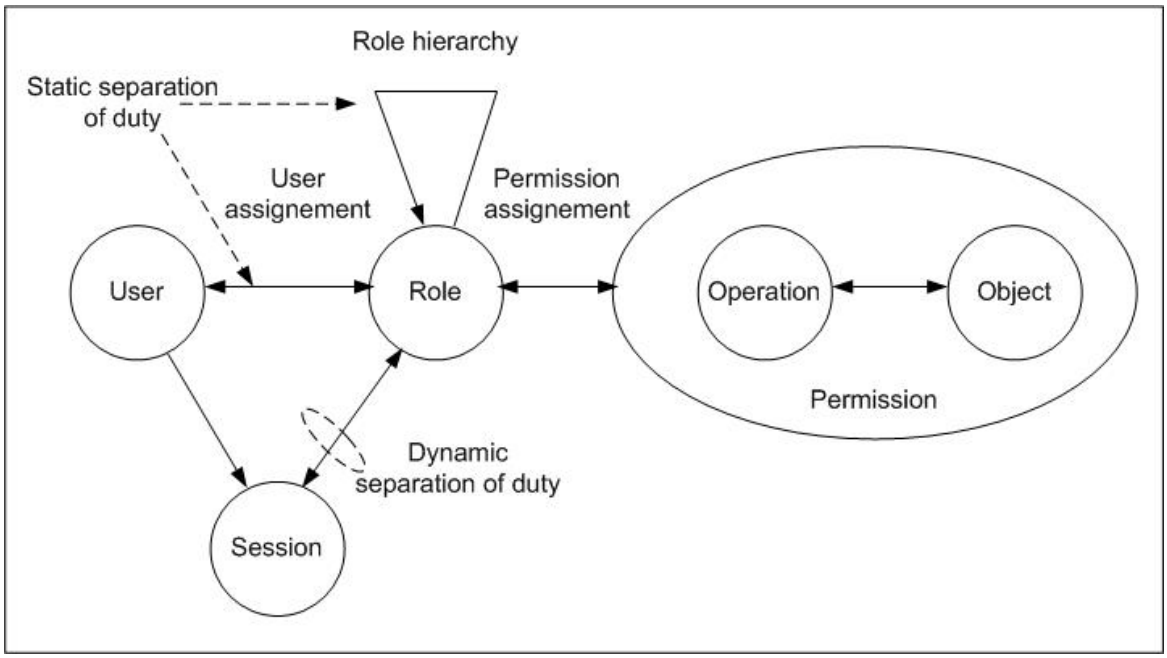

Figure 1: RBAC Model

Furthermore, RBAC is an approach to implement *Separation of Duties* within a system. Based on well-defined constraints, the assignment of specific *permissions* to opposing *roles* can be excluded. As an example, the same subject should not be permitted to administrate and review security-relevant functionalities on the resource.

2. Questions for IEC TC57 Working Groups

The following questions are listed in order to get feedback in relation to the above definitions.

1. What common roles are found in your environment? Please remember that people or automated agents can be assigned to such roles.
2. What is the smallest unit of resource for which permissions must be granted? Per data point? Per type of data? Per data record? Per database?
3. Are permissions granted on the basis of the class of resource, or individual instances of the class of resource?
4. What permissions must each role have? On which resources?
5. Are constraints (to exclude opposing rules) necessary to reflect your system / organizational policies?

Please create the table below for each resource to answer questions 1-4. Add or delete columns for permissions depending on the resource. Note that if many resources have the same roles and permissions; please group them together in the same table. The types of resources you define will determine the granularity of access control to your system. *Role_1* and *Role_2* are just examples that can be deleted.

Name of Resource: _____										
Role	Permissions									
	View	Read	Write	Execute	Configure	Create	Delete	Assign Permission	…	…
Role_1	*x*	*x*	*x*	*x*						
Role_2	*x*	*x*								

Please add further descriptions of RBAC definitions in your domain as well as general comments.

3. Procedure

WG15 would appreciate the convenors of WGs to provide this Questionnaire to their members and to request them to respond either through the convenor or directly (convenor's choice) to both:

- Maik Seewald at maik.seewald@siemens.com
- Frances Cleveland at fcleve@xanthus-consulting.com