Protection Profile Title: Role-Based Access Control Protection Profile

Protection Profile Version: 1.0 dated July 30, 1998

Criteria Version: Version 2.0 of the Common Criteria dated May 1998

Authors: Jim Reynolds of CygnaCom Solutions, Inc. and Ramaswamy Chandramouli of the National Institute of Standards and Testing

Role-Based Access Control (RBAC) Protection Profile

1 Introduction

1.1 Identification

1 Title: Role-Based Access Protection.

2 Registration: <to be filled in by registry>

3 Keywords: Access control, role-based access, non-discretionary controls, separation of duties, least privilege, information protection.

1.2 Protection Profile Overview

4 The security of a computer system depends on how well it is managed. System management involves many tedious tasks, which are often prone to error. The repetition of such tasks multiplies the probability of mistakes, any one of which can compromise security. In particular, the creation and deletion of users and their associated authorization data are onerous tasks. Any tool or system administration feature that would simplify or streamline these tasks would contribute greatly to strengthening assurance in a system's security. Such a tool or feature would reduce costs of operation as well.

5 At the same time, it is often the case that a user is granted more access to resources than is needed because of limited control over the type of access that can be associated with users and resources. Users may need to list directories and modify existing files, for example, without creating new files, or they may need to append records to a file without modifying existing records. Any increase in the flexibility of controlling access to resources within a computer system also strengthens the application of the least privilege principle, that users should only be granted the privileges needed for their jobs.

6 Role-based access control is intended to improve both aspects of system management: convenience and flexibility. More convenient management reduces the likelihood of mistakes of commission and omission in granting privileges to users, and greater access control flexibility reduces the need to grant too much access to too many users.

7 Role-based access control allows the system administrator to define roles based on job functions within an organization. The administrator assigns privileges to those roles, which may require finely grained operations to organization resources. Users are granted membership in the roles based on their job responsibilities. As the user's job responsibilities change, which may be frequent, user membership in roles can be

granted and revoked easily. As the organization inevitably changes, which generally is less frequent, roles can be modified easily through role hierarchies. Role hierarchies allow new roles to inherit most of their definition from existing roles. As the job changes, privileges are changed for the individual roles, which are relatively few, not for individual users, who may number in the hundreds or thousands.

8 Role-based access control can implement sophisticated security policies that are difficult to implement otherwise. For example, separation of duties can be implemented with role-based access control, where, for example, routine administrative functions can be limited to one role and more powerful administrative functions can be reserved for an entirely different role. This of course is impossible in systems where there is a pre-defined and immutable superuser, and anyone occasionally needing access to more privileges than granted to ordinary users must necessarily be granted the highest level of privileges. Separation of duties can be either automatically enforced or procedurally supported depending on the implementation. More advanced implementations would also provide for dynamic separation of duties, when membership in two exclusive roles would be allowed, but not their activation at the same time.

9 The Role-Based Access Control Protection Profile (PP) is meant to define a minimal set of requirements. More advanced functionality can be specified in the security target (ST). Meeting the requirements in this protection profile would significantly enhance the security of many operating systems, database management systems, systems management tools, and other applications.

10 The RBAC PP uses the Common Criteria (CC) requirement components to model ***role-based access control*** as described in the CS3 profile from the Federal Criteria (FC). Unlike the FC CS3 profile, the CC RBAC PP specifies a minimal set of security functions and assurances for general purpose multi-user operating systems, database management systems, systems management tools, and other applications in sensitive environments. The CC RBAC PP is intended for environments in which access to programs, transactions, and information can be restricted according to the assigned organizational role(s) of users for the purpose of convenient and flexible administration.

11 RBAC compliant products are expected to be used in sensitive commercial and governmental environments.

2 TOE description

12 RBAC defines a set of security requirements to be levied on Targets of Evaluation

(TOEs) which include general purpose operating systems, database management systems, systems management tools, and other applications.

13 Such TOEs implement the basic services, which permit IT applications to access and manage the computing hardware resources and interact with users and other applications in a controlled and protected manner. RBAC compliant TOEs permit multiple users to perform a variety of functions based on defined roles, which allow controlled, shared access to data and IT processes.

2.1 Operational Environment

14 RBAC is applicable to TOEs that provide facilities for on-line interaction with users. RBAC is also generally applicable to TOEs incorporating network functions, but this PP contains no network specific requirements. Networking is covered only to the extent to which it can be considered part of a centrally managed system that meets a common set of security requirements. However, this should not be interpreted to exclude complementary local control within a networked environment.

2.2 Required Security Functionality

15 RBAC assumes that the organization is the owner of all data. All data are centrally administered and are under the control of the TOE. The data are stored in named objects, and the TOE can associate with each object a finely grained description of the access rights to that object.

16 All individual users are assigned a unique user identifier. This user identifier supports individual accountability. The TOE authenticates the claimed identity of the user before allowing the user to perform any further actions.

17 An RBAC compliant TOE enforces controls such that access to the data objects and permitted actions with respect to them can only take place in accordance with the role-based access restrictions placed on that object by the authorized system administrator. The system administrator will associate each user with one or more roles which the TOE will use to make access decisions. Each role can be assigned to zero or more users. Authority to assume a role can only be granted and revoked by the system administrator. A set of operations is allocated to each role by the system administrator. Each operation includes an action or transformation procedure and a set of associated data items. A role is a set of non-discretionary associations of user - operations - data objects. Roles can be hierarchically defined. A role can include zero or more different roles. (See FDP_ACC.1, FDP_ACF.1, and FMT_SMR.2)

18 RBAC provides procedural support for the policy of separation of duties, in which roles may not conflict. No single individual should have to be authorized to perform all parts of a transaction represented by a set of operations against a set of data objects. This capability can be extended to system administrators in order to prevent a 'privileged user' or 'superuser' from having a wide set of privileges when only a subset is needed. This profile does not require automatic enforcement of separation of duties; this must be carefully managed by the administrator. It also does not support the dynamic separation of duties, when the activation of a role's privileges for a particular user is prevented by the user's other, already active roles.

19 An RBAC compliant TOE is assured to provide effective security measures only if it is installed, managed, and used correctly. The operational environment must be managed in a manner that supports the RBAC security objectives. In particular this includes allowing a determination that the evaluated TOE has been received without modification, that a secure state has been established during installation, and that the secure state is maintained during operation. In addition, roles must be defined and assigned to users in a way that correctly reflects security policies and requirements.

3 Security Environment

3.1 Summary

20 This section identifies the security issues that form the basis for choice of the RBAC security requirements. It identifies assumptions about the physical, personnel and other aspects of the environment of the TOE, the organizational security policies for which RBAC compliant TOEs are appropriate, and the threats to data security which the RBAC requirements are intended to counter.

3.2 Secure Usage Assumptions

21 An RBAC compliant TOE helps provide effective security measures only if it is installed, managed, and used correctly. The operational environment must be managed according to the RBAC assurance requirements documentation for delivery, operation, and user and administrator guidance.

22 The following specific conditions are assumed to exist in an RBAC environment:

3.2.1 Physical Assumptions

23 RBAC is intended for use in areas that have different levels of physical control and monitoring. It is assumed that the following physical conditions will exist:

A.ASSET It is also assumed that the value of the stored assets merits moderately intensive penetration or masquerading attacks. It is also assumed that physical controls in place would alert the system authorities to the physical presence of attackers within the controlled space.

A.LOCATE The processing resources of the TOE are located within controlled access facilities that will prevent unauthorized physical access.

A.PROTECT The TOE hardware and software critical to security policy enforcement will be physically protected from unauthorized modification by potentially hostile outsiders.

3.2.2 Personnel Assumptions

24 It is assumed that the following personnel conditions will exist:

A.ACCESS Rights for users to gain access and perform operations on information are based on their membership in one or more roles. These roles are granted to the users by the TOE Administrator. These roles accurately reflect the users job function, responsibilities, qualifications, and/or competencies within the enterprise.

A.MANAGE There will be one or more competent and trustworthy individuals assigned to manage TOE security. These individuals will have sole responsibility for the following functions: (a) create and maintain roles (b) establish and maintain relationships among roles (c) Assignment and Revocation of users to roles. In addition these individuals (as ‘owners of the entire corporate data’), along with object owners will have the ability to assign and revoke object access rights to roles.

A.OWNER A limited set of users is given the rights to “create new data objects” and they become owners for those data objects. The organization is the owner of the rest of the information under the control of TOE.

3.2.3 Connectivity Assumptions

25 RBAC contains no explicit network or distributed system requirements. However, the specification of resource access control is sufficiently flexible for a developer to define a policy for dealing with networks at the RBAC level.

26 It is assumed that the following connectivity conditions exist:

A.CONNECT All connections to peripheral devices reside within the controlled access facilities.

27 RBAC only addresses security concerns related to the manipulation of the TOE through its legitimate interfaces. Internal communication paths to interfaces points such as terminals are assumed to be adequately protected.

3.3 Organizational Security Policies

28 RBAC is capable of enforcing a broad class of organizational security policies that include:

specification of user capability to perform specific tasks;

user's access rights based on job responsibilities;

enforcement of least privilege for administrators and users;

specification and enforcement of conflicts-of-interest rules which may entail duty assignment and separation of duties; and

other access rights restriction governed by "need-to-know" principles

29 For commercial environments, RBAC compliant TOEs are considered suitable to protect information in situations in which access to and operations on that information need to be flexibly and conveniently controlled.

30 For government environments, RBAC compliant TOEs are considered suitable to protect sensitive-but-unclassified or single level classified information. RBAC compliant TOEs are not intended to protect multilevel classified information, as they are not specifically designed to control the flow of information between higher and lower levels of information sensitivity.

31 The organizational security policies discussed below are addressed by RBAC

compliant TOEs.

P.ACCESS Access rights to specific data objects are determined by the owner of the object, the role of the subject attempting access, and the implicit and explicit access rights to the object granted to the role by the object owner.

32 RBAC's ability to enforce user access to data objects makes it applicable to the class of organizational security policies generally described as 'need-to-know'.

3.4 Threats to Security

33 RBAC compliant TOEs are required to counter threats which may be broadly categorized as the threat of attack from hostile outsiders with no legitimate access to the system, and threats from insiders with legitimate access to the system attempting to gain access to and perform operations on information for which they have no individually defined rights. In addition, certain threats of a non-IT nature can affect the security of RBAC compliant TOEs and must be dealt with by the operating environment.

3.4.1 Threats Addressed by TOE

34 The threat possibilities discussed below are addressed by RBAC compliant TOEs.

T.ACCESS A user may gain access to resources or perform operations for which no access rights have been granted.

35 The term user is used to cover those who are granted some form of legitimate access to the system, but not necessarily to all data objects or possible operations on those objects.

36 It is assumed that such persons may possess a wide range of technical skills and, because they have some rights of access, are minimally trusted not to attempt to subvert the system or exploit the information stored thereon. However, in view of the need for separation of function inherent in the selection of RBAC, it is assumed that there is some potential for personal gain to users from attempts to perform operations on data for which they have no authority. Some users may also be motivated by curiosity to gain access to information for which they have no authority.

37 Two broad categories of users are identified with respect to this threat. The first category can be assumed to have limited technical skills and only be accessing the system through application level facilities. The second category can be assumed to be granted access to programming facilities (through published APIs) with the appropriate technical skills and hence may have access to more TOE functions.

T.ENTRY An unauthorized person may gain logical access to the TOE.

38 The term unauthorized person is used to cover all those persons who have, or may attempt to gain, physical access to the system and its terminals but have no authority to gain logical access to the system or perform operations on its information.

3.4.2 Threats To Be Addressed By The Operating Environment

39 The threat possibilities discussed below must be countered in order to support the RBAC security capabilities but are not addressed by RBAC compliant TOEs. Such threats must be addressed by the operating environment.

T.OPERATE Compromise of the IT assets may occur because of improper administration and operation of the TOE.

40 The security offered by RBAC can be assured only to the extent that the TOE is operated correctly by system administrators and users.

41 Users or external threat agents may, through accidental discovery or directed search, discover inadequacies in the security administration of the TOE which permit them to gain logical access to and perform operations on its resources in breach of any permissions they may have.

42 Potential attackers may seek to develop methods whereby the improperly administered security functions of the TOE may be circumvented during normal operation.

T.ROLEDEV The development and assignment of user roles may be done in a manner that undermines security.

43 In general, roles could be developed which have an incorrect or improper combination of authorizations to perform operations on objects. In addition, users could be

assigned to roles that are incommensurate with their duties, giving them either too much or too little scope of authorization.

44 A particular concern arises in that users could be assigned conflicting roles with respect to ‘separation of duties’. An individual user could be authorized to perform multiple operations on data objects that represent the parts of a transaction that should be separated among different individuals.

4 Security Objectives

4.1 Security Objectives for the TOE

45 The following are the RBAC TOE IT security objectives:

O.ACCOUNT The TOE must ensure that all users can be held accountable for their security relevant actions.

O.ADMIN The TOE must provide functions to enable an authorized administrator to effectively manage the TOE and its security functions, ensuring that only authorized administrators can access such functionality.

O.AUDIT The TOE must provide the means of recording security relevant events in sufficient detail to help an administrator of the TOE detect attempted security violations or potential misconfiguration of the TOE security features that would leave the IT assets open to compromise.

O.DUTY The TOE must provide the capability of enforcing ‘separation of duties’, so that no single user has to be granted the right to perform all operations on important information.

46 RBAC is capable of enforcing separation of duties through roles that restrict users to a subset of operations on specific data objects.

O.ENTRY The TOE must prevent logical entry to it by persons or processes with no rights to access it.

O.HIERARCHICAL The TOE must allow hierarchical definitions of roles. Hierarchical definition of roles means the ability to define roles in terms of other roles. This saves time and allows for more convenient administration of the TOE.

O.KNOWN Legitimate users of the system must be identified before rights of access can be granted.

47 RBAC assumes that there is a finite community of known users who will be granted rights of access and that system management has authority over that user community.

O.ROLE The TOE must prevent users from gaining access to and performing operations on its resources/objects unless they have been granted access by the resource/object owner or they have been assigned to a role (by an authorized administrator) which permits those operations.

4.2 Security Objectives for the Environment

48 The RBAC TOE is assumed complete and self-contained and, as such, is not dependent upon any other products to perform properly. However, certain objectives with respect to the general operating environment must be met in order to support the RBAC security capabilities.

49 The following are the RBAC non-IT security objectives:

O.CONNECT Those responsible for the TOE must ensure that no connections to outside systems or users undermine the security of IT assets.

O.INSTALL Those responsible for the TOE must ensure that it is delivered, installed, configured, administered, and operated in a manner which maintains IT security. This includes the definition and assignment of roles.

O.PHYSICAL Those responsible for the TOE must ensure that that those parts of the TOE that are critical to the security policy are protected from physical attack.

5 TOE IT Security Requirements

50 This section contains functional and assurance requirements that must be satisfied by an RBAC compliant TOE. These requirements consist of functional components from Part 2 of the CC and an augmented Evaluation Assurance Level (EAL) containing assurance components from Part 3.

5.1 Functional Requirements

51 Table 5.1 below summarizes the RBAC functional requirements as expressed in CC Part 2 (Version 2.0 Draft) components. Following the table, details of each required functional component are provided, including the elements and the operations performed on them to meet specific needs of RBAC. Where reference is made to the 'RBAC ST', this is intended to mean an ST for a TOE that is compliant with the RBAC PP.

Table 5.1 - RBAC Functional Requirements

Component	Name
FAU_GEN.1	Audit Data Generation
FAU_GEN.2	User Identity Generation
FAU_SAR.1	Security Audit Review
FAU_SAR.2	Restricted Audit Review
FAU_SAR.3	Selectable Audit Review
FAU_SEL.1	Selective Audit
FAU_STG.1	Permanent Audit Storage
FDP_ACC.1	Subset Access Control
FDP_ACF.1	Security Attribute Based Access Control
FIA_ATD.1	User Attribute Definition
FIA_UAU.2	User Authentication before any action
FIA_UID.2	User Identification before any action
FIA_USB.1	User-Subject Binding
FMT_MSA.1	Management of Security Attributes
FMT_MSA.2	Secure Security Attributes
FMT_MSA.3	Static Attribute Initialization
FMT_MTD.1	Management of TSF Data
FMT_MTD.3	Secure TSF Data
FMT_REV.1	Revocation
FMT_SMR.2	Security Roles
FPT_AMT.1	Abstract Machine Testing
FPT_FLS.1	Failure with preservation of Secure State
FPT_RCV.1	Manual Recovery

FPT_RCV.4	Function Recovery
FPT_RVM.1	Non-bypassability of the TSP
FPT_SEP.1	TSF Domain Separation
FPT_STM.1	Reliable Time Stamps
FPT_TST.1	TSF Self Test
FTA_LSA.1	Limitation on Scope of Selectable Attributes
FTA_TSE.1	TOE Session Establishment

5.1.1 Security Audit Requirements

FAU_GEN.1 Audit Data Generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

(a) Start-up and Shutdown of the audit functions;
(b) All auditable events for the *basic* level of audit; and
(c) (i) *Assignment of Users, Roles and Privileges to Roles*
(ii) *Deletion of Users, Roles and Privileges from Roles*
(iii) *Creation and Deletion of Roles*

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

(a) Date and Time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
(b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST the following information:
(i) *For each invocation of a* security function, *the RBAC Administrator role that made invocation of that* security function *possible.*
(ii) *For each access control action on the user data, the role that made possible the invocation of that action.*

FAU_GEN.2 User Identity Generation

FAU_GEN.2.1 The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

FAU_SAR.1 Security Audit Review

FAU_SAR.1.1 The TSF shall provide the *set of authorized RBAC administrators* with the capability to read the following audit information from the audit records:

(a) Date and Time of Audit Event
(b) The UserID responsible for the Event and optionally the role membership which enabled the

user to perform the event successfully
(c) The access control operation and the object on which it was performed.
(d) The outcome of the event (success or failure)
(e) *The User Session Identifier or Terminal Type*

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

FAU_SAR.2 Restricted Audit Review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

FAU_SAR.3 Selectable Audit Review

FAU_SAR.3.1 The TSF shall provide the ability to perform *searches, sorting and ordering* of audit data based on the following criteria:

(a) Date and Time of Audit event
(b) UserID
(c) Object Name & type of access
(d) Role that enabled the access
(e) *Any combination of the above items (a), (b), (c) or (d).*

FAU_SEL.1 Selective Audit

FAU_SEL.1.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:

(a) *Object identity, user identity, subject identity, host identity, and event type*
(b) *Users belonging to a specified Role and Access types (e.g. delete, insert) on a particular object*

FAU_STG.1 Permanent Audit Trail Storage

FAU_STG.1.1 The TSF shall protect the stored audit records from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to *prevent* modifications to the audit records.

5.1.2 User Data Protection

FDP_ACC.1 Subset Access Control

FDP_ACC.1.1 The TSF shall enforce the *Role-based Access Control (RBAC) SFP* on:

(a) *Subjects (specified in the RBAC ST) covered by RBAC SFP*
(b) *Objects (specified in the RBAC ST) covered by RBAC SFP*

(c) *All Operations on Objects (specified in RBAC ST) covered by RBAC SFP*

FDP_ACF.1 Security Attribute Based Access Control

FDP_ACF.1.1 The TSF shall enforce the *RBAC SFP* to objects based on the following *user attributes*:

(a) *User Identity*
(b) *Authorized Roles for the User (refer to Glossary for definition)*

The TSF shall enforce the *RBAC SFP* to objects based on the following *subject attributes*:

(a) *Subject Identity*
(b) *Role(s) which can invoke the subject*

The TSF shall enforce the *RBAC SFP* to objects based on the following *object attributes*:

(a) *Object Identity*
(b) *Operations permitted on the objects for various Roles*

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if any operation among controlled subjects and controlled objects is allowed: *The subject invoking the operation on an object is assigned to a role whose privilege set includes the operation on the object.*

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *Allow an access operation by a subject on an object only if the user associated with the subject belongs to a role that permits the access operation on the object.*

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the *user associated with the subject not belonging to any role that permits the requested access operation on the object*

5.1.3 Identification and Authentication Requirements

FIA_ATD.1 User Attribute Definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

(a) *List of Authorized Roles*
(b) *Any other user attributes related to Roles, as defined in the RBAC ST.*

FIA_UAU.2 User Authentication before any action

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any

other TSF-mediated actions on behalf of that user.

FIA_UID.2 User Identification before any action

FIA_UID.2.1 The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

FIA_USB.1 User-Subject Binding

FIA_USB.1.1 The TSF shall associate the appropriate user security attributes with subjects acting on behalf of the user.

5.1.4 Security Management

FMT_MSA.1 Management of Security Attributes

FMT_MSA.1.1 The TSF shall enforce the *RBAC SFP* to restrict the ability to [*modify, delete, create* i*nstances*] of the *following user* security attribute to *a set of RBAC Administrative Roles*:

(a) *User Role Authorizations*

FMT_MSA.1.1 The TSF shall enforce the *RBAC SFP* to restrict the ability to [*create, modify the composition]* of the *following user* security attribute to *a set of RBAC Administrative Roles*:

(a) *Default Active Role Set (refer to Glossary for definition)*

FMT_MSA.1.1 The TSF shall enforce the RBAC SFP to restrict the ability to [*modify the composition*] of the *following session* security attribute to *session owner*:

(a) *Active Role set for a user (refer to Glossary for definition)*

FMT_MSA.1.1 The TSF shall enforce the *RBAC SFP* to restrict the ability to [*modify]* the *object* security attributes to (i) *Object Owners* and (ii) *set of RBAC administrative roles.*

FMT_MSA.2 Secure Security Attributes

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes.

FMT_MSA.3 Static Attribute Initialization

FMT_MSA.3.1 The TSF shall enforce the *RBAC SFP* to provide [selection: property to be specified in RBAC ST]] default values for object security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the *following* roles to specify alternative initial values to override the default values when an object or information is created:

(a) *Set of RBAC Administrative Roles*

FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to [*modify, create]* the *following list of TSF Data* to a *set of RBAC Administrative Roles*:

(a) *All User Passwords*
(b) *Role Definitions & Role Attributes*
(c) *Role Hierarchies (by assigning one or more roles to other roles)*
(d) *Constraints among Role Relationships*
(e) *List of Auditable Events*

FMT_MTD.3 Secure TSF Data

FMT_MTD.3.1 The TSF shall ensure that only secure values are accepted for TSF data.

FMT_REV.1 Revocation

FMT_REV.1.1 The TSF shall restrict the ability to revoke security attributes associated with the *users* within the TSC to a *set of RBAC Administrative Roles*.

The TSF shall restrict the ability to revoke security attributes associated with the *objects* within the TSC to *the following*:

(a) *Object Owners and*
(b) *A set of RBAC Administrative Roles*

FMT_REV.1.2 The TSF shall enforce the rules *described by the following*:

(a) *User Security Attributes: Revocation will take place on the next login of the user*
(b) *Object Security Attributes: Revocation will take place on the next attempt to access the object.*

FMT_SMR.2 Security Roles

FMT_SMR.2 Restrictions on Security Roles

FMT_SMR.2.1 The TSF shall maintain the *following* roles:

(a) *Set of RBAC administrative roles (the exact roles in this set are specified in the RBAC ST).*
(b) *Roles for Object Owners*

FMT_SMR.2.2 The TSF shall be able to associate users with roles.

FMT_SMR.2.3 The TSF shall ensure that the *following conditions* for (a) *Roles of Object Owners* and (b) the *set of RBAC administrative roles* are satisfied:

(a) *Object Owners can modify security attributes for only the objects they own*
(b) *The set of RBAC administrative roles can modify security attributes for all objects under the control of TOE (since they automatically inherit the privileges of all Object Owners).*

5.1.5 Protection of TOE Security Functions

FPT_AMT.1 Abstract Machine Testing

FPT_AMT.1.1 The TSF shall run a suite of tests [*periodically during normal operation and at the request of an authorised use*r] to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.

FPT_FLS.1 Failure with preservation of Secure State

FPT_FLS.1.1 The TSF shall preserve a secure state *when the following failures* occur:

(a) The entire RBAC database containing data on Privileges assigned to a role, Users authorized for a role, Role constraints and relationships or some specific tables containing subsets of these data are off-line, corrupt or inaccessible.

FPT_RCV.1 Manual Recovery

FPT_RCV.1.1 After a failure or service discontinuity, the TSF shall enter a maintenance mode where the ability to return the TOE to a secure state is provided.

FPT_RCV.4 Function Recovery

FPT_RCV.4.1 The TSF shall ensure that *the following SFs and failure scenarios* have the property that the SF either completes successfully, or for the indicated failure scenarios, recovers to a consistent and secure state:

(a) *The SF that checks whether a specified privilege is assigned to any role but the database containing the privilege data is not on-line or the particular data table is inaccessible.*
(b) *The SF that checks whether a specified role has been assigned to a particular user but the database containing the role membership information is not on-line or the particular data table is inaccessible.*
(c) *[Any other function implemented in the Security Target for checking Role Memberships or Privilege Assignments]*

FPT_RVM.1 Non-bypassability of the TSP

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before

each function within the TSC is allowed to proceed.

FPT_SEP.1 TSF Domain Separation

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

FPT_STM.1 Reliable Time Stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

FPT_TST.1 TSF Self Test

FPT_TST.1.1 The TSF shall run a suite of self tests [*periodically during normal operation, at the request of the authorised user, and when invocation of access rights on selected objects occurs]* to demonstrate the correct operation of the TSF.

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of TSF data.

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.

5.1.6 TOE Access

FTA_LSA.1 Limitation on Scope of Selectable Attributes

FTA_LSA.1.1 The TSF shall restrict the scope of the session security attributes (*Active Role Set for the User*) based on *the set of Authorized Roles for the User*.

FTA_TSE.1 TOE Session Establishment

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on *the default active role set for the user being empty*.

5.2 Strength of Function Requirement

52 The minimum strength of function level for the TOE security functional requirements is SOF-basic.

5.3 Assurance Requirements

52 The assurance requirements for RBAC are portrayed in Table 3.2 below. The

assurance augmentation components are described following the table.

Table 5.2 - RBAC assurance requirements

Requirement	Name
EAL2	Structurally Tested
ADV_SPM.1	Informal TOE Security Policy Model

ADV_SPM.1 Informal TOE security policy model

Dependencies:

ADV_FSP.1 Informal functional specification

Developer action elements:

ADV_SPM.1.1D The developer shall provide a TSP model.

ADV_SPM.1.2D The developer shall demonstrate correspondence between the functional specification and the TSP model.

Content and presentation of evidence elements:

ADV_SPM.1.1C The TSP model shall be informal.

ADV_SPM.1.2C The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modeled.

ADV_SPM.1.3C The TSP model shall include a rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP that can be modeled.

ADV_SPM.1.4C The demonstration of correspondence between the TSP model and the functional specification shall show that all of the security functions in the functional specification are consistent and complete with respect to the TSP model.

Evaluator action elements:

ADV_SPM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6 Environmental IT Security Requirements

52 RBAC is primarily applicable to TOEs which are fully responsible for enforcement of the TOE Security Policy (TSP) and do not, therefore, require that the IT environment of the TOE accept any TSP enforcement responsibility.

53 Application of RBAC to a TOE that requires some of the RBAC IT security requirements to be met by the TOE IT environment is permissible. Should this be the case, the Security Target must explain the partition of security requirements between the TOE and its IT environment and demonstrate that the TOE in its IT environment satisfies all of the RBAC security requirements.

GLOSSARY OF TERMS

Authorized Roles for the User: This is the set of roles directly assigned to the user by the RBAC Administrator together with the set of roles contained in those roles (due to role to role assignments)

Active Role Set (ARS): This is the subset of the set of authorized roles for a user that has actually been activated for the user in a particular user session. The total set of access rights (privileges) available to a user in a session is the sum of the access rights directly assigned to each member of ARS together with the privileges inherited by each member of ARS through roles assigned to it.

Default Active Role Set (DARS): Instead of forcing the user to build an Active Role Set (ARS) during every user session, the RBAC administrator provides a default set of roles (from the list of authorized roles for the user). The composition of DARS determines the initial available access rights for the user at the start of the session. In other words, DARS is the ARS at the time of session creation. In many software environment the user may be able to change the composition of this initial ARS (i.e. DARS) during the course of the user session.

Object Owner: In many software environments, the user who creates a data object becomes the object owner by default. In some environments, the object owner can be changed by the system administrator. The object owner has generally all access rights on the object and in some environments the power to grant access rights on the objects he/she owns to roles and other users.

Privilege Set for a Role: The total set of access rights on various objects granted to a role.