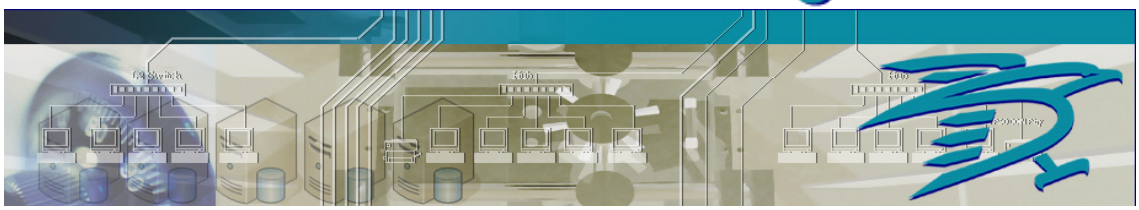

# Eaglehawk
# SBX Enigma™
# EAL 2+ Common Criteria Evaluation
# Security Target

BAE SYSTEMS

Prepared By: BAE Systems Australia Datagate Pty Ltd
3 Second Avenue
Technology Park
MAWSON LAKES SA 5095

Approved By: _____ Date: _____
Chris Walsh
Chief Information Security Officer

# Contents

**1 ST Introduction ..... 7**
1.1 ST Reference ..... 7
1.2 TOE Reference ..... 7
1.3 TOE Overview ..... 7
1.3.1 Usage and major security features of the TOE ..... 8
1.3.2 TOE Type ..... 10
1.3.3 Required non-TOE hardware/software/firmware ..... 10
1.4 TOE Description ..... 10
1.4.1 SBX Enigma™ Concept ..... 10
1.4.2 SBX Enigma™ physical scope ..... 11
1.4.3 SBX Enigma™ logical scope ..... 11
1.4.4 SBX Enigma™ Fine-Grained Access Control ..... 13
1.4.5 SBX Enigma™ Role-Based User Structure ..... 14
1.4.6 SBX Enigma™ Access Procedures ..... 18
1.4.7 SBX Enigma™ Audit Functions ..... 21

**2 Conformance Claim ..... 23**
2.1 CC Conformance Claim ..... 23
2.2 PP Claim ..... 23
2.3 Conformance Rationale ..... 23

**3 Security Problem Definition ..... 25**
3.1 Introduction ..... 25
3.2 Threats ..... 25
3.3 Organizational Security Policies ..... 26
3.4 Assumptions ..... 26

**4 Security Objectives ..... 27**
4.1 Security Objectives for the TOE ..... 27
4.2 Security Objectives for the Operational Environment ..... 27
4.3 Security Objectives Rationale ..... 28
4.3.1 Tracing between security objectives and the security problem definition ..... 28
4.3.2 Providing a justification for the trace ..... 29
4.4 Security objectives: conclusion ..... 31

**5 Extended Components Definition ..... 33**

**6 Security Requirements ..... 35**
6.1 Security functional requirements ..... 35
6.1.1 Security Audit (FAU) ..... 36

6.1.2 Cryptographic support (FCS) ..... 38
6.1.3 User data protection (FDP) ..... 38
6.1.4 Identification and authentication (FIA) ..... 42
6.1.5 Security management (FMT) ..... 43
6.1.6 TOE Access (FTA) ..... 49
6.1.7 Dependencies ..... 49
6.1.8 SFR security requirement rationale ..... 50
6.2 Security assurance requirements ..... 53
6.2.1 SAR security requirements rationale ..... 54
6.3 Security requirements: conclusion ..... 55

**7 TOE Summary Specification ..... 56**
7.1 Identification and Authentication Functionality ..... 56
7.2 Role-base Management Functionality ..... 56
7.3 Access Control Functionality ..... 57
7.4 Secure Data Storage Functionality ..... 58
7.5 Security Audit Functionality ..... 58

## List of Figures

Figure 1 – SBX Enigma™ Object Store ..... 11
Figure 2 – SBX Enigma™ Architecture ..... 12
Figure 3 – SBX Enigma™ Access Control ..... 14
Figure 4 – SBX Enigma™ Roles and Functions ..... 16
Figure 5 – ACLs on Metadata Objects ..... 19
Figure 6 – ACLs on Data Element Objects ..... 20
Figure 7 – Relations between the security problem definition, the security objectives and the security requirements ..... 55

## List of Tables

Table 1 – Enterprise-Level Components ..... 13
Table 2 – Organization-Level Components ..... 13
Table 3 – Enterprise-Level User Structure ..... 15
Table 4 – Organization-Level User Structure ..... 17
Table 5 – Threat to the TOE ..... 25
Table 6 – Organizational Security Policies ..... 26
Table 7 – Applicable Assumptions ..... 26

Table 8 – Security objective for the TOE ..... 27
Table 9 – Security objective for the operational environment ..... 28
Table 10 – Security objective rationale ..... 29
Table 11 – Security Functional Requirements ..... 36
Table 12 – Auditable events ..... 38
Table 13 – SFR direct dependencies ..... 50
Table 14 – Tracing between SFRs and the security objectives ..... 51
Table 15 – Assurance Requirements ..... 54

**This page intentionally left blank.**

# 1 ST Introduction

This chapter covers the Security Target (ST) Reference, TOE Reference, TOE Overview and TOE Description.

## 1.1 ST Reference

Title: Eaglehawk SBX Enigma™ EAL2+ Common Criteria Evaluation Security Target;

ST documentation number: TDG6014-ASE-001;

ST version: 1.5

ST date of publication: 5 February 2009;

## 1.2 TOE Reference

Target of Evaluation (TOE): Eaglehawk SBX Enigma™

TOE part number: SBX.E2

TOE Version: 4.2.4.

## 1.3 TOE Overview

SBX Enigma™ is server-based data security software that provides a virtual Lockbox designed to protect an organization's most valuable information assets. SBX grants System Architects complete discretion and control over what information gets protected and who can access it, thereby providing exceptional latitude in developing custom data security solutions. Core SBX Enigma™ functions include identification and authentication, role based management, access control, secure data storage and comprehensive security audit capabilities, instantly available to support Client Applications through the SBX Application Program Interface (API).

Regardless of data type or location, SBX Enigma™ enables an organization to protect essentially any of its information assets, ranging from Enterprise applications, to Service-Oriented Architecture (SOA) services, to discrete data components such as encryption keys or Personally Identifiable Information (PII). SBX functions are highly configurable and enable an organization to address its specific data security requirements in a manner best suited to its unique environment. SBX Enigma™ readily integrates with and strengthens existing applications and security frameworks, and provides a direct path to address such issues as securely sharing information between organizations and need-to-know protection of high-value data.

SBX Enigma™ is a highly scalable, in-memory, object-oriented data management system that includes advanced security features related to role-based user administration, metadata and data functions, element-level access control based on least privilege, and centralized audit.

### 1.3.1 Usage and major security features of the TOE

Within a typical Enterprise data environment there generally are a multitude of dynamic components: numerous Client Applications serving a range of internal and external Organizations, each of which services large User/User Group populations, with everything operating from multiple geographic locations.

As an Enterprise attempts to leverage the value of its data assets by sharing these multifaceted resources across the entire scope of its operations, e.g., through adoption of dynamic approaches such as a SOA, difficult data security issues arise that require comprehensive, flexible Enterprise-wide solutions. IT security, which traditionally focuses on each discrete legacy resource and its defined set of users, must evolve to support Enterprise-level services which, by definition, package previously autonomous components and cut across established resource and user boundaries.

Responding to both traditional and emerging Enterprise data security challenges, SBX provides functionality in the following areas:

**Identification and Authentication**

SBX augments existing ID Management systems with an additional, Enterprise-wide layer of security which is invoked when users seek access to protected data resources through supported Client Applications & SOA Services.

Authentication is based on presentation of valid user credentials. Valid credentials (User ID and Password/Passphrase) are established by all users through secure SBX procedures.

**Role-Based Management**

Successful authentication of an SBX Administrative User results in Role-Based authorization to access a strictly defined (and limited) sub-set of system functions, e.g., Enterprise Metadata Administrators gain access to Enterprise Metadata Maintenance functions, Organization User Managers gain access to Organization User Maintenance functions.

The SBX Role-Based Administrative Framework is specifically designed to minimize security risks associated with internal abuse by separating and distributing access to key functions. In this regard, access privileges are constrained by an administrative user's Role which, in turn, is functionally separated from other administrative Roles by the following categories:

- System Administration
- Organization Administration
- Metadata Administration
- User Administration
- Data Administration
- Audit Administration

Successful authentication of a non-administrative Limited User results in User Group-Based authorization to access specifically permitted Metadata Objects and Data Element Objects secured by SBX. User Groups are mainly composed of non-administrative Limited Users.

Each discrete Metadata or Data Element Object has an associated Access Control List (ACL) Object specifying the User Group(s) with access privileges. Membership in such an authorized User Group is required for a Limited User to be granted access to the Object.

**Access Control**

In response to query calls it receives, SBX provides Client Applications & SOA Services with Fine-Grained Access Control over data resources across the Enterprise.

Metadata Object Access Control: Within the context of an Enterprise data architecture SBX Metadata can be viewed as a blueprint that describes the underlying Enterprise data assets and how they are organised. The Metadata blueprint may describe all Enterprise data assets, their types, locations, and storage methods, thereby providing a description of the aggregate Enterprise data architecture.

By incorporating ACLs for all components of the Enterprise data architecture into the Metadata blueprint, SBX supports access management and control across that architecture down to the level of individual components. SBX responds to Application/Service queries regarding user access permissions to Metadata Objects as follows:

Querying through the SBX API, the Application/Service requests SBX to provide the user's access authority to the sought-after Metadata Objects.

Responding through the API, SBX confirms or denies the user's authority to access, first, the data structure (e.g., the database) and, second, specific components (e.g., database tables and fields) within that structure.

Data Element Object Access Control: SBX provides designers of Client Applications & SOA Services with the ability to store high-value data elements (e.g., Personally Identifiable Information, encryption keys) from their typical location in database tables and safeguard them as discrete Data Element Objects in SBX. Subsequent access to these high-value data elements is authorized or denied based on the discrete Access Control List of each such Data Element Object.

SBX responds to Application/Service queries via the SBX API regarding user access permissions to Data Element Objects secured within SBX by confirming or denying user authority to access these specified Data Element Objects – i.e., need-to-know authority.

Using this approach, SBX can be utilized to manage and authorize access to almost any named Enterprise data asset. Examples include:

Confirm/deny user authority to access a specified Client Application or SOA Service.

Confirm/deny user authority to access other Enterprise resources – e.g., servers, data centres.

Confirm/deny user authority to access storage elements and components – e.g., folders, files.

**Secure Data Storage**

The Data Element Objects are encrypted in accordance with the Advanced Encryption Standard with a 256 bit cryptographic key.

**Security Audit**

SBX simplifies audit procedures through standardization of Enterprise-wide audit processes available to all Enterprise Client Applications & SOA Services, thus providing for real-time identification and monitoring of Enterprise-wide resource usage through:

- Comprehensive, mandatory audit of administrative activities.
- Flexible, optional audit of SBX interactions with Client Applications and SOA Services.
- Generic, as-required audit of any independent Client Application/Service event.

### 1.3.2 TOE Type

SBX Enigma™ is an object-oriented data management system providing access control and secure data management services.

### 1.3.3 Required non-TOE hardware/software/firmware

The TOE consists of the components provided with Eaglehawk SBX Enigma™ (SBX). The following Operating System (OS) and Virtual Machine software underlay the TOE, but are outside the scope of this evaluation:

- Computing Platform Hardware
- BIOS firmware
- Microsoft Windows Server 2003
- Microsoft SQL Server
- Apache Tomcat 5.x
- Eaglehawk FalconVS virtual machine
- Eaglehawk Remote thin-client

## 1.4 TOE Description

### 1.4.1 SBX Enigma™ Concept

The basic concept of SBX Enigma™ is an in-memory data management system. An SBX object store contains all classes, users, metadata, data elements and other persistent objects in an in-memory repository. In order for users to access SBX, it must be executing within an instance of the Eaglehawk FalconVS virtual machine. SBX persistent objects are periodically written to disk storage by FalconVS for backup and recovery purposes.

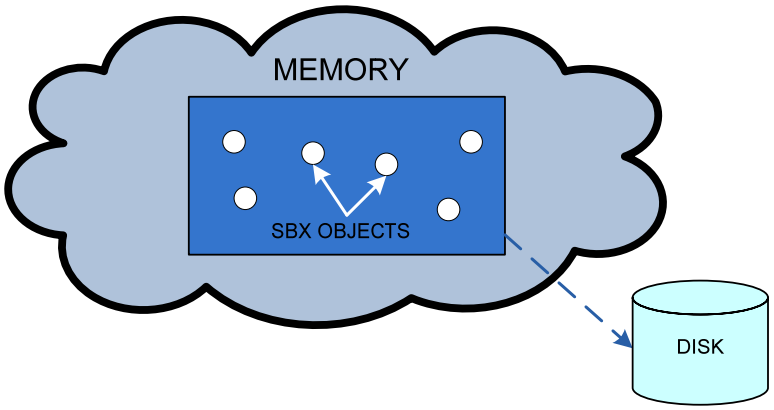


Figure 1 – SBX Enigma™ Object Store

### 1.4.2 SBX Enigma™ physical scope

The SBX Enigma™ TOE physical scope consists of the SBX Enigma™ Server application and the Client API providing the remote web-based access. The system is scalable and can support multiple clients and multiple enterprises.

### 1.4.3 SBX Enigma™ logical scope

SBX Enigma™ provides a scalable framework for an enterprise information system. Under the root Enterprise-level Organization, multiple sub-Organizations can be established. These Organizations serve as discrete units comprised of macro-populations of Users, e.g., a company, agency, division, or department. All non-Enterprise Administrative Users belong to a single Organization.

Each Organization has its own discrete administrative and management structure concerned with the following functions:

- Creation, maintenance, and removal of Users and User Groups
- Recovery of deleted Data Element Objects
- Selection and audit of Client Applications used by the Organization
- Assignment or removal of access rights to Metadata and Data Element Objects

Figure 2 shows the conceptual elements of SBX Enigma™ that comprise Enterprise-Level (i.e., system) components and Organization-Level components associated with each discrete organization established within the enterprise. Table 1 describes the Enterprise-Level Components listed in Figure 2 while Table 2 describes the Organizational-Level components.

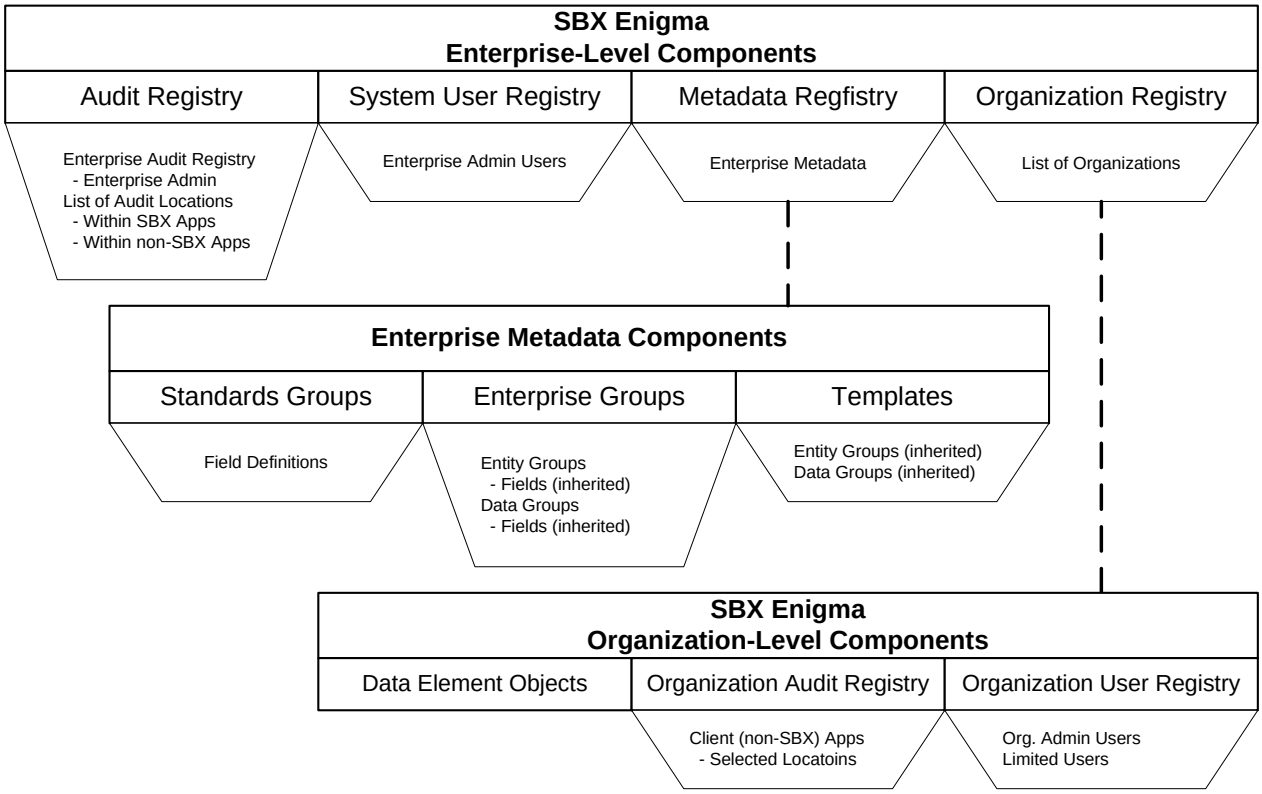


Figure 2 – SBX Enigma™ Architecture

| ***Enterprise-Level Components*** | |
|---|---|
| **Audit Registry** | Mandatory audit of all SBX applications and all activity by Enterprise administrative users. |
| **Audit Location List** | All SBX and non-SBX (Client) applications/services are registered, and audit locations (static location within program code) within each application/service can be specified. Audit of all SBX applications is automatic & mandatory. Audit of all non-SBX applications/services at specified audit locations is discretionary (i.e., can be turned on/off) for each Organization in the Enterprise. |
| **User Registry** | Enterprise administrative users, each having a user name and password. |
| **Metadata Registry** | All Enterprise metadata, comprised of the following:<br>• **Field(s)** – a metadata Field is the description of a data field. Fields may describe objects managed in the SBX |

| *Enterprise-Level Components* | |
|---|---|
| | Object Store or objects that are not managed by SBX, e.g., fields in a database.<br>• **Standards Group(s)** – a logical container that holds Field definitions.<br>• **Entity Group(s)** - a logical container for metadata Fields inherited from a Standards Group. An Entity Group is a special class of Data Group and is always the initial group added to a Template. A single Entity Group can be the initial group for more than one Template.<br>• **Data Group(s)** - a logical container for metadata Fields inherited from a Standards Group. When a field in a Standards Group is modified, the inherited field in a Data Group will automatically reflect the modification.<br>• **Template(s)** - a logical container for associated Data Groups. A Template can be configured to represent a data structure such as a database and tables with fields, enabling a metadata representation of a separate database or database(s). An Entity Group is always the initial Group in the structure. |
| **Organization Registry** | A list of Organizations in the Enterprise. Each Organization maintains User Name and Password policy as well as Audit table locations. All users belong to an Organization. |

Table 1 – Enterprise-Level Components

| *Organization-Level Components* | |
|---|---|
| **Audit Registry** | Discretionary (on/off) audit at specified audit locations within registered non-SBX applications/services. |
| **User Registry** | Organization administrative users (managers) and limited users, each having a user name and password. |
| **Data Element Objects** | Data elements (objects containing user created/variable data) managed by SBX must be identified by a metadata Field contained in an Entity Group that in turn is contained in a Template. |

Table 2 – Organization-Level Components

### 1.4.4 SBX Enigma™ Fine-Grained Access Control

SBX Enigma™ provides pervasive, fine-grained access control over each Metadata Component and Data Element Object as shown below.

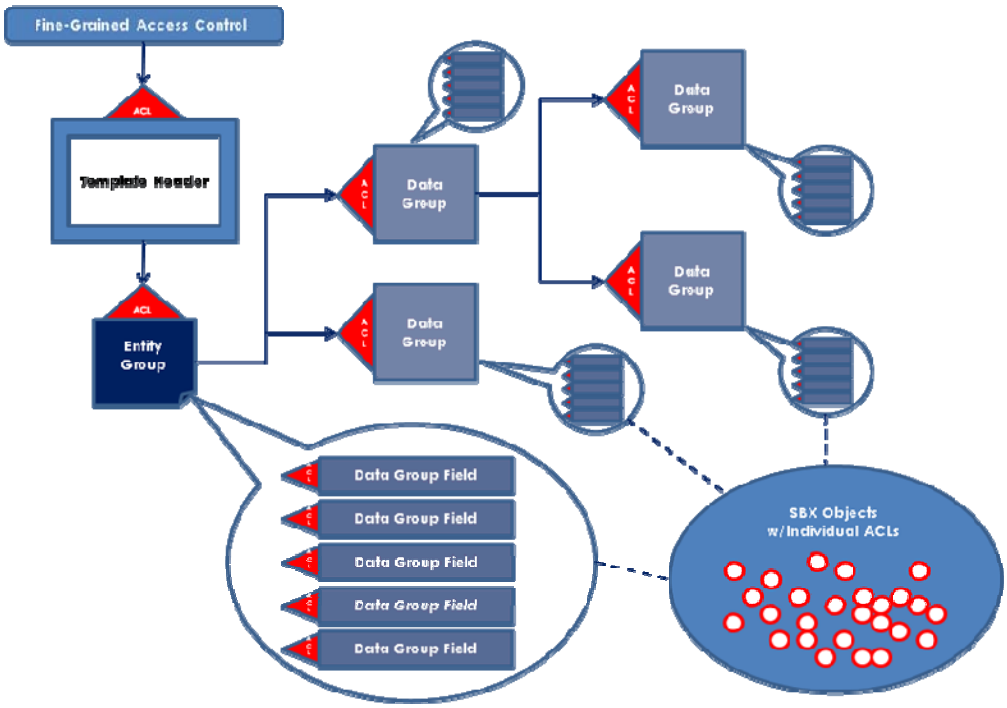


Figure 3 – SBX Enigma™ Access Control

### 1.4.5 SBX Enigma™ Role-Based User Structure

The user structure provided by SBX is designed to support management of data security through a system of role separation as applied to administrative functions and access privileges. Administrative Users are created with specific privileges. Administrative functions in SBX are only accessible by Administrative Users with specific role privileges appropriate to the function. Metadata and Data Element security is managed by Administrative Users. Administrative Users consist of the following roles:

- Enterprise-Level Admin Users
  - SBX System Administrator(s)
  - SBX User Administrator
  - SBX Metadata Admin(s)
- Organization-Level Admin Users
  - User Manager(s)
  - Data Manager(s)
  - Audit Manager(s)

Limited Users (LU) (i.e., non-Administrative Users) belong to an Organization and must have a unique User Name and Password. User Groups contain LUs and provide a grouping mechanism for access privileges. Access Control is the process of defining a LU's access to Metadata (read or deny) and access to Data Elements (read, read/write, or deny).

Role-based Access Control is used to selectively share Metadata and Data Element information with User Groups containing LUs. This access control mechanism can be used to enforce need-to-know style confidentiality by controlling the disclosure, creation, modification and deletion of data elements. The Role-based Access Control mechanism manages access to Metadata and Data Element Objects. Metadata and Data Element access privileges are always granted to User Groups and not to individual users.

As shown in Figure 4, there are specific user roles/functions at both the Enterprise-Level and the Organization-Level.

| ***Enterprise-Level User Structure*** | |
|---|---|
| **SBX System Administrator** | Enters Encryption Key<br>Creates Organizations<br>Maintains each Organization's attributes<br>Creates SBX Metadata Administrator(s)<br>Creates SBX User Administrator<br>Creates SBX Audit Registry Application/Location List<br>Cannot be added to another User Group<br>No access to Metadata or Data Element Objects |
| **SBX Metadata Administrator** | Creates Metadata<br>Cannot be added to another User Group<br>No access to Data Element Objects |
| **SBX User Administrator** | Creates initial User Manager for each Organization<br>Cannot be added to another User Group<br>No access to Metadata or Data Element Objects |

Table 3 – Enterprise-Level User Structure

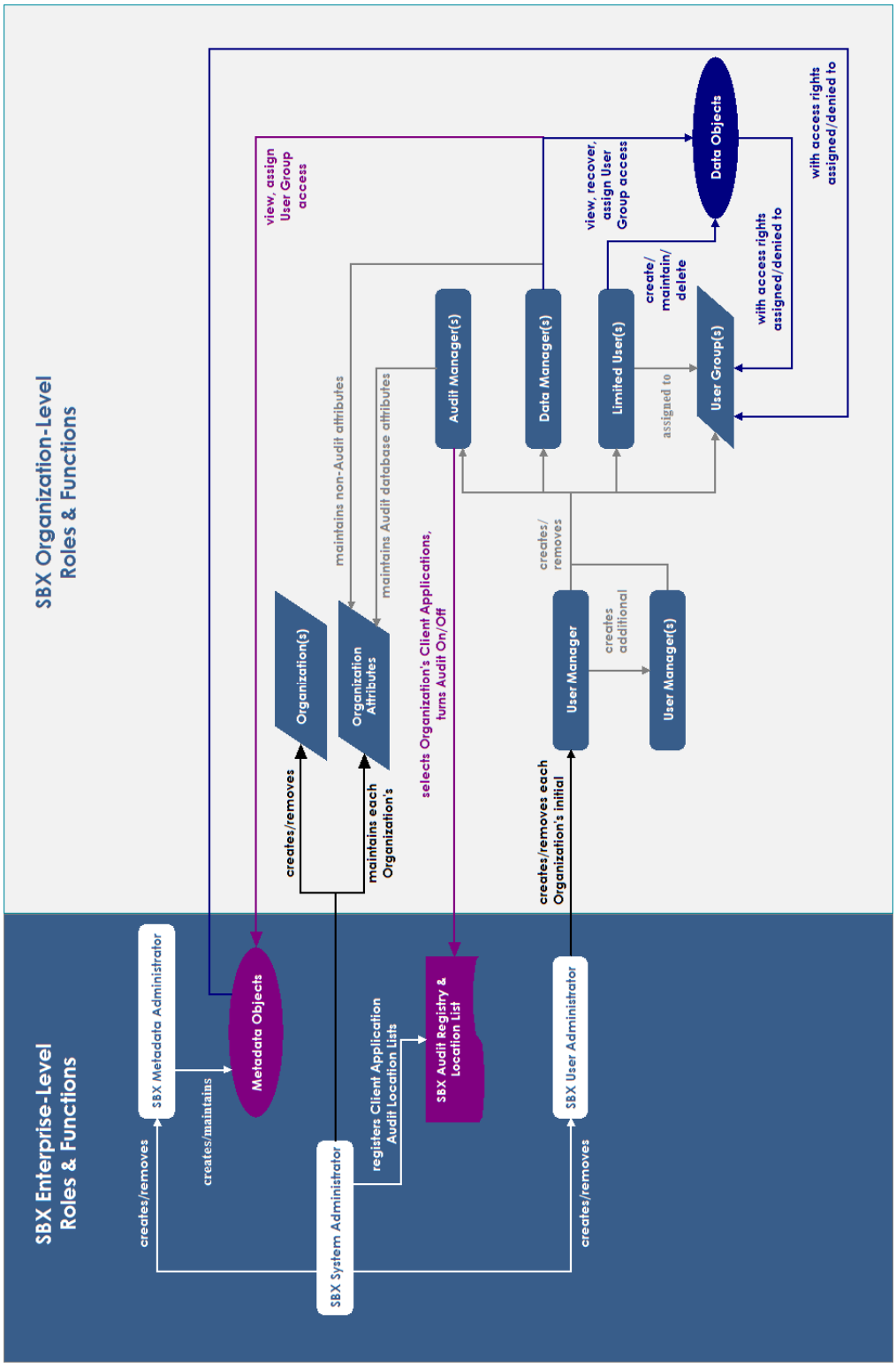


Figure 4 – SBX Enigma™ Roles and Functions

| *Organization-Level User Structure* | |
|---|---|
| **User Manager** | Creates Additional User Manager(s) for own Organization<br>Creates Audit Manager(s) for own Organization<br>Creates Data Manager(s) for own Organization<br>Creates Limited Users for own Organization<br>Creates User Groups<br>Adds own Organization's Limited Users to User Groups<br>Cannot be added to another User Group<br>No access to Metadata or Data Element Objects |
| **Data Manager** | Maintains own Organization's non-Audit attributes<br>Maintains User Group access to Metadata<br>Maintains User Group access to own Organization's Data Elements<br>Read Only access to Metadata & own Organization's Data Element Objects<br>Can recover own Organization's deleted Data Elements<br>Cannot be added to another User Group |
| **Audit Manager** | Maintains own Organization's Audit attributes<br>Maintains own Organization's Audit Registry entries<br>Maintains fine-grained control of Organization's audit directives<br>Cannot be added to another User Group<br>No access to Metadata or Data Element Objects |
| **Limited Users** | Not a member of any Administrative Role<br>No access to any administrative functions<br>Assigned membership in User Group(s)<br>Inherits User Group privileges to access Metadata and Data Element Objects<br>Can create, maintain, delete Data Element Objects based on User Group Privileges |
| **User Groups** | Virtual sub-population of Users from one or multiple Organizations<br>Assigned access privileges to Metadata and Data Element Objects |

Table 4 – Organization-Level User Structure

### 1.4.6 SBX Enigma™ Access Procedures

#### 1.4.6.1 Identification and Authentication

SBX Enigma™ always authorizes a user prior to establishing a session for that user. A user must specify a user name and password in order to establish a session. For any user name, the password specified is compared to the password stored in SBX and, if they match, an SBX Enigma™ session is created. The user's password is stored in SBX in a one-way encrypted form, so before the comparison is made, the password specified by the user is also one-way encrypted.

#### 1.4.6.2 Communications/Connection

Depending on the type of functions or services being sought, SBX Enigma™ provides two types of user connections:

Administrative functions are accessed by Administrative Users using the Eaglehawk Remote Thin Client.

All custom client service access to SBX Enigma™ is established and managed by the SBX Enigma™ Application Program Interface (API).

Once an SBX Enigma™ session is established, a user's ability to access Metadata and/or Data Elements is determined by SBX access control processes. For Administrative Users these access authorities extend to administrative functions associated with specific administrative roles. For Limited Users, these access authorities are determined by, first, the LU's membership in established User Groups and, second, the access authorities extended to those specific User Groups.

While the user has a valid session, the user can make requests to SBX to read and write information in its in-memory object store. SBX handles each request, performing the read and write access to objects and returning data and results to the user, in accordance with the user's access authority to objects or administrative role.

#### 1.4.6.3 Password Management

A user may change his or her password at any time. SBX provides the facility for suitably privileged Administrative Users to create password complexity-check policies that can screen new passwords for certain criteria, e.g.:

- a minimum number of characters in length
- includes a minimum number of alpha characters
- includes a minimum number of numeric characters
- includes a minimum number of special characters
- includes mixed case characters

A suitably authorized Administrative User can also set password lifetime and identify a user for limited access, forcing a user account to become disabled when the password lifetime is reached.

In addition, SBX has facilities for challenge questions with answers that are completely controlled by the user with no oversight by User Managers or other Administrative Users. Utilizing this method of administering their account, users are able to manage their own password without ever disclosing it to administrative personnel.

#### 1.4.6.4 Access Control Lists

Access Control Lists, or ACLs, manage access to all Metadata and Data Element Objects. For each such object, the ACL specifies:

- User Groups with access permissions vis-à-vis the object, and
- Type of access (read/write, read only, or deny) assigned to each User Group

A User's access to Metadata and Data Element Objects, therefore, is determined by the User's membership in a User Group with authority to access such objects and by the type of access assigned to that User Group.

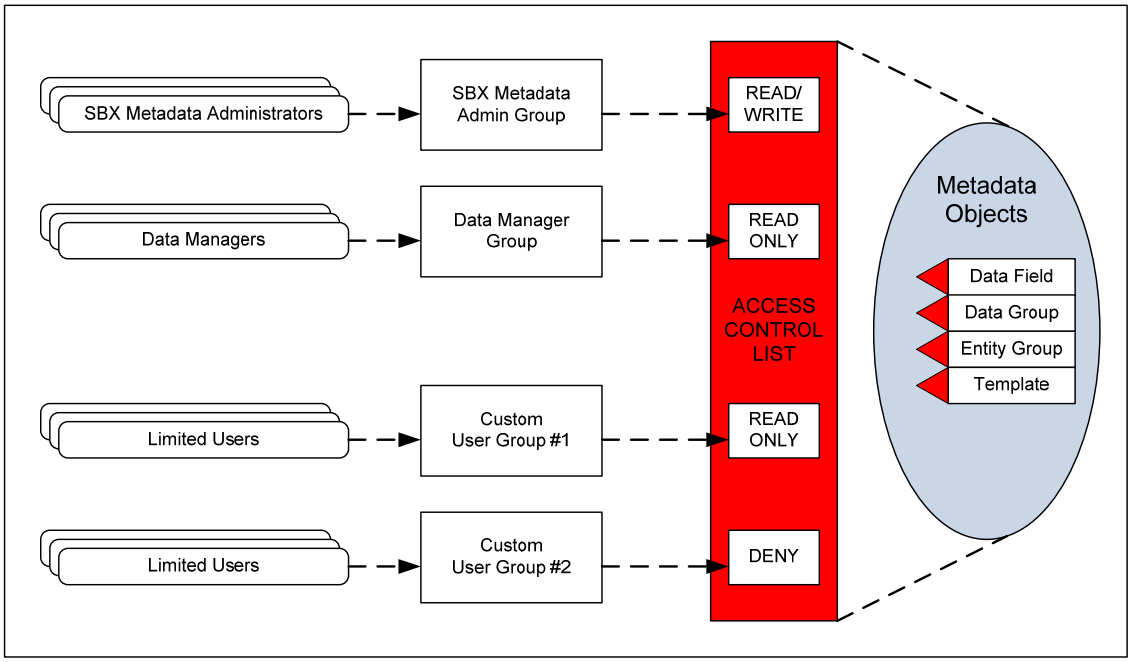


Figure 5 – ACLs on Metadata Objects

As indicated in Figure 5, the ACLs on Metadata Objects specify the following User Group access:

- SBX Metadata Administrator Group with Read/Write access authority on all Enterprise Metadata Objects
- Data Manager Group with Read Only access authority on all Enterprise Metadata Objects
- Custom User Group with Read Only access authority on Metadata Objects specified by the Organization's Data Manager

- Custom User Group with Deny access authority on Metadata Objects specified by the Organization's Data Manager

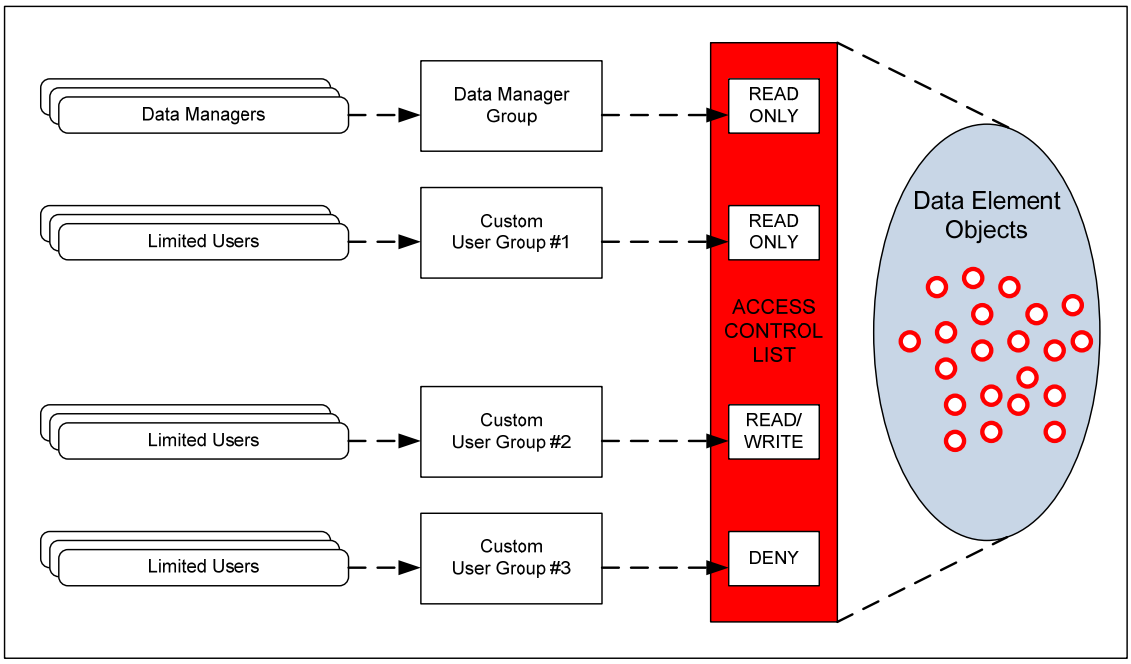


Figure 6 – ACLs on Data Element Objects

As indicated in Figure 6 the ACLs on Data Element Objects specify the following User Group access:

- Data Manager Group with Read Only access authority on own Organization's Data Element Objects
- Custom User Group with Read Only access authority on own Organization's Data Element Objects specified by the Organization's Data Manager
- Custom User Group with Read/Write access authority on own Organization's Data Element Objects specified by the Organization's Data Manager
- Custom User Group with Deny access authority on own Organization's Data Element Objects specified by the Organization's Data Manager

### 1.4.7 SBX Enigma™ Audit Functions

#### 1.4.7.1 Audit

SBX ensures that relevant information about operations performed by users can be recorded so that the consequences of those operations can later be linked to the user in question, and the user held accountable for his or her actions.

SBX does this by providing auditing options that are designed to be as granular and flexible as possible to ensure that exactly what needs to be audited, as dictated by the service or system security policy, is recorded, but nothing more. This helps to ensure that the size of audit logs remains manageable and the important records easily accessible. SBX provides capabilities to permit auditing plans to be quickly enabled to implement crisis responses. In addition to mandatory audit of all SBX administrative functions, custom client service-specific audit can be implemented with fine-grained control of specific SBX interaction.

#### 1.4.7.2 Audit Options

All SBX administrative functions are subject to mandatory audit. Custom client applications/services must have an entry in the SBX Audit Registry in order for SBX interaction to take place. Users with appropriate privilege (Audit Managers) have fine-grained control over whether a specific audit should be activated, whether the service request, response, or both should be audited, and if required, SBX can be instructed to create a hash value for the audit record and store the hash value in a separate database table so that audit log tampering can be detected.

#### 1.4.7.3 Audit Records

SBX provides for a suitably privileged Administrative User to direct audit records to be written to a database audit trail of their choice. The audit database type and location can be unique for each Organization. SBX audit records include items such as;

- User
- Organization
- Terminal identifier
- Date and Timestamp
- Relevant operation data

#### 1.4.7.4 Audit Analysis

If SBX writes to the audit log, then the SQL data manipulation and reporting facilities of the DBMS can be used by appropriately authorized database Administrative Users to perform selective analysis of relevant SBX operations, user actions and object access in a secure manner.

**This page intentionally left blank.**

# 2 Conformance Claim

## 2.1 CC Conformance Claim

This Security Target conforms to the ***Common Criteria for Information Technology Security Evaluation Version 3.1 Release 2 September 2007.***

This Security Target is ***CC Part 2 conformant.***

This Security Target is ***CC Part 3 conformant.***

This Security Target conforms to the ***Evaluation Assurance Level 2 augmented with the additional Security Assurance Requirement ALC_FLR.1 Basic flaw remediation. (EAL2+)*** packages.

## 2.2 PP Claim

This Security Target for SBX Enigma™ makes no claim of conformance to a protection profile.

## 2.3 Conformance Rationale

As there is no conformance claim to a PP, there is no conformance rationale.

**This page intentionally left blank.**

# 3 Security Problem Definition

## 3.1 Introduction

The security problem definition defines the threats within the operational environment that are to be addressed by the Eaglehawk SBX Enigma™ TOE. The Threats represent a risk within the operational environment and need to be countered by the TOE. Some security problem threats are mitigated by the Organizational Security Policies (OSP) that are enforced by either the TOE, its operational environment, or a combination of both. Assumptions are made regarding the operational environment, and define supporting security countermeasures that are outside the scope of the TOE ICT security and are needed for the secure solution to reduce the security problem to an acceptable level.

This section defines the threats, the OSP and assumptions of the security problem of the Eaglehawk SBX Enigma™ TOE.

## 3.2 Threats

Threats are implemented by a threat agent who wishes to compromise an asset through an adverse action of the threat agent on that asset. The threats in Table 5 are to be countered by either the TOE, its operational environment, or a combination of both.

| Threat | Definition |
|---|---|
| T.ACCIDENTAL_ADMIN | An administrator may incorrectly install or configure the TSF resulting in ineffective security mechanisms. |
| T.AUDIT_ COMPROMISE | A user, process or hostile external party may compromise audit records, cause audit records to be lost or modified, or prevent future audit records from being recorded. |
| T.BYPASS | An unauthorised user or hostile external party may attempt to bypass the access control policy to gain access to the trusted data or compromise the integrity of the data. |
| T.DATA_COMPROMISE | A user, process or hostile external party may cause data to be inappropriately accessed (viewed, modified, or deleted), thus compromising the confidentiality and integrity of the data protected by the system. |
| T.MASQUERADE | A user, process or hostile external party may masquerade as another entity in order to gain unauthorized access to the trusted data or compromise the integrity of the data. |

Table 5 – Threat to the TOE

## 3.3 Organizational Security Policies

Organizational Security Policies (OSP) are a set of rules, procedures, or guidelines imposed by an organization that are to be enforced by the TOE and its Organizational environment to address its security needs.

| Policy | Definition |
|---|---|
| P.ACCOUNTABILITY | The authorized users of the TOE shall be held accountable for their actions within the TOE. |
| P.CRYPTO_KEY_ MANAGEMENT | Key management is a manual Organizational security policy practice. |
| P.ROLES | The TOE shall provide an authorized administrator and management roles for secure administration and configuration of the TOE. |

Table 6 – Organizational Security Policies

## 3.4 Assumptions

This section contains assumptions regarding the IT environment in which the TOE will reside.

| Assumption | Definition |
|---|---|
| A.EDUCATED_ MANAGEMENT | Administrators and managers are educated in respect to their responsibilities, security functionality under their control and the benefits/protection of successful implementation. |
| A.NETWORK_ SECURITY | All SBX Enigma™ data that traverses a network is protected from disclosure to unauthorised parties. |
| A.NO_EVIL | Administrators are non-hostile, appropriately trained, and follow all administrator guidance. |
| A.NO_GENERAL_ PURPOSE | There are no general-purpose computing capabilities (e.g., compilers or user applications) available on SBX Enigma™ servers. |
| A.OS_VALIDATED | The underlying OS has been evaluated and provides a level of trust. |
| A.PHYSICAL | It is assumed that appropriate physical security is provided within the domain for the value of the IT assets protected by the TOE and the value of the stored, processed, and transmitted information. |

Table 7 – Applicable Assumptions

# 4 Security Objectives

This section describes the security objectives of the TOE, the security objectives for the operational environment and a security objectives rationale. The security objectives identify the responsibilities of the TOE and its operational environment in resolving the security problem described in section 3.

## 4.1 Security Objectives for the TOE

The TOE provides security functionality to solve elements of the security problem defined in the security problem definition. This part of the problem resolution is based on implementing the objectives of the TOE as listed in Table 8.

| TOE Objective Name | TOE Objective Definition |
|---|---|
| O.ACCESS_CONTROL | The TOE will store and retrieve information (to authorized users) related to the user profile and access rights. |
| O.AUDIT_GENERATION | The TOE will provide the capability to create audit records associated with the security-relevant event. |
| O.CRYPTOGRAPHY | The TOE shall encrypt data maintained in SBX data element objects. |
| O.I&A | The TOE will identify and confirm the accuracy of authentication credentials before allowing the user to gain access to the TOE. |
| O.ROLE-BASE_ MANAGEMENT | The TOE will provide authorized administrators and managers roles that isolate administrative actions. |

Table 8 – Security objective for the TOE

## 4.2 Security Objectives for the Operational Environment

The security objectives of the operational environment are listed in Table 9.

| Environmental Objective Name | Environmental Objective Definition |
|---|---|
| OE.CRYPTO_KEY_ MANAGEMENT | Key management is a manual practice. How keys are managed is not an objective of the environment as it can vary from installation to installation. |
| OE.MANAGMENT_ EDUCATION | SBX Administrators and Managers are educated in respect to their responsibilities, the security functionality under their control, and the benefits/protection of successful implementation and operation. |

| | |
|---|---|
| OE.NO_EVIL | Sites using the TOE shall ensure that authorized administrators are non-hostile, appropriately trained and follow all administrator guidance. |
| OE.NO_GENERAL_ PURPOSE | There will be no general-purpose computing capabilities (e.g., compilers or user applications) available on SBX Enigma™ Servers. |
| OE.OS_ VALIDATED | The underlying OS has been evaluated and provides a level of trust. |
| OE.PHYSICAL | Physical security will be provided within the domain for the value of the IT assets protected by the TOE and the value of the stored, processed, and transmitted information. |
| OE.SECURE_NETWORK | SBX Enigma™ data traverses a secure network that protects the data from disclosure to unauthorised parties. This is achieved using a network security protocol. (e.g. Transport Layer Security (TLS) or Secure Sockets Layer (SSL) cryptographic protocols). |

Table 9 – Security objective for the operational environment

## 4.3 Security Objectives Rationale

The security objectives of the TOE are to mitigate the security problem. The security objectives rationale trace each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective. The security objectives rationale shall demonstrate that the security objectives counter all threats. The security objectives rationale shall demonstrate that the security objectives enforce all OSPs. The security objectives rationale shall demonstrate that the security objectives for the operational environment uphold all assumptions.

### 4.3.1 Tracing between security objectives and the security problem definition

The following table shows the tracing between the security objectives and the threats, OSPs and assumptions as described in section 3, the security problem definition.

The tracing as shown in Table 10 obey the three rules:

- No spurious objectives: Each security objective traces to at least one threat, OSP or assumption.
- Complete with respect to the security problem definition: Each threat, OSP and assumption has at least one security objective tracing to it.
- Correct tracing: Since assumptions are always made by the TOE on the operational environment, security objectives for the TOE do not trace back to assumptions.

| Threats / Organizational Security Policy / Assumptions — Security objectives of the TOE / Security objectives of the Operational Environment | T.ACCIDENTAL_ADMIN | T.AUDIT_COMPROMISE | T.BYPASS | T.DATA_COMPROMISE | T.MASQUERADE | P.ACCOUNTABILITY | P.CRPTO_KEY_MANAGEMENT | P.ROLES | A. EDUCATED_MANAGEMENT | A.NETWORK_SECURITY | A.NO_EVIL | A.NO_GENERAL_PURPOSE | A.OS_VALIDATE | A.PHYSICAL |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| O.ACCESS_CONTROL | | | | X | X | X | | X | | | | | | |
| O.AUDIT_GENERATION | X | X | | X | | X | | | | | | | | |
| O.CRYPTOGRAPHY | | | X | | | | | | | | | | | |
| O.I&A | | | X | X | X | X | | X | | | | | | |
| O.ROLE-BASE_MANAGEMENT | X | X | | X | | | | X | | | | | | |
| OE.CRYPTO_KEY_MANAGEMENT | | | | | | | X | | | | | | | |
| OE.MANAGEMENT_EDUCATION | X | X | | | | | | X | X | | | | | |
| OE.NO_EVIL | | | | | | | | | | | X | | | |
| OE.NO_GENERAL_PURPOSE | | | | | | | | | | | | X | | |
| OE.OS_VALIDATE | | | | | | | | | | | | | X | |
| OE.PHYSICAL | | | | | | | | | | | | | | X |
| OE.SECURE_NETWORK | | | | | | | | | | X | | | | |

Table 10 – Security objective rationale

### 4.3.2 Providing a justification for the trace

This section of the security objectives rationale defines the effectiveness of the security objectives countering the particular threat/OSP/assumption to an acceptable level.

This analysis is based on the threat and threat agent, the OSP and how the assumptions are realised through the objectives of the environment.

**Threats**

The threat **T.ACCIDENTAL_ADMIN**, is where an administrator may incorrectly install or configure the TSF resulting in ineffective security mechanisms, and is primarily countered by the objective. This threat is mitigated by the **OE.MANAGEMENT_EDUCATION** where the SBX Administrators and Managers are educated in respect to their responsibilities, the security functionality under their control, and the benefits/success of successful implementation and operation. The threat is also addressed by the **O.AUDIT_GENERATION** and **OE.ROLE-BASE_MANAGEMENT** where the actions of the SBX Administrators are audited and only the authorized administrator can perform the administrative role and actions.

The threat **T.AUDIT_COMPROMISE**, is where a user, process or hostile external party may compromise audit records, cause audit records to be lost or modified, or prevent future audit records from being recorded. This threat is mitigated by the **OE.MANAGEMENT_EDUCATION** where the SBX administrator and managers are educated in respect to their responsibilities and successful implementation and operation. The objective of **OE.ROLE-BASE_MANAGEMENT** is the authority that provides the basis for, first, the System Administrator's role that registers (at the

Enterprise Level) and specifies audit locations for client applications in the SBX Audit Registry and, second, the Audit Manager's role that registers (at the Organization Level) and defines the client application events that are to be audited, plus activates and deactivates audit functions in the SBX Audit Registry. The objective **O.AUDIT_GENERATION** also provides supporting countermeasures in the form of a hash for each audit element that is stored separately from the Audit log. By analysis of the hash in conjunction with the log the Audit manager would be able to determine an audit compromise.

The threat **T.BYPASS**, is where an unauthorised user or hostile external party may attempt to bypass the access control policy to gain access to the trusted data or compromise the integrity of the data. This threat is mitigated by the **O.CRYPTOGRATHY** objectives and supported by **O.I&A** objective. The **O.I&A** provides the security mechanisms to prevent unauthorised/unauthenticated access to the TOE, while **O.CRYPTOGRATHY** prevents access to the data held in memory by bypassing the TOE.

The threat **T.DATA_COMPROMISE,** is where a user, process or hostile external party may cause data to be inappropriately accessed (viewed, modified, or deleted), thus compromising the confidentiality and /or the integrity of the data protected by the system. This is the prime threat to the TOE and is mitigated by the **O. ACCESS_CONTROL, O.I&A, O.ROLE-BASE_MANAGEMENT** and the supporting objective **O.AUDIT_GENERATION**. The **O.I&A** and the **O.ROLE-BASE_MANAGEMENT** objectives ensure that an authorised person is identified and authenticated by the system, the **O. ACCESS_CONTROL** objective only allows the appropriate user access to the protected data held in memory, while the objective is monitoring all the transactions that could potentially compromise the system.

The threat **T.MASQUERADE**, is where a user, process or hostile external party may masquerade as another entity in order to gain unauthorized access to the trusted data or compromise the integrity of the data. This threat is mitigated by the **O.I&A** where an authorised user is identified and authenticated by the system. If a user who has been authorised and has accessed the system the **O. ACCESS_CONTROL** objective prevents them from masquerading as another user and getting access to inappropriate information.

**Organizational Security Policies**

The Organizational security policy **P.ACCONTABILITY**, is where the authorized users of the TOE shall be held accountable for their actions within the TOE. This policy is implemented by the objectives **O.I&A, O. ACCESS_CONTROL** and **O.AUDIT_GENERATION** where the implementation of the policy can be realised as each user transaction can be analysed. The **O.I&A** and the **O.ACCESS_CONTROL** objectives ensure that anybody who has access to the data is authenticated and therefore has been made accountable.

The Organizational security policy **P.CRYPTO_KEY_MANAGEMENT** is associated with the manual management of the Cryptographic Key requirements. This policy is implemented by the objective of the environment **OE.CRYPTO_KEY_MANAGEMENT**. This objective defines that the Key management is a manual practice. How keys are managed is not an objective of the environment as it can vary from installation to installation.

The Organizational security policy **P.ROLES**, is where the TOE shall provide an authorized administrator and management roles for secure administration and configuration of the TOE. This policy is implemented by the objectives **O.I&A, O.ACCESS_CONTROL** and **O.ROLE-BASE_MANAGEMENT** where the role-base management is authorised before gaining access to the specific system elements based on their access privileges to conduct their individual distinct

role-based activities to manage, configure and maintain the system. This policy is supported by the **OE.MANAGEMENT_EDUCATION** where the SBX administrator and managers are educated in respect to their responsibilities and operational tasks to maintain the system.

**Assumptions**

The supporting assumption **A.EDUCATED_MANAGEMENT**, assumes that administrative and management users are educated in respect to their responsibilities, the security functionality under their control and the benefit / protection of a successful implementation and operation. This assumption is addressed by the objective of the environment **OE.MANAGEMANT_EDUCATION**.

The assumption **A.NETWORK_SECURITY**, assumes that network security is protecting the SBX Enigma™ data from being disclosed to a third party who does not have authority to see or access the data. This assumption is addressed by the objective of the environment **OE.SECURE_NETWORK** which requires that SBX Enigma™ data traversing the network be secure. For example this may be achieved by the operating systems utilising Transport Layer Security (TLS) or Secure Sockets Layer (SSL) cryptographic protocols.

The supporting assumption **A.NO_EVIL**, assumes that administrators are non-hostile, appropriately trained, and follow all administrator guidance. This assumption is addressed by the objective of the environment **OE.NO_EVIL**.

The assumption **A.NO_GENERAL_PURPOSE**, assumes that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on SBX Enigma™ servers. This assumption is addressed by the objective of the environment **OE.NO_GENERAL_PURPOSE** which requires that there be no such capabilities on the SBX Enigma™ servers.

The assumption **A.OS_VALIDATION**, assumes that the underlying OS has been evaluated and provides a level of trust. This assumption is addressed by the objective of the environment **OE.OS_VALIDATION** which requires that the system is installed and operated on a trusted operating system as a secure platform.

The assumption **A.PHYSICAL**, assumes that appropriate physical security is provided within the operational environment that is sufficient for the protection of the IT assets being processed by the TOE. This assumption is addressed by the objective of the environment **OE.PHYSICAL**.

## 4.4 Security objectives: conclusion

Based on the security objectives and the security objectives rationale, the following conclusion can be drawn: if all security objectives are achieved then the security problem as defined in section 3 is solved: all threats are countered, all OSPs are enforced, and all assumptions are upheld.

**This page intentionally left blank.**

# 5 Extended Components Definition

There are no extended components within this security target.

**This page intentionally left blank.**

# 6 Security Requirements

The security requirements consist of two groups of requirements:

- The Security Functional Requirements (SFR): a translation of the security objectives for the TOE into a standardised language;
- The Security Assurance Requirements (SAR): a description of how assurance is to be gained that the TOE meets the SFRs.

## 6.1 Security functional requirements

This section defines the functional requirements for the TOE. These SFRs were drawn directly from Part 2 of the CC. These requirements are relevant to supporting the secure operation of the TOE.

| **Functional Components** | |
|---|---|
| Class FAU: Security Audit | |
| FAU_GEN.1 | Audit data generation |
| FAU_GEN.2 | User identity association |
| Class FCS: Cryptographic Support | |
| FCS_COP.1 | Cryptographic operation |
| Class FDP: User Data Protection | |
| FDP_ACC.1 | Subset access control |
| FDP_ACF.1 | Security attribute based access control |
| Class FIA: Identification and Authentication | |
| FIA_AFL.1 | Authentication failure handling |
| FIA_ATD.1 | User attribute definition |
| FIA_UAU.1 | Timing of authentication |
| FIA_UID.1 | Timing of identification |
| FIA_USB.1 | User-subject binding |
| Class FMT: Security Management | |
| FMT_MSA.1 | Management of security attributes |
| FMT_MSA.3 | Static attribute initialisation |

| Functional Components | |
|---|---|
| FMT_MTD.1 | Management of TSF data |
| FMT_REV.1 | Revocation |
| FMT_SMF.1 | Specification of management functions |
| FMT_SMR.2 | Restrictions on security roles |
| Class FTA: TOE Access | |
| FTA_TAH.1 | TOE access history |

Table 11 – Security Functional Requirements

## 6.1.1 Security Audit (FAU)

### 6.1.1.1 Audit data generation (FAU_GEN.1)

Dependencies: FPT_STM.1 Reliable time stamps

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

- Start-up and shutdown of the audit functions;
- All auditable events for the [**selection:** *not specified* ] level of audit
- [**assignment:** *Start-up and shutdown of the SBX Enigma; All SBX Administrator events*].

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 (if applicable), 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, [**assignment:** *information specified in column three of Table 12 following*].

**Application Note**: *Table 12 lists all the SFRs of the SBX Enigma™ TOE. Column 3, "Audit Record Contents" is used to designate data that should be included in the audit record in the context of the event that generates the record. If no information is required (other than that listed in item a) above) for a particular auditable event, then an assignment of "none" has been made and there is no additional contents to the audit record.*

| Security Functional Requirement | Auditable Event(s) | Additional Audit Record Contents |
|---|---|---|
| FAU_GEN.1 | None | |
| FAU_GEN.2 | None | |
| FCS_COP.1 | None | |
| FDP_ACC.1 | None | |
| FDP_ACF.1 | Successful requests to perform an operation on an object covered by the SFP | The identity of the subject performing the operation |
| FIA_AFL.1 | The reaching of the threshold for the unsuccessful authentication attempts and the action taken and the subsequent restoration to the normal state | The identity of the subject failing to authenticate. |
| FIA_ATD.1 | None | |
| FIA_UAU.1 | Unsuccessful use of the authentication mechanism | The identity of the user failing to authenticate. |
| FIA_UID.1 | Unsuccessful use of the identification mechanism including the users identity provided | The identity provided of the user failing to correctly identify. |
| FIA_USB.1 | Unsuccessful binding of user security attributes to a subject | The identity of the user and the subject that failed to bind |
| FMT_MSA.1 | None | |
| FMT_MSA.3 | None | |
| FMT_MTD.1 | None | |
| FMT_REV.1 | Unsuccessful revocation of security attributes | Identity of the individual attempting to revoke security attributes |
| FMT_SMF.1 | Use of the management functions | Identity of the administrator performing these functions |
| FMT_SMR.2 | Modifications to the group of users that are part of a role | Identity of the authorized administrator modifying the role definition |
| FTA_TAH.1 | None | |

Table 12 – Auditable events

#### 6.1.1.2 User identity association (FAU_GEN.2)

Dependencies FAU_GEN.1 Audit Data Generation

FIA UID.1 Timing of identification

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

### 6.1.2 Cryptographic support (FCS)

#### 6.1.2.1 Cryptographic operation (FCS_COP.1)

Dependencies FCS_CKM.1 Cryptographic key generation

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [**assignment:** *data encryption, and decryption*] in accordance with a specified cryptographic algorithm [**assignment:** *Advanced Encryption Standard (AES)*] and cryptographic key size [**assignment:** *256 bits*] that meet the following: [**assignment:** *FIPS197*].

### 6.1.3 User data protection (FDP)

#### 6.1.3.1 Subset access control (FDP_ACC.1)

Dependencies FDP_ACF.1 Security attributes based access control

FDP_ACC.1.1 The TSF shall enforce the [**assignment:** *Role-based Access Control policy*] on [**assignment:** *The following subjects:*

- *SBX System Administrator(s);*
- *SBX User Administrator;*
- *SBX Metadata Administrator(s);*
- *User Manager(s);*
- *Data Manager(s);*
- *Audit Manager(s); and*
- *Limited User(s)*

*The following objects:*

- *Organization;*
- *SBX Audit Register location List;*

- *Metadata Objects; and*
- *Data Objects;*

*With the following operations between the subjects and objects:*

- *SBX System Administrator(s)*
  - *Create, maintains and removes organizations;*
  - *Registers client applications audit location lists;*
  - *Creates and removes SBX Metadata Administrator*
  - *Creates and removes SBX User Administrator*
- *SBX User Administrator;*
  - *Creates and removes the initial User Manager of each Organization;*
- *SBX Metadata Administrator(s);*
  - *Creates and maintains Metadata Objects;*
- *User Manager(s);*
  - *Creates additional User Manager(s)*
  - *Creates and removes Audit Manager(s)*
  - *Creates and removes Data Manager(s)*
  - *Creates and removes Limited User(s)*
  - *Creates and removes User Groups(s)*
- *Data Manager(s);*
  - *Views Data Element Objects and, assigns User Group access to Data Element Objects;*
  - *Recovers deleted Data Element Objects;*
  - *Views Metadata Objects and, assigns User Group access to Metadata Objects;*
  - *Maintains non-Audit attributes of the Organizations*
- *Audit Manager(s);*
  - *Maintains Audit database attributes*
  - *Selects Client application (Turns Client audit on/off)*
- *Limited User(s);*

- *Create, maintain and delete Data Element Objects*].

#### 6.1.3.2 Security attribute based access control (FDP_ACF.1)

Dependencies FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1 The TSF shall enforce the [**assignment:** *Role-based Access Control policy*] to objects based on the following: [**assignment:**

*Objects*

- *Organization(s):*
  - *cryptographic keys;*
  - *number of organization security questions;*
  - *number of limited user Q/A;*
  - *login failure limit;*
  - *user name policy;*
  - *user password policy;*
  - *password;*
  - *credentials;*
  - *user detail;*
  - *assigned groups;*
  - *client applications audit registry elements;*
- *Metadata Objects:*
  - *metadata fields, groups and templates;*
  - *Metadata Objects User Group access list;*
- *Data Element Objects:*
  - *Data Object User Group access list;*
- *SBX Audit Registry:*
  - *Audit registry fields*

*Subjects*

- *Administrators:*
  - *cryptographic keys*;

- *Audit registry fields;*
- *Enterprise level Administrator roles;*
- *number of organization security questions;*
- *number of limited user Q/A;*
- *login failure limit;*
- *user name policy;*
- *user password policy;*
- *password;*
- *credentials;*
- *user details;*
- *assigned groups;*
- *client applications audit registry elements;*
- *Metadata user group access list;*
- *Data Object user group access list;*
- *non-Audit attributes;*

- *Users*
  - *password:*].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**assignment:** *based on the following ordered rules:*

- *If the requested mode of access is denied to any group of which the authorized user is a member, deny access;*
- *If the requested mode of access is read only to a group of which the authorized user is a member, grant read only access to the user;*
- *If the requested mode of access is read/write to a group of which the authorized user is a member, grant read and write access to the user;*
- *Deny access*].

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [**assignment:**

- *The user with the role SBX System Administrator can remove and maintain the Organization(s);*

- *The user with the role SBX Metadata Administrator can Maintain the Metadata Object;*
- *The user with the role Data Manager can access the Metadata Object to view and assign User Group Access;*
- *The user with the role Data Manager can access the Data Element Object to view, recover and assign User Group Access;*
- *The user with the role Data Manager maintains the Organization non-Audit attributes;*
- *The Audit Manager maintains the Organization Audit database attributes;*].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following rules: [**assignment:**

- *SBX System Administrator has no access to Metadata or Data Element Objects;*
- *SBX User Administrator has no access to Metadata or Data Element Objects;*
- *SBX Metadata Administrator has no access to Data Element Objects;*
- *An Organization User Manager has no access to Metadata or Data Element Objects;*
- *An Organization Audit Manager has no access to Metadata or Data Element Objects*]

### 6.1.4 Identification and authentication (FIA)

#### 6.1.4.1 Authentication failure handling (FIA_AFL.1)

Dependencies FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when [**selection:** *an administrator configurable positive integer within* [**assignment:** *a range from 1to 9*] unsuccessful authentication attempts occur related to [**assignment:** *system login*].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [**selection:** *met*], the TSF shall [**assignment:** *lock out user*].

#### 6.1.4.2 User attribute definition (FIA_ATD.1)

Dependencies No dependencies

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

- *SBX Enigma™ user password;*
- *group memberships;*
- *SBX roles*].

#### 6.1.4.3 Timing of authentication (FIA_UAU.1)

Dependencies FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow [**assignment:** *the SBX user to be identified; and a new account request*] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated action on behalf of that user.

#### 6.1.4.4 Timing of identification (FIA_UID.1)

Dependencies No dependencies.

FIA_UID.1.1 The TSF shall allow [**assignment**: *a new account request*] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated action on behalf of that user.

#### 6.1.4.5 User subject binding (FIA_USB.1)

Dependencies FIA_ATD.1 User attribute definition

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on behalf of that user: [**assignment:** *User Group membership and their SBX roles*].

FIA_USB.1.2 The TSF shall associate the following rules on the initial association of user security attributes with subjects acting on behalf of users: [**assignment:** *None*].

FIA_USB.1.3 The TSF shall associate the following rules governing changes to the user security attributes with subjects acting on behalf of users: [**assignment:** *None*].

### 6.1.5 Security management (FMT)

#### 6.1.5.1 Management of security attributes (FMT_MSA.1A)

Dependencies FDP_ACC.1 Subset access control

FMT_SMR.1 Security roles

FMT_SMF.1 Specifications of Management Functions

FMT_MSA.1A.1 The TSF shall enforce the [**assignment:** *Role-based Access Control policy*] to restrict the ability to [**selection:** ***[assignment:*** *initiate]*] the security attributes [**assignment:** *cryptographic keys*] to [**assignment:** *SBX System Administrators*].

**Application Note:** *this SFR is associated with the Establishment of Data Element Object Encryption.*

#### 6.1.5.2 Management of security attributes (FMT_MSA.1B)

Dependencies FDP_ACC.1 Subset access control

FMT_SMR.1 Security roles

FMT_SMF.1 Specifications of Management Functions

FMT_MSA.1B.1 The TSF shall enforce the [**assignment:** *Role-based Access Control policy*] to restrict the ability to [**selection:** *modify [**assignment:** create]*] the security attributes [**assignment:** *Audit registry fields*] to [**assignment:** *SBX System Administrators*].

**Application Note:** *this SFR is associated with the creation and modification client application audit register location lists of the SBX Audit registry.*

#### 6.1.5.3 Management of security attributes (FMT_MSA.1C)

Dependencies FDP_ACC.1 Subset access control

FMT_SMR.1 Security roles

FMT_SMF.1 Specifications of Management Functions

FMT_MSA.1C.1 The TSF shall enforce the [**assignment:** *Role-based Access Control policy*] to restrict the ability to [**selection:** *modify [**assignment:** create]*] the security attributes [**assignment:** *Enterprise level Administrator roles*] to [**assignment:** *SBX System Administrators*].

**Application Note:** *this SFR is associated with the creation and maintenance of the SBX Metadata Administrator(s) and SBX User Administrator(s).*

#### 6.1.5.4 Management of security attributes (FMT_MSA.1D)

Dependencies FDP_ACC.1 Subset access control

FMT_SMR.1 Security roles

FMT_SMF.1 Specifications of Management Functions

FMT_MSA.1D.1 The TSF shall enforce the [**assignment:** *Role-based Access Control policy*] to restrict the ability to [**selection:** *modify [**assignment:** create]*] the security attributes [**assignment:** *number of organization security questions, number of limited user Q/A, login failure limit, user name policy, user password policy*] to [**assignment:** *SBX System Administrators*].

**Application Note:** *this SFR is associated with the SBX Organization security attributes.*

#### 6.1.5.5 Management of security attributes (FMT_MSA.1E)

Dependencies FDP_ACC.1 Subset access control

FMT_SMR.1 Security roles

FMT_SMF.1 Specifications of Management Functions

FMT_MSA.1E.1 The TSF shall enforce the [**assignment:** *Role-based Access Control policy*] to restrict the ability to [**selection:** *modify [**assignment:** create]*] the security attributes

[**assignment:** *metadata fields, groups and templates*] to [**assignment:** *SBX Metadata Administrators*].

**Application Note:** *this SFR is associated with the SBX Metadata Objects.*

#### 6.1.5.6 Management of security attributes (FMT_MSA.1F)

Dependencies FDP_ACC.1 Subset access control

FMT_SMR.1 Security roles

FMT_SMF.1 Specifications of Management Functions

FMT_MSA.1F.1 The TSF shall enforce the [**assignment:** *Role-based Access Control policy*] to restrict the ability to [**selection:** *delete, modify [**assignment:** create]*] the security attributes [**assignment:** *password, credentials, user details, assigned groups*] to [**assignment:** *User Managers*].

**Application Note:** *this SFR is associated with the Organization User groups.*

#### 6.1.5.7 Management of security attributes (FMT_MSA.1G)

Dependencies FDP_ACC.1 Subset access control

FMT_SMR.1 Security roles

FMT_SMF.1 Specifications of Management Functions

FMT_MSA.1G.1 The TSF shall enforce the [**assignment:** *Role-based Access Control policy*] to restrict the ability to [**selection:** modify *[**assignment:** activate, deactivate]*] the security attributes [**assignment:** *client applications audit registry elements*] to [**assignment:** *Audit Manager*].

**Application Note:** *this SFR is associated with the SBX Audit registry and location lists.*

#### 6.1.5.8 Management of security attributes (FMT_MSA.1H)

Dependencies FDP_ACC.1 Subset access control

FMT_SMR.1 Security roles

FMT_SMF.1 Specifications of Management Functions

FMT_MSA.1H.1 The TSF shall enforce the [**assignment:** *Role-based Access Control policy*] to restrict the ability to [**selection:** *modify [**assignment:** assign]*] the security attributes [**assignment:** *User Group access list for Metadata Objects*] to [**assignment:** *Data Managers*].

**Application Note:** *this SFR is associated with the Data Managers and SBX Metadata Objects.*

#### 6.1.5.9 Management of security attributes (FMT_MSA.1I)

Dependencies FDP_ACC.1 Subset access control

FMT_SMR.1 Security roles

FMT_SMF.1 Specifications of Management Functions

FMT_MSA.1I.1 The TSF shall enforce the [**assignment:** *Role-based Access Control policy*] to restrict the ability to [**selection:** *modify [**assignment:** assign, recover]*] the security attributes [**assignment:** *User group access list for Data Objects*] to [**assignment:** *Data Managers*].

**Application Note:** *this SFR is associated with the Data Managers and SBX Data Element Objects.*

#### 6.1.5.10 Management of security attributes (FMT_MSA.1J)

Dependencies FDP_ACC.1 Subset access control

FMT_SMR.1 Security roles

FMT_SMF.1 Specifications of Management Functions

FMT_MSA.1J.1 The TSF shall enforce the [**assignment:** *Role-based Access Control policy*] to restrict the ability to [**selection:** *modify [**assignment:** maintain]*] the security attributes [**assignment:** *non-Audit attributes*] to [**assignment:** *Data Manager*].

**Application Note:** *this SFR is associated with the Data Managers and Organization attributes.*

#### 6.1.5.11 Static attribute initialisation (FMT_MSA.3)

Dependencies FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the [**assignment:** *Role-based Access Control policy*] to provide [**selection:** *restrictive*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [**assignment:** *None*] to specify alternative initial values to override the default values when an object or information is created.

#### 6.1.5.12 Management of TSF data (FMT_MTD.1A)

Dependencies FMT_SMR.1 Security roles

FMT_SMF.1 Specifications of Management Functions

FMT_MTD.1A.1 The TSF shall restrict the ability to [**selection:** *modify*] the [**assignment:** *User group access to Metadata Objects*] to [**assignment:** *Data Manager*].

#### 6.1.5.13 Management of TSF data (FMT_MTD.1B)

Dependencies FMT_SMR.1 Security roles

FMT_SMF.1 Specifications of Management Functions

FMT_MTD.1B.1 The TSF shall restrict the ability to [**selection:** *modify, delete*] the [**assignment:** *audit event Fields*] to [**assignment:** *Audit Manager*].

#### 6.1.5.14 Revocation (FMT_REV.1A)

Dependencies FMT_SMR.1 Security roles

FMT_REV.1A.1 The TSF shall restrict the ability to revoke [**assignment:** *Login privileges*] associated with the [**selection:** *Users*] under the control of the TSF to [**assignment:** *SBX System Administrator, User Manager*].

FMT_REV.1A.2 The TSF shall enforce the rules [**assignment:** *Next time a user logs on to the system*].

#### 6.1.5.15 Revocation (FMT_REV.1B)

Dependencies FMT_SMR.1 Security roles

FMT_REV.1B.1 The TSF shall restrict the ability to revoke [**assignment:** *Metadata ACLs and Group assess Fields*] associated with the [**selection:** *Metadata Objects*] under the control of the TSF to [**assignment:** *SBX Metadata Administrator*].

FMT_REV.1B.2 The TSF shall enforce the rules [**assignment:** *Next time the associated Metadata field is accessed*].

#### 6.1.5.16 Revocation (FMT_REV.1C)

Dependencies FMT_SMR.1 Security roles

FMT_REV.1C.1 The TSF shall restrict the ability to revoke [**assignment:** *User Manager Role*] associated with the [**selection:** *Users*] under the control of the TSF to [**assignment:** *SBX User Administrator*].

FMT_REV.1C.2 The TSF shall enforce the rules [**assignment:** *Next time the User Manager attempts to login*].

#### 6.1.5.17 Revocation (FMT_REV.1D)

Dependencies FMT_SMR.1 Security roles

FMT_REV.1D.1 The TSF shall restrict the ability to revoke [**assignment:** *User Group Access at the Organization-Level*] associated with the [**selection:** *[**assignment:** Metadata Objects, Data Element Objects]*] under the control of the TSF to [**assignment:** *Data Manager*].

FMT_REV.1D.2 The TSF shall enforce the rules [**assignment:** *Next time the associated Metadata or Data Element Object field is accessed,*].

#### 6.1.5.18 Revocation (FMT_REV.1E)

Dependencies FMT_SMR.1 Security roles

FMT_REV.1E.1 The TSF shall restrict the ability to revoke [**assignment:** *Organizational roles*] associated with the [**selection:** *Users [**assignment:** User groups]*] under the control of the TSF to [**assignment:** *User Manager*].

FMT_REV.1E.2 The TSF shall enforce the rules [**assignment:** *Next time the associated user attempts to login*].

### 6.1.5.19 Specification of Management Functions (FMT_SMF.1)

Dependencies No dependencies

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [**assignment:** *For SBX System Administrator:*

- *Establish encryption of Data Element Objects;*
- *Maintain Metadata Administration role;*
- *Maintain Enterprise SBX User Administration role;*
- *Establish and maintain organizations;*
- *Management of organization attributes;*
- *Establish audit registry application/location list.*

*For SBX Metadata Administrator:*

- *Establish and maintain Metadata Objects.*

*For SBX User Administrator:*

- *Maintain Initial Organization User Management role.*

*For User Manager:*

- *Maintain Audit Management Role;*
- *Maintain Data Management Role;*
- *Additional User Management Role(s);*
- *Maintain Limited Users;*
- *Maintain User Groups.*

*For Data Manager:*

- *Maintain Organization non-Audit attributes;*
- *Maintain Metadata Object User Group access;*
- *Maintain Data Element Object User Group access.*

*For Audit Manager:*

- *Maintenance of Organization Audit database Attributes;*
- *Maintenance of SBX Audit registry*].

#### 6.1.5.20 Restrictions on security roles (FMT_SMR.2)

Dependencies FIA_UID.1 Timing of identification

FMT_SMR.2.1 The TSF shall maintain the roles: [**assignment:**

- *SBX System Administrator(s);*
- *SBX User Administrator;*
- *SBX Metadata Administrator(s);*
- *User Manager(s);*
- *Data Manager(s);*
- *Audit Manager(s); and*
- *Limited User(s)*].

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

FMT_SMR.2.3 The TSF shall ensure that the conditions [**assignment:** that a user can only have one role] are satisfied.

### 6.1.6 TOE Access (FTA)

#### 6.1.6.1 TOE access history (FTA_TAH.1)

Dependencies No dependencies

FTA_TAH.1.1 Upon successful session establishment, the TSF shall display the [**selection:** *date and time*] of the last successful session establishment to the user.

FTA_TAH.1.2 Upon successful session establishment, the TSF shall display the [**selection:** *date and time*] of the last unsuccessful attempt to session establishment and the number of unsuccessful attempts since the last successful session establishment.

FTA_TAH.1.3 The TSF shall not erase the access history information from the user interface without giving the user an opportunity to review the information.

### 6.1.7 Dependencies

The following tables list the SFRs and their dependencies

| Dependency / SFR | FAU_GEN.1 | FCS_CKM.1‡ | FCS_CKM.4‡ | FDP_ACC.1 | FDP_ACF.1 | FIA_ATD.1 | FIA_UAU.1 | FIA_UID.1 | FMT_MSA.1 | FMT_MSA.3 | FMT_SMF.1 | FMT_SMR.1* | FPT_STM.1‡ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| FAU_GEN.1 | | | | | | | | | | | | | X |

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| FAU_GEN.2 | X | | | | | | | X | | | | | |
| FCS_COP.1 | | X | X | | | | | | | | | | |
| FDP_ACC.1 | | | | | X | | | | | | | | |
| FDP_ACF.1 | | | | X | | | | | | X | | | |
| FIA_AFL.1 | | | | | | | X | | | | | | |
| FIA_ATD.1 | | | | | | | | | | | | | |
| FIA_UAU.1 | | | | | | | | X | | | | | |
| FIA_UID.1 | | | | | | | | | | | | | |
| FIA_USB.1 | | | | | | X | | | | | | | |
| FMT_MSA.1 | | | | X | | | | | | | X | X | |
| FMT_MSA.3 | | | | | | | | | X | | | X | |
| FMT_MTD.1 | | | | | | | | | | | X | X | |
| FMT_REV.1 | | | | | | | | | | | | X | |
| FMT_SMF.1 | | | | | | | | | | | | | |
| FMT_SMR.2 | | | | | | | | X | | | | | |
| FTA_TAH.1 | | | | | | | | | | | | | |

*‡ FPT_STM.1, FCS_CKM.1 and FCS_CKM.4 are dependency not met*
** FMT_SMR.1 is a dependency met by FMT_SMR.2 which is hierarchical to it.*

Table 13 – SFR direct dependencies

#### 6.1.7.1 Dependencies not met

The following dependencies are not met FPT_STM.1, FCS_CKM.1 and FCS_CKM.4.

FPT_STM.1 Reliable time stamps is met by the underlying trusted operating system Microsoft Windows 2003 Server. Though the Operating system is not part of the TOE it is part of the operational environment and is relied upon to provide a reliable time stamps.

FCS_CKM.1 Cryptographic key generation is met by a manual process in accordance with **P.CRYPTO_KEY_MANAGEMENT** where elements of the key are held by three people and at least two are required to key the system.

FCS_CKM.4 Cryptographic key destruction is met by SBX maintaining the key in a non-persistent object in memory during operation. The key is not ever written to any persistent location and is lost (destroyed) if the system fails or is shut down.

### 6.1.8 SFR security requirement rationale

The SFR security requirements rationale provides two elements:

- A tracing that shows which SFRs address which security objectives for the TOE;

- A set of justifications that shows that all security objectives for SBX Enigma™ are effectively addressed by the SFRs.

#### 6.1.8.1 Tracing between SFRs and the security objectives

Table 14 shows the correspondence between security functional requirements and the SBX Enigma™ security objectives.

| | O.ACCESS_CONTROL | O.AUDIT_GENERATION | O.CRYPTOGRAPHY | O.I&A | O.ROLE-BASE_MANAGMENT |
|---|---|---|---|---|---|
| FAU_GEN.1 | | X | | | |
| FAU_GEN.2 | | X | | | |
| FCS_COP.1 | | | X | | |
| FDP_ACC.1 | X | | | | X |
| FDP_ACF.1 | X | | | | X |
| FIA_AFL.1 | | | | X | |
| FIA_ATD.1 | | | | X | |
| FIA_UAU.1 | | | | X | |
| FIA_UID.1 | | | | X | |
| FIA_USB.1 | | | | X | |
| FMT_MSA.1 | X | | | | |
| FMT_MSA.3 | X | | | | |
| FMT_MTD.1 | X | | | | |
| FMT_REV.1 | | | | | X |
| FMT_SMF.1 | | | | | X |
| FMT_SMR.2 | | | | | X |
| FTA_TAH.1 | | X | | | |

Table 14 – Tracing between SFRs and the security objectives

#### 6.1.8.2 Justification that the SFRs represent the security objectives

SBX Enigma™ provides a secure repository for Windows-based applications seeking to manage access to and protect high value data assets. Its security objectives are:

a. **O.ACCESS_CONTROL**;

b. **O.I&A;**

c. **O.ROLE-BASED_MANAGEMENT;**

d. **O.CRYPTOGRAPHY;**

e. **O.AUDIT_GENERATION.**

##### 6.1.8.2.1 O.ACCESS_CONTROL

The objective **O.ACCESS_CONTROL** is addressed by the SFRs **FDP_ACC.1** and **FDP_AFC.1** of the user data protection class, where **FDP_ACC.1** defines the Role-based Access Control policy and **FDP_ACF.1** defines the functions.

The supporting management functions **FMT_MSA.1, FMT_MSA.3** and **FMT_MTD.1** of security management class also support the **O.ACCESS_CONTROL** objective. **FMT_MSA.1** is realised a number of times and addresses the management of security functional behaviour of the different Administrators/Managers. These SFRs are the authority that provides protection of information by limiting the roles of the Administrators/Managers to predefined tasks and functions. **FMT_MSA.3** is the SFRs that limits the range of security attributes for user input to acceptable values. **FMT_MTD.1** enforces the Access Control List (ACL) security by allocating User Group access to the *Data Element* and/or *Metadata Objects*.

##### 6.1.8.2.2 O.I&A

Before a user can gain access to the system they need to identify and authenticate (I&A) themselves. This then determines their role within the system and their access to data. The **O.I&A** objective is addressed by the SFRs **FIA_AFL.1, FIA_ATD.1, FIA_UAU.1, FIA_UID.1** and **FIA_USB.1** of the identification and authentication class and **FTA_TSE.1** of the TOE access class. The FIA, Identification and Authentication functionality class defines the requirements for authentication and the resultant actions if the identification and authentication combination fail. **FIA_AFL.1** defines that the user is locked out if they fail to prove their identity and authenticate themselves. **FIA_ATD.1** ensures that users have a password, are a member of an SBX group and have a SBX Enigma™ role. **FIA_UAU.1** will only authenticate users after they have entered their correct SBX user identity and password. **FIA_UID.1** is the requirement that allows the system to record a successful or failed attempt of users identifying and authenticating themself prior to accessing the system. This is to allow the user to know if somebody has attempted to access the system on their behalf since the last time that they have personally had access to the SBX Enigma™ system. **FIA_USB.1** is the SFR that associates the user with subjects acting on its behalf based on the user's group membership and role.

#### 6.1.8.2.3 O.ROLE-BASED_MANAGEMENT

Users of the system have been categorised as administrators, managers or limited users. The Administrators/Managers have distinct roles and responsibilities in establishing, operating, and maintaining the system. The objective **O.ROLE-BASE_MANAGEMENT** is addressed by the SFRs **FDP_ACC.1**, **FDP_ACF.1, FMT_REV.1, FMT_SMF.1** and **FMT_SMR.2** of the security management functionality class. The **FDP_ACC.1** and **FDP_ACF.1** addresses the functionality that roles have and to the data type objects to which they have access. **FMT_REV.1** lists the functionality that the Administrators/Managers of an SBX Enigma™ system can revoke. **FMT_SMF.1** defines the specifications of the management roles, while **FMT_SMR.2** defines the restrictions on the roles.

#### 6.1.8.2.4 O.CRYPTOGRAPHY

**O.CRYPTOGRAPHY** is addressed by the SFR **FCS_COP.1** of the cryptographic support functionality class. Persistent data that is saved to hard disc memory and other such devices is protected by being encrypted in accordance with the Advanced Encryption Standard (AES) with a 256 bit key.

#### 6.1.8.2.5 O.AUDIT_GENERATION

**O.AUDIT_GENERATION** is addressed by the SFRs **FAU_GEN.1** and **FAU_GEN.2** of the security audit functionality class and **FTA_TAH.1** of the TOE access class. The audit objective to create audit events of security relevant activities are associated with **FAU_GEN.1** which define that start-up, shutdown and all SBX Administrator events are mandatory audit events. It also includes a list of events related to specific auditable SFRs. Users are made accountable for their actions in accordance with **FAU_GEN.2** where the identity of each user that has caused the event is recorded.

**FTA_TAH.1** provides a supporting security audit function by allowing the user to know the last time that they have successfully established a session, logged-on and any failed attempts since that log-on. This information is only displayed after they have successfully logged-on.

## 6.2 Security assurance requirements

The Security Assurance Requirements (SAR) are drawn from the Common Criteria for Information Technology Security Evaluation, Part 3, Version 3.1, Release 2 dated September 2007, CCMB-2007-09-003 which define the EAL 2 requirement with the additional SAR ALC_FLR.1 Basic flaw remediation (EAL 2+).

The following is a list of the assurance requirements needed for EAL 2+.

| Assurance Class | Assurance Components | |
|---|---|---|
| Development | ADV_ARC.1 | Security architecture description |
| | ADV_FSP.2 | Security-enforcing functional specification |
| | ADV_TDS.1 | Basic design |
| Guidance documents | AGD_OPE.1 | Operational user guidance |

| Assurance Class | Assurance Components | |
|---|---|---|
| | AGD_PRE.1 | Preparative procedures |
| Life-cycle support | ALC_CMC.2 | Use of a CM system |
| | ALC_CMS.2 | Parts of the TOE CM coverage |
| | ALC_DEL.1 | Delivery procedures |
| | ALC_FLR.1 | Basic flaw remediation |
| Security Target evaluation | ASE_CCL.1 | Conformance claims |
| | ASE_ECD.1 | Extended components definition |
| | ASE_INT.1 | ST introduction |
| | ASE_OBJ.2 | Security objectives |
| | ASE_REQ.2 | Derived security requirements |
| | ASE_SPD.1 | Security problem definition |
| | ASE_TSS.1 | TOE summary specification |
| Tests | ATE_COV.1 | Evidence of coverage |
| | ATE_FUN.1 | Functional testing |
| | ATE_IND.2 | Independent testing sample |
| Vulnerability assessment | AVA_VAN.2 | Vulnerability analysis |

Table 15 – Assurance Requirements

### 6.2.1 SAR security requirements rationale

SBX Enigma™ requires an EAL2+ level of assurance to provide security within a commercial grade Service Orientated Architecture. As EAL2+ provides assurance by a full security target and an analysis of the SFRs in that ST, using a functional and interface specification, guidance documentation and a basic description of the architecture of SBX Enigma™ to understand the security behaviour.

The evaluation analysis is supported by independent testing of the TSF by the AISEF, evidence of Eaglehawk testing based on the functional specifications, selective independent confirmation of the test results and a vulnerability analysis (based upon the functional specification, the SBX Enigma™ design and the guidance evidence) to demonstrate resistance to penetration attackers with a basic attack potential.

Assurance is also provided through the use of a configuration management system and evidence of secure delivery procedures.

An EAL2+ level of assurance is applicable to SBX Enigma™ where the end users require a low to moderate level of independently assured security.

## 6.3 Security requirements: conclusion

The security problem definition of SBX Enigma™ as defined in section 3 consists of threats, OSPs and assumptions. In the security objectives section 4, the solution is provided in the form of two sub-solutions:

- security objectives for the TOE;
- security objectives for the operational environment.

Additionally, a security objectives rationale is provided showing that if all security objectives are achieved, the security problem is solved: all threats are countered, all OSPs are enforced, and all assumptions are upheld.

In the security requirements section 6.1, the security objectives for the TOE are translated to SFRs and a security requirements rationale is provided showing that if all SFRs are satisfied, all security objectives for the TOE are achieved.

Additionally, a set of SARs is provided to show how the TOE is evaluated, together with an explanation for selecting these SARs.

All of the above can be combined into the following statement: If all SFRs and SARs are satisfied and all security objectives for the operational environment are achieved, then there exists assurance that the security problem as defined in section 3 is solved: all threats are countered, all OSPs are enforced, and all assumptions are upheld. This is illustrated in Figure 7.

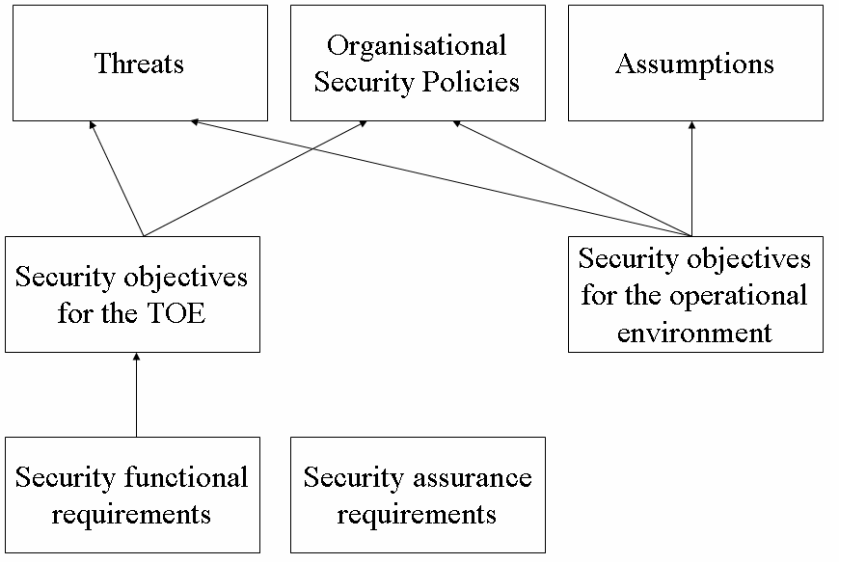


Figure 7 – Relations between the security problem definition, the security objectives and the security requirements

The amount of assurance obtained is an evaluation assurance level of EAL2+.

# 7 TOE Summary Specification

SBX Enigma™ is an in-memory object-oriented data management system providing security functionality for multi-user distributed data environments such as Service Orientated Architecture (SOA) information management systems.

It provides security at the boundaries of the system with the identification and authentication mechanism. Users' access is restricted on a need-to-know basis by a fine-grained access control functions. The system management has been segregated to specific tasks and roles and is conducted by the SBX Administrators and Managers. The system is monitored by an audit system that monitors all administration activities and selected custom application activities.

This TOE summary specification describes how it satisfies the SFRs by correlating them to the security mechanisms that implements them. The SFRs provide a semi-formal method of describing the system security functionality.

## 7.1 Identification and Authentication Functionality

The following SFRs have been included to describe the identification and authentication functionality.

FIA_AFL.1 Authentication failure handling – failure of authentication is set as part of the Organization attributes. The number of failed attempts, 1 to 9, before lock out is defined by either the SBX System Administrator or the Data Manager.

FIA_ATD.1 User attribute definition – the attributes required by each administrator/user before they can log onto and get access to the system are their user identification and password. These attributes are confirmed by the SBX Organization before the user gains access to any system functionality.

FIA_UAU.1 Timing of authentication – the SBX Enigma™ confirms the user's identity before they can be authenticated. This allows the Organization to track if an administrator/user has attempted to logon numerous times before succeeding. Or if a threat agent is trying to attempt a brute-force attack to determine an administrator/users password.

FIA_UID.1 Timing of identification – the only action that is allowed before the user identity is confirmed by SBX Enigma™ is a request for an account by a potential new user.

FIA_USB.1 User subject binding – this SFR binds the User Group access lists to object ACLs and administrator/user roles. The SFR has been implemented within SBX Organizations.

## 7.2 Role-base Management Functionality

The following SFRs have been included to describe the role-base management functionality.

FDP_ACC.1 Subset access control – the Role-Based access control functionality has been met by the fine-grained access control to the Metadata and Data Element

Objects. This is implemented by the ACLs and the User Groups that define what access is restricted to specific roles.

FDP_ACF.1 Security attribute based access control – this SFR defines how the role-based access control policy is implemented on all user/administrators, all roles and all objects (organization, metadata and data). It has been implemented within all parts of the SBX Enigma™ system.

FMT_REV.1 Revocation – this SFR also has a number of iterations for the different roles and different objects that can be revoked. They have been implemented by the associated role changing the attributes of the relevant object (User/User group/ACL).

FMT_SMF.1 Specification of management functions – the specification of management functions is correlated to administrator/user roles and has been defined in accordance with the type of function. If the function relates to the metadata it is implemented within the Metadata Object. If it is related to the data it is implemented within the Data Element Object. If it is a system type function it is implemented at the Organization level.

FMT_SMR.2 Restrictions on security roles – the roles of the system are defined within this SFR and the fact that a user can only have one role is a major concept of SBX Enigma™. This has been implemented within Organizations and is closely related to the identification and authentication functions.

## 7.3 Access Control Functionality

The following SFRs have been included to describe the access control functionality.

FDP_ACC.1 Subset access control – the access control functionality has been met by the access control to the Metadata and Data Element Objects. This is implemented by the ACLs and the User Groups that define what access is restricted to specific roles.

FDP_ACF.1 Security attribute-based access control – this SFR defines how the role-based access control policy is implemented on all user/administrators, all roles and all objects (organization, metadata and data). It has been implemented within all parts of the SBX Enigma™ system.

FMT_MSA.1 Management of security attributes – security functions have security attributes that can be created, modified, deleted and maintained. These have been implemented at the Organization level of the SBX Enigma.

FMT_MSA.3 Static attribute initialisation – the security attributes have default initial values that cannot be changed until after an object is created. These have been implemented within the Organization and are Organization attributes.

FMT_MTD.1 Management of TSF data – this SFR defines how and who can modify the TSF security attributes and relates to Metadata Objects and “audit registers list of events” that have been implemented within the Enterprise level of the SBX Enigma™ system.

## 7.4 Secure Data Storage Functionality

The following SFRs have been included to describe the cryptographic functionality.

FCS_COP.1 Cryptographic operation – is a functionality that occurs in the background and results in the Enterprise encrypting all data held in data element objects that are saved to disc. It uses the AES 256 bit encryption standard implemented in accordance with FIPS197. It is implemented at the lowest level of the SBX Enigma™ system.

## 7.5 Security Audit Functionality

The following SFRs have been included to describe the security audit functionality.

FAU_GEN.1 Audit data generation – generation of audit data occurs within the Organization and Enterprise levels of the system. All administration events are audited as a mandatory requirement. Client Application events are audited as defined by the audit manager.

FAU_GEN.2 User Identification association – recording of user/administrator identity occurs for all audit events and it is also implemented within the Organization and Enterprise levels of the SBX Enigma™ system.

FTA_TAH.1 TOE access history – is a discrete audit event and informs the user/administrator the last time that they accessed the system. It is implemented in conjunction with the FID_UID SFR which ensures that the system recognises the user/administrator before they have been authorised to access the system.