Secure Objects incorporating Secure Envelopes

Security Target

Common Criteria: EAL4 augmented with ALC_FLR.1

Document ID: SO 0074 EN

Version 1.3

March 2011

Document History

Version	Date	Author	Description
1.0	30-NOV-10	Cocoon Data	Initial release.
1.1	09-FEB-11	Cocoon Data	Updated to reflect correct TOE component build numbers.
1.2	14-FEB-11	Cocoon Data	Consistency updates.
1.3	02-MAR-11	Cocoon Data	Updated to address certifier comments.

Table of Contents

List of Tables

List of Figures

1 Security Target Introduction

1.1 TOE overview

1 The Target of Evaluation (TOE), Secure Objects incorporating Secure Envelopes – Enterprise Version, is an encryption-based access control system for protecting the confidentiality and integrity of electronic files. Secure Objects controls and monitors the exchange of digital files based on recipient identity, to protect against the deliberate or unintentional release of sensitive user data.

2 The TOE includes both client software (Secure Envelopes) and a central enterprise server (Secure Objects). The client software provides the Creator with the interface that enables them to create "secure objects" containing data files or any type of user data (attachments). The client software also provides the interface to the recipient allowing them to open and access the contents of a secure object. The central server provides an enterprise security management platform that provides an ongoing capability for centralised control of created envelopes, key management and object access auditing.

3 Once Secure Objects incorporating Secure Envelopes has been implemented within the enterprise any document owner can create a secure object to secure and control specified electronic files. Data files secured within a secure object can then be controlled throughout the life of that secure object- the Creator has the ability to dynamically control which recipients may open a secure object and access data files contained.

4 Secure Objects incorporating Secure Envelopes' security model ensures the secrets needed to decrypt an envelope are never physically distributed with the secure object. Decryption secrets are only available to the Secure Envelopes software once a user has electronically authenticated their identity. Secure objects can be copied, forwarded or burned on CD as easily as any other digital document. They cannot be opened unless the recipient has the proper identity credential determined by the Creator of the secure object.

5 As illustrated in Figure 1, Secure Objects incorporating the Secure Envelopes client provide a highly flexible and secure method for distributing and controlling data files within the enterprise.

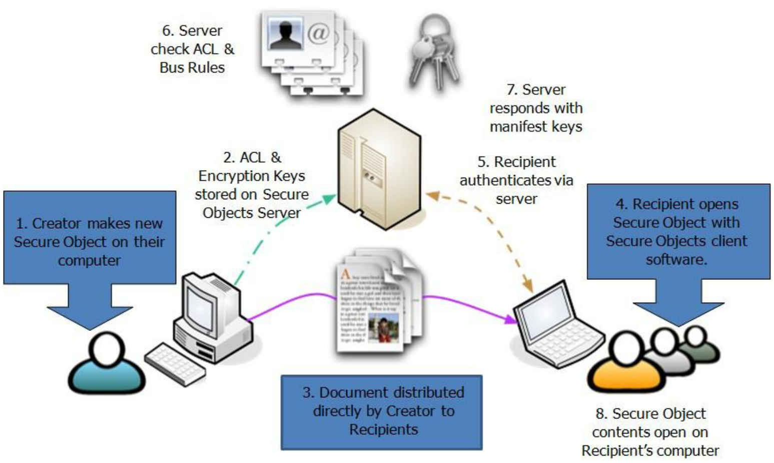
6. Server check ACL & Bus Rules
7. Server responds with manifest keys
2. ACL & Encryption Keys stored on Secure Objects Server
5. Recipient authenticates via server
1. Creator makes new Secure Object on their computer
4. Recipient opens Secure Object with Secure Objects client software.
3. Document distributed directly by Creator to Recipients
8. Secure Object contents open on Recipient's computer

Figure 1 – The secure object creation process

1.2 TOE security features

6 Table 1 highlights the range of security functions and features implemented by the Secure Objects incorporating Secure Envelopes product.

Table 1 – TOE security functions and features

Security function	Security feature
Data protection. The TOE provides the capability to protect user and TOE Security Function (TSF) data both at rest and in transit.	**Object protection.** The TOE has the ability to encrypt data files to provide protection whilst being transmitted and also at rest.
	Trusted communications path. The Secure Envelopes client provides a trusted communications path via an SSL encrypted tunnel to the Secure Objects Enterprise Server for securely transmitting TSF data such as audit records and encryption keys.
Object access audit. The TOE provides the capability to capture audit records for events of interest.	**Generation of audit records.** The TOE has the capability to generate and centrally store audit records for events of interest that relate to actions performed on a secure object.
	Audit review. The TOE provides the Creator of a secure object the ability to review audit records generated and captured as a result of actions being performed on a secure object.
Object control. The TOE has inbuilt security mechanisms to provide controlled access to secure objects.	**User identification and authentication.** The TOE has the capability to issue one-time passwords to specified recipient emails to provide a method for identifying and authenticating users.
	Controlled access. The TOE has the capability to allow the Creator of a secure object to control access to the secure object and contained attachments.
Security management. The TOE provides the capability to manage the system and secure objects through a set of clearly defined roles.	**Defined roles.** The TOE maintains a set of security-related roles: Super Administrator, Administrator, Creator, Manager & Recipient that enable the secure management of the Secure Objects system.
	Object management. The TOE permits Creators and Managers to continue to manage secure access rights and controls that pertain to a specific secure object and contained attachments.
	Centralised key management. The TOE provides a centralised key management capability that distributes and manages keys separately outside user data.

1.3 ST and TOE identification

Table 2 – ST and TOE identification information

ST Title	Secure Objects incorporating Secure Envelopes Security Target
ST Version	1.3, 2-MAR-11
TOE Software	Secure Objects incorporating Secure Envelopes, version 1.5.1. The specific build number of the TOE components includes: • Auth Server component: build 1.5.1.6 • All other components: build 1.5.1.5[1]
Assurance Level	EAL4 augmented with ALC_FLR.1
CC Identification	Common Criteria for Information Technology (IT) Security Evaluation, Version 3.1, July 2009, incorporating: • Part One – Introduction and General Model, Revision Three, July 2009; • Part Two – Security Functional Components, Revision Three, July 2009; and • Part Three – Security Assurance Components, Revision Three, July 2009. International Standard – International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 15408:1999.

1.4 Conformance Claims

7 The following conformance claims are made for the TOE and ST:

a) **Part 2 conformant.** Conformant with Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, version 3.1, July 2009.

b) **Part 3 augmented.** Conformant with Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, version 3.1, July 2009. Evaluation is EAL4 augmented with ALC_FLR.1.

1.5 Document conventions

8 Part 2 of the Common Criteria defines an approved set of operations that may be applied to security functional requirements. Following are the approved operations and the document conventions that are used within this ST to depict their application:

a) **Assignment.** The assignment operation provides the ability to specify an identified parameter within a requirement. Assignments are depicted using bolded text and are surrounded by square brackets as follows [**assignment**].

[1] Procedures to validate the build number for each TOE component is included in both the Preparative Procedures and Operational Procedures guidance documents.

b) **Selection.** The selection operation allows the specification of one or more items from a list. Selections are depicted using bold italics text and are surrounded by square brackets as follows [***selection***].

c) **Refinement.** The refinement operation allows the addition of extra detail to a requirement. Refinements are indicated using bolded text, for **additions**, and strike-through, for ~~deletions~~.

d) **Iteration.** The iteration operation allows a component to be used more than once with varying operations. Iterations are depicted by placing a letter at the end of the component identifier as follows FDP_IFF.1a and FDP_IFF.1b.

1.6 Terminology

Table 3 – Terminology

Term	Description
Administrator	Role with privileged access rights to provide central administration and management for the Secure Objects Enterprise Server.
Admin Server	A component of the Secure Objects Enterprise Server that provides a web interface used by Administrators to review logs and to administer users and groups.
Attachment	Any file added by the Creator to a Secure Object.
Authorisation Code	Server generated one-time passcode (OTP) sent to an email address. Authorisation codes are used to authenticate all users of the TOE.
Auth Server	A major component of the Secure Objects Enterprise Server that provides the identification, authentication and authorisation functionality for the TOE for Creator and Recipient users.
Creator	Role with access permitting the creation of secure objects.
Gatekeeper Server	A component of the Secure Objects Enterprise Server that provides session management for the TOE.
Group	A collection of users as defined by an Administrator. Used to simply granting the Manager role to users.
Manager	Roles with access permitting the management of secure objects, notably the ability to grant and revoke access to a specific secure object and its contained attachments.
Manager Server	A component of the Secure Objects Enterprise Server that provides a web interface used by Managers and Creators to review logs, and modify access controls for previously created secure objects.

Term	Description
Recipient	Role which permits the access to a specific secure object and one or more contained attachments.
RNG Server	A server component that provides random number generation (RNG) functionality for use by the Secure Objects Enterprise Server.
Secure Envelope	The framework used by the Secure Envelopes application to create a secure object.
Secure Envelopes	The title of the client software that provides an interface to the end-users (Creators and Recipients).
Secure Object	The resultant data file generated by a Creator using the Secure Envelopes application, containing one or more attachments (contained files). The secure object data file has a .senv filename extension.
Secure Objects Enterprise Server	The title of the server components of the Secure Objects system.
Super Administrator	Role with privileged access to grant, revoke and manage Administrator access.
Super Admin Server	A component of the Secure Objects Enterprise Server that provides a web interface used by Super Administrators to review logs and to manage Administrator accounts.
Template Server	Component of the Secure Objects Enterprise Server which is used to store and manage templates used to customise the display of a specific Secure Envelopes client.

1.7 Document organisation

9 This document is organised into the following sections:

a) Section 1 provides the introductory material for the ST.

b) Section 2 provides the TOE description and includes the physical and logical scope of the TOE.

c) Section 3 describes the expected environment for the TOE. This section also defines the set of threats that are to be addressed by either the technical countermeasures implemented within the TOE or through environmental controls.

d) Section 4 defines the security objectives for the TOE and environment.

e) Section 5 contains the functional and assurance requirements derived from the Common Criteria, Part 2 and 3, respectively that must be satisfied by the TOE.

f) Section 6 provides a summary of the TOE specification, identifying the IT security functions provided by the TOE and also the assurance measures designed to meet the assurance requirements.

g) Section 7 provides a rationale to explicitly demonstrate that security objectives have been satisfied by the TOE.

2 TOE Description

2.1 TOE type and usage

10 The TOE is a data protection product that provides confidentiality and integrity controls for user data while in transit and at rest. The TOE also provides mechanisms for protecting TSF data through a separate communications channel that provides client connectivity to an enterprise server.

11 The TOE has been designed for three main methods of use:

a) **Secure Transmission of documents.** The TOE provides a framework for the transmission of documents, both within an organisation and to third parties.

b) **Connecting remote enterprise user.** The TOE can be used to provide a method for remote users to protect user data that has to be communicated with other remote users or with users contained within the enterprise environment.

c) **Providing an enclave environment within the enterprise.** The TOE can also be used for protecting user data within the enterprise. This method of use is popular for those organisations that have specifically sensitive information that only a limited amount of people within the organisation may need to access or communicate. The TOE can be established on an existing enterprise network whilst still providing the necessary data protection and separation.

12 The TOE has been designed for deployment in either a traditional enterprise model whereby all server components exist within the boundaries of the enterprise network, or through a Software-as-a-Service (SaaS) type deployment. The latter employing the use of externally hosted and managed server TOE components, with the enterprise managing only the client component of the TOE.

2.2 Physical scope of the TOE

2.2.1 TOE Components

13 The TOE consists of three components:

a) Secure Envelopes Client;

b) Secure Objects Enterprise Server (made up of Administrator, Gatekeeper, Auth, Manager, Super Administrator and Template Server components); and

c) The RNG Server.

14 Details of the operating requirements of the TOE are provided in the following sections.

2.2.2 User environment

15 The Secure Envelopes client software is installed locally on a user’s laptop or desktop system. The client software requires specific hardware and software components for all features to be installed and to execute correctly:

a) **Hardware.** Standard personal or multimedia computer with any modern processor.

b) **Memory.** A minimum of 256 MB of Random Access Memory (RAM) available for use by the operating system, Secure Envelopes and the optional email application.

c) **Hard disk.** Secure Envelopes requires approximately 5 MB of hard disk space for installation.

d) **Operating system.** Microsoft Windows XP, Windows Vista or Windows 7.

e) **Additional software.** Besides requiring the operating system, the Secure Envelopes client also requires that users have the Microsoft .NET framework (version 2.0 or greater) as well as an email program installed.

f) **Email account.** The user requires access to an email account in order to receive authentication codes from the Secure Objects Enterprise Server.

2.2.3 Enterprise environment

16 The Secure Objects Enterprise and RNG Servers exist within the enterprise environment along with a number of other components required to support the Secure Objects incorporating Secure Envelopes solution. The requirements for each are:

2.2.3.1 Secure Objects Enterprise Server.

17 The Secure Objects Enterprise Server has six software components (Administrator, Gatekeeper, Auth, Manager, Super Administrator and Template Server) that can co-exist on the one server, or can also be installed on separate server hardware. The requirements for each server component are detailed below:

a) **Hardware.** Standard server with any modern processor.

b) **Memory.** A minimum of 256 MB of Random Access Memory (RAM) for each component.

c) **Hard disk.** 6 MB of disk space for each component.

d) **Operating system.** Linux or Windows based operating system.

e) **Additional software.** The following software is required for each server hosting a Secure Objects Enterprise Server component:

i) Java application server; and

ii) Java runtime environment.

2.2.3.2 RNG Server

f) The Random Number Generator (RNG) server is a Java based service supported by a set of Java Archives and shared object files which implement the cryptographic key and random number generation capabilities. The RNG server components can be installed on the same server as the Secure Objects Enterprise Server, or on a separate server within the enterprise environment.

18 The requirements for the RNG Server are detailed below:

a) **Hardware.** Standard server with any modern processor.

b) **Memory.** A minimum of 256 MB of Random Access Memory (RAM).

c) **Hard disk.** 6 MB of disk space.

d) **Operating system.** Linux operating system.

e) **Additional software.** The following software is required:

i) Java runtime environment.

2.2.3.3 PostgreSQL database server

19 The enterprise environment must provide a PostgreSQL database server that can be used by the Secure Objects Enterprise Server to store role, authorisation, audit records and cryptographic key information.

2.2.3.4 SMTP server

20 The enterprise environment must provide a Simple Mail Transfer Protocol (SMTP) server for use by the Secure Objects Enterprise Server. The SMTP server is used to email one-time passwords (OTPs) to users when they required authentication.

2.2.4 Network environment

21 Active network connectivity needs to be maintained between the Secure Envelopes client and the Secure Objects Enterprise Server to provide the capability to transmit audit records and encryption keys. To support this, a routable IP address must be assigned to the server(s) hosting the Secure Objects Enterprise Server components. Additionally, the enterprise boundary firewall must be capable of accepting HTTPS connections (TCP port 443) to enable users with the Secure Envelopes client to contact each of the server components.

22 Additionally, within the enterprise environment, active network connectivity is required between all Secure Objects Enterprise Server components, the RNG server, database server and SMTP server.

2.3 Logical scope of the TOE

As illustrated in

23 Figure 2, the TOE is comprised of the Secure Objects Enterprise Server, RNG Server and the Secure Envelopes client.

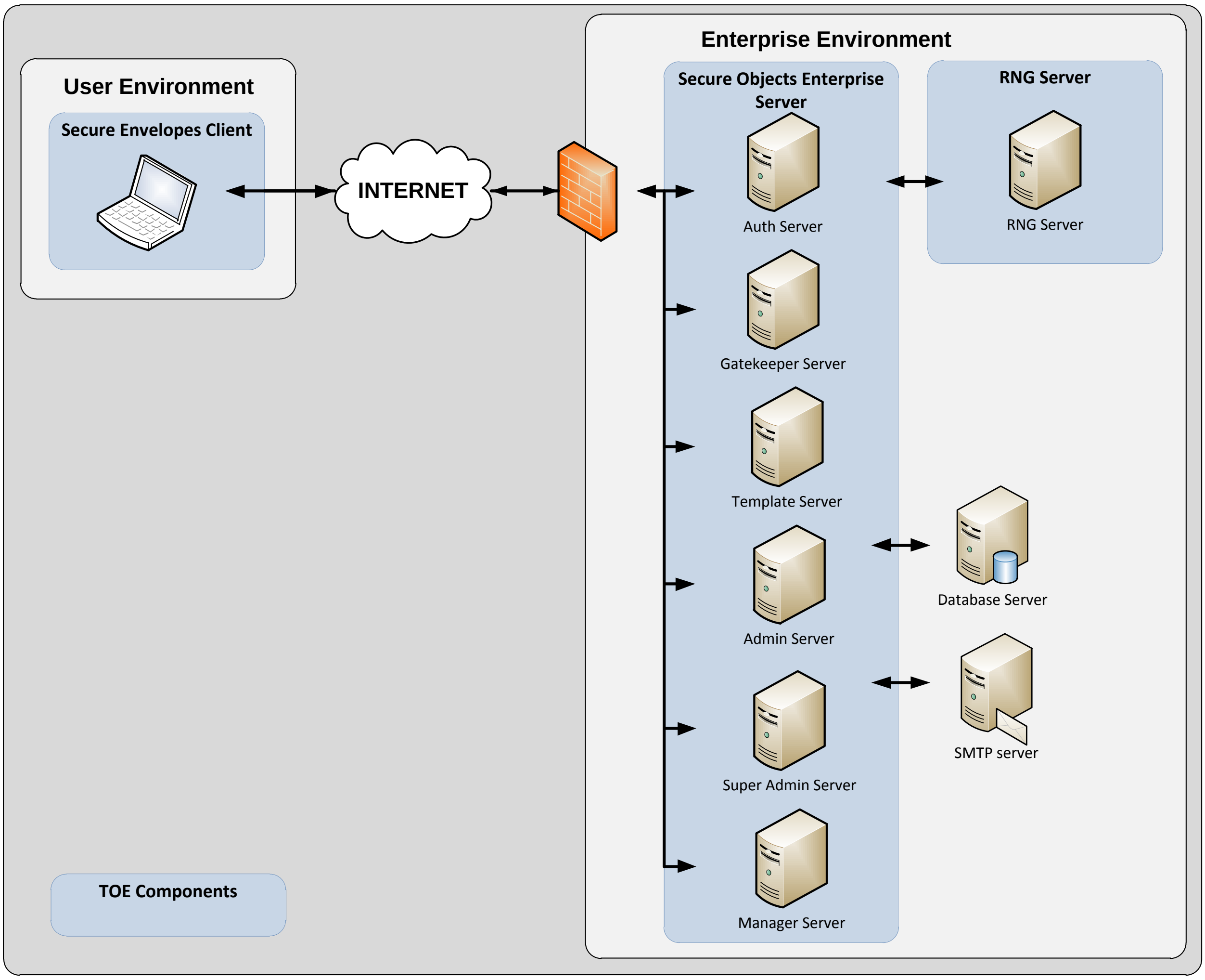

Figure 2 – Major components of the TOE

2.3.1 Secure Envelopes Client

24 The Secure Envelopes TOE component is comprised of four modules as illustrated in Figure 3; the user interface, core, cryptography shim and cryptography.

a) **User interface**. The user interface provides the interface for users of Secure Envelopes as well as connectivity into the core and cryptography components. The user interface is implemented as SecEnv.exe.

b) **Core**. The core provides the main functionality for Secure Envelopes including display and workflow functions, email contact integration, exception handling, communication with the Secure Objects Enterprise Server, application of templates, the reading and writing of secure objects as well as maintaining general settings. The core is implemented as SecObjCore.dll.

c) **Cryptography Shim**. The Cryptography Shim subsystem is a small set of wrapper functions. The purpose of the Cryptography Shim is to exist as an intermediary between the Cryptography component and the Secure Envelopes User Interface. The cryptography Shim is implemented as cli.dll.

d) **Cryptography**. The cryptography component provides functionality to the core to enable the use of cryptographic keys received from the Secure Objects Enterprise Server to either encrypt or decrypt a secure object or the attachments contained within. The cryptography component is implemented as cpp.dll.

25 Secure Envelopes integrates with three application program interfaces (APIs) to provide integration within the underlying operating system, as well as additional functionality. These APIs include Google Mail, Outlook Address and Microsoft .NET. Of these APIs, only Microsoft .NET is a mandatory requirement for the operation of Secure Envelopes. The Google Mail and Outlook Address APIs are required only if the user wishes for Secure Envelopes to directly integrate with either Google Mail or Microsoft Outlook. All of these APIs are outside of the scope of the TOE.

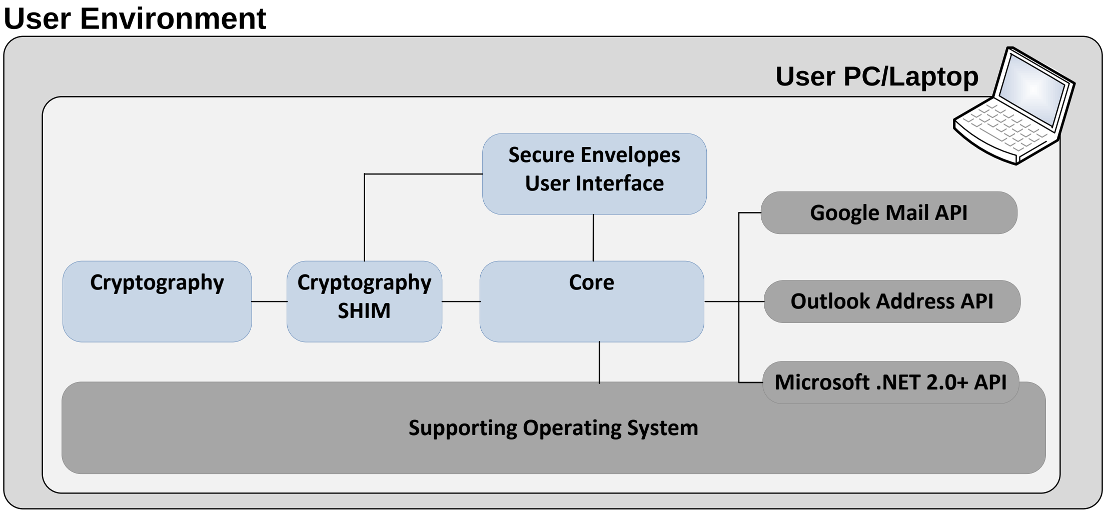

Figure 3 - Secure Envelope TOE Components

2.3.2 Secure Objects Enterprise Server

26 The Secure Objects Enterprise Server TOE component is comprised of eight modules as illustrated in Figure 4 and described below.

a) **Gatekeeper Server.** Provides session management for all connections with Secure Envelopes clients. Also includes routing and client software version features.

b) **Auth Server.** Provides the mechanisms for identifying users, generating and validating authentication codes and authorising users. Also provides the cryptographic functionality for the TOE by generating encryption keys and general key management for the Secure Envelopes capability.

c) **Template Server.** Provides content to customise the Secure Envelopes client display specific to the individual enterprise.

d) **Admin Server.** Provides the central security management capability for the TOE for Administrators, delivered as a web-based service. This service is used by Administrators to manage user groups and rights, as well as to view security logs.

e) **Super Admin Server.** Provides the central security management capability for the TOE for Super Administrators, delivered as a web-based service. This service is used by Super Administrators to manage Administrator accounts, as well as to view security logs.

f) **Manager Server.** Provides the central security management capability for the TOE for Creators and Managers, delivered as a web-based service. This service is used by Creators and Managers to manage previously created secure objects, as well as to view security logs.

g) **Data Library.** Provides common utilities and database integration functions to each of the web services.

h) **Web Library.** Provides common web functions to the Manager, Admin and Super Admin servers.

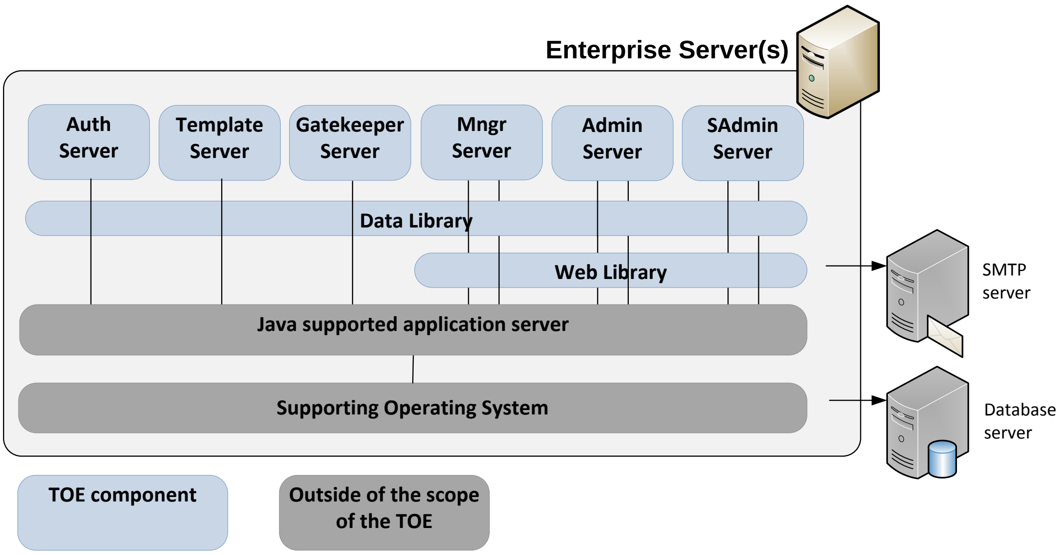

Figure 4 - Secure Objects Enterprise Server TOE Components

2.3.3 RNG Server

27 The RNG TOE component is comprised of six modules which are installed from a single RPM package. The RNG Server requires a Java Virtual Machine to support the operation of these six modules which collectively provide random number and cryptographic key generation capabilities required by the Secure Objects Enterprise Server.

3 Security problem definition

3.1 Overview

28 This section describes the nature of the security problem that the TOE is designed to address. The security problem is described through assumptions about the security aspects of the environment and any threats to the assets that the TOE will be providing protection.

3.2 Assumptions

Table 4 – Assumptions

Identifier	Assumption statement
A.USAGE	Users are trusted to: • follow user guidance, • ensure that files extracted from secure envelopes are not disclosed and distributed, and • ensure that the TOE continues to operate in the evaluated configuration.
A.IT_ENTERPRISE	The Secure Objects Enterprise Server and RNG Server are located within the enterprise boundary and are protected from unauthorized logical access.
A.ADMIN	The Administrator (and Super Administrator) is not careless, wilfully negligent, or hostile, and will follow and abide by the instructions provided by administrator documentation.
A.ENTERPRISE	The Secure Objects Enterprise Server and RNG Server are protected from unauthorized physical access.
A.COMMS	There exists active network connections between: • the Secure Envelopes client and the Secure Objects Enterprise Server, • the Secure Objects Enterprise Server and RNG Server, • the Secure Objects Enterprise Server and SMTP Server, and • the SMTP Server, any intermediary SMTP servers and the Secure Envelopes client.
A.COMMS_SECURE	The communications between the Secure Objects Enterprise Server and both the database and SMTP Server is secure. The communications between the SMTP Server and any intermediary SMTP servers is secure.

Identifier	Assumption statement
A.OS	The operating systems supporting the TOE components protect against the unauthorized access, modification or deletion of the individual TOE components that they host.
A.TIME	The Secure Objects Enterprise Server is provided with a reliable time source.
A.SECRET	The Java application server supporting the Secure Objects Enterprise Server provides a random alphanumeric character generator that may be used by the Secure Objects Enterprise Server to generate one-time passcodes.

3.3 Threats to security

Table 5 – Threats to security

Identifier	Threat statement
T.USERDATA_COMM	An attacker may compromise the confidentiality and/or integrity of user data by monitoring communications between the creator and recipient.
T.USERDATA_REST	An attacker may compromise the confidentiality and/or integrity of user data by gaining direct physical or logical access to a data file of either the creator or recipient.
T.TSFDATA	An attacker may compromise the confidentiality and/or integrity of enterprise TSF data by monitoring and/or actively modifying communications between users and the Secure Objects Enterprise Server.
T.ROLES	A user may attempt to access or delete user data that they are not allowed to.
T.MANAGEMENT	A user may attempt to make modifications to security policy settings in an attempt to gain unauthorised access to user data.

3.4 Organisational Security Policies

29 Organisational Security Policies (OSPs) are a set of rules, procedures, or guidelines imposed by an organisation that are to be enforced by the TOE and it Organisational environment to address its security needs.

Table 6 – Organisational Security Policies

Identifier	Assumption statement
OSP.ACCOUNTABLE	The authorised user of the TOE shall be held accountable for their actions within the TOE.

4 Security objectives

4.1 Overview

30 The security objectives are concise statements of the TOE's response to the security problem. Some objectives are to be achieved through the security functionality of the TOE and some elements of the problem will be addressed through the establishment of a secure environment in which the TOE must operate.

4.2 Security objectives for the TOE

Table 7 – Security objectives for the TOE

Identifier	Objective statement
O.USRDATA_COMM	The TOE shall preserve the confidentiality and integrity of user data transmitted between Creators and Recipients.
O.USRDATA_REST	The TOE shall preserve the confidentiality and integrity of user data stored by Creators and Recipients.
O.TSFDATA	The TOE shall preserve the confidentiality and integrity of TSF data transmitted between the Secure Envelopes Client and the Secure Objects Enterprise Server.
O.AUDIT	The TOE shall be capable of capturing audit records for all events of interest associated with accessing Secure Objects.
O.USER_AUTH	The TOE shall prevent users from gaining access to TOE functions or user data prior to authentication.
O.ROLES	The TOE will maintain a number of roles to distinguish access to functions of the TOE.
O.MANAGEMENT	The TOE shall be capable of having security policy settings defined by an Administrator or Super Administrator, which cannot be modified or overwritten by end users.

4.3 Security objectives for the IT environment

Table 8 – Security objectives for the IT environment

Identifier	Objective statement
OE.IT_ENTERPRISE	The IT environment must ensure that the Secure Objects Enterprise Server and RNG Server are located within the enterprise boundary and are provided with logical access controls to prevent unauthorised access.
OE.COMMS	The IT environment must provide active network connections between the Secure Envelopes client and the Secure Objects Enterprise Server, the Secure Objects Enterprise Server and RNG Server, the Secure Objects Enterprise Server and SMTP Server, and the SMTP Server, any intermediary SMTP servers and the Secure Envelopes client.
OE.COMMS_SECURE	The IT environment must provide secure communications between the Secure Objects Enterprise Server and both the database and SMTP servers, as well as between the SMTP Server and any intermediary SMTP servers[2].
OE.OS	The IT environment must provide protection of the components of the TOE from unauthorized access, modification or deletion, implemented by the operating systems supporting the TOE components.
OE.TIME	The IT environment must provide a reliable time service for the Secure Objects Enterprise Server, implemented by the operating system supporting the Secure Objects Enterprise Server.
OE.SECRET	The Java application server supporting the Secure Objects Enterprise Server must provide a random alphanumeric character generator, accessible by components of the Secure Objects Enterprise Server which can be used to generate random 16 character, alphanumeric one-time passwords

4.4 Security objectives for the non-IT environment

Table 9 – Security objectives for the non-IT environment

Identifier	Objective statement

[2] Securing communications between SMTP servers may be achieved through the implementation and enforcement of Transport Layer Security (TLS).

OE.USAGE	The Administrator shall ensure that all users are aware of the need to: • follow user guidance, • ensure that files extracted from secure envelopes are not disclosed and distributed; and • ensure that the TOE continues to operate in the evaluated configuration.
OE.ENTERPRISE	The Administrator shall ensure that the Secure Objects Enterprise Server and RNG Server are protected from unauthorised physical access.
OE.ADMIN	The Administrator (and Super Administrators) shall not be careless, wilfully negligent, or hostile, and shall follow and abide by the instructions provided by the administrator documentation.

5 IT security requirements

5.1 Overview

31 This section defines the security requirements satisfied by the TOE. Each requirement has been extracted from version 3.1 of the Common Criteria, part 2 providing functional requirements and part 3 providing assurance requirements.

5.2 TOE security functional requirements

32 This section contains the security functional components from part 2 of the Common Criteria with the operations completed.

33 Standard Common Criteria text is in regular black font and the text inserted to perform an operation on the requirement is in accordance with the conventions specified in section 1.5 of this ST.

Table 10 – Summary of TOE security functional requirements

Identifier	Title
Security audit	
FAU_GEN.1	Audit data generation
FAU_GEN.2	User identity association
FAU_SAR.1a	Audit review (Creator)
FAU_SAR.1b	Audit review (Administrator)
FAU_SAR.1c	Audit review (Manager)
FAU_SAR.1d	Audit review (Super Administrator)
Cryptographic support	
FCS_CKM.1	Cryptographic key generation
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1a	Cryptographic operation (3DES)
FCS_COP.1b	Cryptographic operation (AES)
FCS_COP.1c	Cryptographic operation (SHA-1)
User data protection	
FDP_ACC.1	Subset access control (Object Control SFP)

Identifier	Title
FDP_ACF.1	Security attribute based access control (Object Control SFP)
Identification and authentication	
FIA_ATD.1	User attribute definition
FIA_UAU.1	Timing of authentication
FIA_UAU.4	Single-use authentication mechanisms
FIA_UID.1	Timing of identification
Security management	
FMT_MSA.1	Management of security attributes (Object Control SFP)
FMT_MSA.3	Static attribute initialisation (Object Control SFP)
FMT_SAE.1	Time-limited authorisation
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security roles
FTP_TRP.1	Trusted Path
Protection of the TSF	
FPT_ITT.2	TSF data transfer separation
FPT_STM.1	Reliable time stamps

5.2.1 FAU_GEN.1 Audit data generation

Hierarchical to:	No other components.
FAU_GEN.1.1	The TSF shall be able to generate an audit record of the following auditable events: a) Start-up and shutdown of the audit functions; b) All auditable events for the [***not specified***] level of audit; and c) [**all actions performed on a Secure Object, decryption of a Secure Object, and application specific activity for a Secure Object.**]
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 ST, [**i) User Identity**, **ii) IP address,** **iii) Session Identity,** **iv) Secure Object Identity (for all actions associated with a secure object),** **v) Event code, and** **vi) Event information.**]
Dependencies:	FPT_STM.1 Reliable time stamps
Notes:	Start-up, shutdown and other system related audit event information is written to the standard output of the Java application server hosting the Secure Objects Enterprise Server components. All audit information related to the creation and modification of user accounts, groups and secure objects is stored in the database configured for use by the TOE.

5.2.2 FAU_GEN.2 User identity association

Hierarchical to:	No other components.
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.
Dependencies:	FAU_GEN.1 Audit data generation FIA_UID.1 Timing of identification

Notes:	None.

5.2.3 FAU_SAR.1a Audit review (Creator)

Hierarchical to:	No other components.
FAU_SAR.1a.1	The TSF shall provide [**Creators**] with the capability to read [**all audit records that relate to secure objects created by the Creator**] from the audit records.
FAU_SAR.1a.2	The TSF shall provide the audit records in a manner suitable for the user to interpret the information.
Dependencies:	FAU_GEN.1 Audit data generation
Notes:	Creators are permitted to access and review all audit records that relate to secure envelopes and Secure Objects that they generate.

5.2.4 FAU_SAR.1b Audit review (Administrator)

Hierarchical to:	No other components.
FAU_SAR.1b.1	The TSF shall provide [**Administrators**] with the capability to read [**all audit records that relate to the actions of Creators and Managers**] from the audit records.
FAU_SAR.1b.2	The TSF shall provide the audit records in a manner suitable for the user to interpret the information.
Dependencies:	FAU_GEN.1 Audit data generation
Notes:	None.

5.2.5 FAU_SAR.1c Audit review (Manager)

Hierarchical to:	No other components.
FAU_SAR.1c.1	The TSF shall provide [**Managers**] with the capability to read [**all audit records that relate to secure objects that they have been granted the Manager role for**] from the audit records.
FAU_SAR.1c.2	The TSF shall provide the audit records in a manner suitable for the user to interpret the information.
Dependencies:	FAU_GEN.1 Audit data generation
Notes:	Managers are permitted to access and review all audit records that relate to secure objects that they have been assigned Manager role for.

5.2.6 FAU_SAR.1d Audit review (Super Administrator)

Hierarchical to:	No other components.
FAU_SAR.1d.1	The TSF shall provide [**Super Administrators**] with the capability to read [**all audit records that relate to the actions of Administrators**] from the audit records.
FAU_SAR.1d.2	The TSF shall provide the audit records in a manner suitable for the user to interpret the information.
Dependencies:	FAU_GEN.1 Audit data generation
Notes:	None.

5.2.7 FCS_CKM.1 Cryptographic key generation

Hierarchical to:	No other components.
FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**a) AES, and** **b) 3DES]** and specified cryptographic key sizes [**a) 256 bits (AES), and** **b) 168 bits (3DES)]** that meet the following: [**a) Federal Information Processing Standard (FIPS) Publication 197, "Advanced Encryption Standard (AES)", 26 November 2001**], **and** **b) Federal Information Processing Standard (FIPS) Publication 46-3, "Data Encryption Standard", 25 October 1999**]
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
Notes:	The Secure Objects Enterprise Server, (supported by the RNG Server) creates, distributes and maintains key material for the TOE.

5.2.8 FCS_CKM.4 Cryptographic key destruction

Hierarchical to:	No other components.
FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**zeroisation**] that meets the following: [**FIPS 140-2 Level 2**].

Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
Notes:	The cryptographic keys are zeroised in memory only after the key is used, but the cryptographic keys permanently stored in the database are not deleted.

5.2.9 FCS_COP.1a Cryptographic operation (3DES)

Hierarchical to:	No other components.
FCS_COP.1a.1	The TSF shall perform [**encryption and decryption for securing objects**] in accordance with a specified cryptographic algorithm [**3DES**] and cryptographic key sizes [**168 bits**] that meet the following: [**Federal Information Processing Standard (FIPS) Publication 46-3, “Data Encryption Standard”, 25 October 1999**].
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
Notes:	None.

5.2.10 FCS_COP.1b Cryptographic operation (AES)

Hierarchical to:	No other components.
FCS_COP.1b.1	The TSF shall perform [**encryption and decryption for securing objects**] in accordance with a specified cryptographic algorithm [**AES**] and cryptographic key sizes [**256 bits**] that meet the following: [**Federal Information Processing Standard (FIPS) Publication 197, “Advanced Encryption Standard (AES)”, 26 November 2001**].
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
Notes:	None.

5.2.11 FCS_COP.1c Cryptographic operation (SHA-1)

Hierarchical to:	No other components.
FCS_COP.1c.1	The TSF shall perform [**hashing**] in accordance with a specified cryptographic

	algorithm [**SHA-1**] and cryptographic key sizes [**N/A**] that meet the following: [**Federal Information Processing Standard (FIPS) Publication 180-1, "Secure Hash Algorithm", 17 April 1995.**].
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
Notes:	The dependencies for FCS_COP.1c are not met due to SHA-1 having no dependency on cryptographic keys.

5.2.12 FDP_ACC.1 Subset access control (Object Control SFP)

Hierarchical to:	No other components.
FDP_ACC.1.1	The TSF shall enforce the [**Object Control SFP**] on [**a) Subjects:** **i) Creator, and** **ii) Recipient.** **b) Objects:** **i) Secure objects, and** **ii) Attachments.** **c) Operations:** **i) Open a secure object, or** **ii) Access an attachment**].
Dependencies:	FDP_ACF.1 Security attribute based access control
Notes:	None.

5.2.13 FDP_ACF.1 Security attribute based access control (Object Control SFP)

Hierarchical to:	No other components.
FDP_ACF.1.1	The TSF shall enforce the [**Object Control SFP**] to objects based on the following: [**a) Creator and Recipient:** **i) Creator Identity or Recipient Identity,** **ii) Email address,** **iii) Authentication code, and** **b) Secure Objects and Attachments:**

	i) **Creator,** ii) **Recipient,** iii) **Status (active or inactive), and** iv) **Access rights**].
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [a) **For all attempts to open a secure object:** i) **The user must be assigned as a Recipient by the Creator or Manager,** ii) **The user must authenticate using the valid authentication code,** iii) **The secure object must have an active status,** iv) **The user must be currently permitted to open the secure object, and** v) **The user must not have exceeded their maximum permitted openings of the secure object.** b) **For all attempts to access an attachment within a secure object:** i) **The user must be assigned as a Recipient by the Creator or Manager, and** ii) **The attachment must have an active status**].
FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**none**].
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules [**if the authentication code has expired all access to the secure object and contained attachments will be denied**].
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization
Notes:	None.

5.2.14 FIA_ATD.1 User attribute definition

Hierarchical to:	No other components.
FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users: [a) **Email address (for all users),** b) **Alias (for all Creators, Managers, Administrators and Super Administrators),**

	c) **Name (for all Creators, Managers, Administrators and Super Administrators),** d) **Group membership (for all Creators, Managers and Administrators),** e) **Department (for all Creators, Managers, Administrators and Super Administrators), and** f) **Billing Code (for all Creators and Administrators).**
Dependencies:	**None**.
Notes:	The billing code attribute is optional.

5.2.15 FIA_UAU.1 Timing of authentication

Hierarchical to:	No other components.
FIA_UAU.1.1	The TSF shall allow [a) **Creation of a one-time password, and** b) **Receipt of a secure object**] 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 actions on behalf of that user.
Dependencies:	FIA_UID.1 Timing of identification
Notes:	None.

5.2.16 FIA_UAU.4 Single-use authentication mechanisms

Hierarchical to:	No other components.
FIA_UAU.4.1	The TSF shall prevent reuse of authentication data related to [**object access, and logon for the Secure Objects Enterprise Server**].
Dependencies:	None.
Notes:	None.

5.2.17 FIA_UID.1 Timing of identification

Hierarchical to:	None.
FIA_UID.1.1	The TSF shall allow [**receipt of a secure object**] 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 actions on behalf of that user.

Dependencies:	None.
Notes:	None.

5.2.18 FMT_MSA.1 Management of security attributes (Object Control SFP)

Hierarchical to:	No other components.
FMT_MSA.1.1	The TSF shall enforce the [**Object Control SFP**] to restrict the ability to [***change default, query, modify, or delete***] the security attributes [**a) Recipient,** **b) Status, and** **c) Access rights.**] to [**the Creator and Manager**].
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	Managers may be individually assigned, or assigned implicitly through group membership. For group membership, upon the successful creation of a secure object, all groups that the creator is a member of are granted Manager rights to the secure object. All members of these groups are granted the Manager role for the secure object.

5.2.19 FMT_MSA.3 Static attribute initialisation (Object Control SFP)

Hierarchical to:	No other components.
FMT_MSA.3.1	The TSF shall enforce the [**Object Control SFP**] to provide [***restrictive***] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow ~~the~~ [**no TOE maintained roles**] to specify alternative initial values to override the default values when an object or information is created.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
Notes:	The ability exists to set session timeout (and hence the lifetime of authentication passcodes) as well as the permitted protocols which all communications between the Secure Envelopes client and Secure Objects Enterprise Server must use, through the modification of the web.xml file maintained on each web server component. The administrator of the Secure Objects Enterprise Server operating system (and any other user granted modify access to this file) maintain the rights to modify this file.

5.2.20 FMT_SAE.1 Time-limited authorisation

Hierarchical to:	No other components.
FMT_SAE.1.1	The TSF shall restrict the capability to specify an expiration time for [**authentication data**] to [**no roles**].
FMT_SAE.1.2	For each of these security attributes, the TSF shall be able to [**a) Prevent the successful creation of a secure object by a Creator,** **b) Prevent access to the secure object for the Recipient, and** **c) Prevent access to the Admin, Manager and Super Administrator console**] after the expiration time for the indicated security attribute has passed.
Dependencies:	FMT_SMR.1 Security roles FPT_STM.1 Reliable time stamps
Notes:	The expiry time for authentication data (the one-time password) is 30 minutes.

5.2.21 FMT_SMF.1 Specification of management functions

Hierarchical to:	No other components.
FMT_SMF.1.1	The TSF shall be capable of performing the following security management functions: [**a) Manage the cryptographic function,** **b) Manage access to secure objects,** **c) Manage access to attachments within a secure object, and** **d) Manage user access to the TOE**].
Dependencies:	None.
Notes:	Management of user access to the TOE is performed through the creation of users and the assignment and revocation of roles maintained by the TSF. Management of the cryptographic function provides the ability to specify the use of either AES or Triple DES to encrypt secure objects. This configuration is defined within an XML template, maintained within the Template server component.

5.2.22 FMT_SMR.1 Security roles

Hierarchical to:	No other components.
FMT_SMR.1.1	The TSF shall maintain the roles [**a) Creator,**

	b) Recipient, **c) Manager,** **d) Administrator, and** **e) Super Administrator**].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.
Dependencies:	FIA_UID.1 Timing of identification
Notes:	Creators and Recipients are the end-users of the Secure Envelopes product, interfacing directly with the client software. Administrators and Super Administrators fulfil roles that manage and control the enterprise implementation through the Secure Objects Enterprise Server. Creators and Managers access the Secure Objects Enterprise Server to manage and maintain access to a specific secure object and contained attachments.

5.2.23 FPT_ITT.2 TSF data transfer separation

Hierarchical to:	FPT_ITT.1 Basic internal TSF data transfer protection
FPT_ITT.2.1	The TSF shall protect TSF data from [***disclosure and modification***] when it is transmitted between separate parts of the TOE.
FPT_ITT.2.2	The TSF shall separate user data from TSF data when such data is transmitted between separate parts of the TOE.
Dependencies:	None.
Notes:	TSF authentication, manifest, and encryption keys are transmitted between the Secure Envelopes client and the Secure Objects Enterprise Server using an SSL protected connection.

5.2.24 FPT_STM.1 Reliable time stamps

Hierarchical to:	No other components.
FPT_ITT.1.1	The TSF shall be able to provide reliable time stamps.
Dependencies:	None.
Notes:	The operating system (outside of the scope of the TOE) of the Secure Objects Enterprise Server provides a reliable time stamp for the TOE.

5.2.25 FTP_TRP.1 Trusted path

Hierarchical to:	No other components.
FTP_TRP.1.1	The TSF shall provide a communication path between itself and [**remote**] users that is logically distinct from other communication paths and provides assured

	identification of its end points and protection of the communicated data from [**disclosure and modification**].
FTP_TRP.1.2	The TSF shall permit [**remote users**] to initiate communication via the trusted path.
FTP_TRP.1.3	The TSF shall require the use of the trusted path for [**all security management functions**].
Dependencies:	None.
Notes:	The Secure Objects Enterprise Server enforces an SSL protected communication channel between Creators and Recipients using the Secure Envelopes client and the Secure Objects Enterprise Server through the specification of HTTPS as the only permitted protocol (as specified in the configuration file, web.xml). The Secure Objects Enterprise Server supports an SSL protected communication channel between users and the web consoles of the Secure Objects Enterprise Server The implementation of the SSL communication channel is performed by the Java application server supporting the Secure Objects Enterprise Server, requiring the transfer of all user and TSF data between the user and the server to be delivered using this channel.

5.3 TOE security assurance requirements

34 The assurance package for the evaluation of the TOE is Evaluation Assurance Level 4 (EAL4) augmented with basic flaw remediation.

35 EAL4 assurance requirements provide confidence in the security functionality of the TOE by analysis using a functional and interface specification, guidance documentation, the high-level design, low-level design and the implementation representation of the TOE, to understand the security behaviour.

36 The analysis is supported by independent testing of the TOE security functions and security-enforcing modules, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, strength of function analysis, and evidence of a developer search for obvious vulnerabilities.

37 EAL4 also provides assurance through a configuration list for the TOE as well as evidence of secure delivery procedures.

38 Table 11 lists the TOE security assurance requirements for this evaluation. Complete details of all assurance components are located in part 3 of the Common Criteria.

Table 11 – Summary of TOE security assurance requirements

Assurance class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description

Assurance class	Assurance components
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic modular design
AGD: Guidance Documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-Cycle Support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
	ALC_FLR.1 Basic flaw remediation
ASE: 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
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability Assessment	AVA_VAN.3 Focused vulnerability analysis

6 TOE summary specification

6.1 Overview

39 This chapter provides the TOE summary specification, a high-level definition of the security functions claimed to meet the functional and assurance requirements.

6.2 Security functions

40 The TOE security functions include the following:

a) **Data protection.**

b) **Object access audit.**

c) **Object control.**

d) **Security management.**

6.2.1 Data protection

6.2.1.1 Object protection

41 The TOE has the ability to encrypt data files to provide protection whilst being transmitted and also at rest. The encryption supported includes:

a) Advanced Encryption Standard (AES) in 256 bit cipher strength, and

b) Data Encryption Standard (DES) using the Triple Data Encryption Algorithm (TDEA), also known as 'Triple DES' (3DES) in 168 bit cipher strength using either two or three unique DES keys.

42 The keys used to encrypt the files are not stored with the files, which makes it more difficult for the key to be broken. Decryption of the secure object is performed via the Secure Envelopes user interface provided. One-time passwords generated by the Secure Objects Enterprise Server sent to the intended recipient's email address. The one-time passwords expire 30 minutes after generation, after which a new one will need to be generated.

6.2.1.2 Trusted communications path

43 The Secure Envelopes client provides a trusted communications path via an SSL encrypted tunnel to the Secure Objects Enterprise Server to securely transmit TSF data such as audit records and encryption keys.

44 Server-side certificates are used to verify the authenticity of the Secure Objects Enterprise Server by the Secure Envelopes client.

6.2.2 Object access audit

6.2.2.1 Generation of audit records

45 The TOE has the capability to generate and centrally store audit records for events of interest that relate to actions performed on a Secure Envelope.

46 The audit records contain all auditable events and the identity of the user that caused the event.

47 The audit records are stored in the Database Server, which is out of the scope of the TOE.

6.2.2.2 Audit review

48 The TOE provides the Creator (as well as assigned Managers) of a secure object the ability to review audit records generated and captured as a result of actions being performed on the secure object.

49 The TOE also provides the Administrator the ability to review all audit records generated regarding the creation and modification of Creators, Managers and groups. The audit records are provided in a manner suitable for the user to interpret the information.

6.2.3 Object control

6.2.3.1 User identification and authentication

50 The TOE has the capability to issue one-time passwords (16 character, alphanumeric passwords) to specified recipient email addresses to provide a method for identifying and subsequently authenticating users. Generation of the one-time passwords is performed by the Secure Objects Enterprise Server through a supporting Java library implemented by the Java application server supporting the Secure Objects Enterprise Server.

51 These authentication passcodes are used to authenticate users in the creation of a secure object, the access of a secure object as well as access to the web-based interfaces (accessible by Managers, Creators, Administrators and Super Administrators) . These one-time passwords are only valid for a limited period of time (30 minutes). After the time is over, the user will have to request a new passcode in order to reauthenticate.

6.2.3.2 Controlled access

52 The TOE has the capability to allow Creators of a secure object to control access to the secure object and contained attachments.

53 The Creators can assign intended recipients during the creation of a secure object. Users whose email addresses are not part of the access control list will not be authorised to access the secure object or its contents.

54 Once the secure object has been distributed, the Creator or an assigned Manager can add additional and/or revoke existing user access to the secure object.

6.2.4 Security management

6.2.4.1 Defined roles

55 The TOE maintains a set of security-related roles that enable the secure management of users and any secure objects created.

56 These roles include Creator, Recipient, Manager, Administrator and Super Administrator and are granted the following capabilities:

a) **Creator**: Creators are permitted to create new secure objects, as well as manage existing secure objects that they have previously created. Creators are permitted to view logs regarding the access and modification of secure objects that they have created.;

b) **Recipient**: Recipients are permitted to open secure objects and access any attachments stored within;

c) **Manager**: Managers are permitted to manage a secure object once created, including modifying Recipients and Managers, as well as the status of the secure object. Managers are permitted to view logs regarding the access and modification of secure objects that they have been assigned the Manger role for;

d) **Administrator**: Administrators are permitted to define and manage Creators and Groups (membership of groups, as well as the active/inactive status of groups). Managers are permitted to view logs regarding the creation and modification of Creators and groups.

e) **Super Administrator**: Super Administrators are permitted to define and manage Administrators as well as view logs regarding the creation and management of Administrators.

6.2.4.2 Object management

57 The TOE permits Creators and Managers to continue to manage secure access rights and controls that pertain to a secure object and contained attachments.

58 Creators and Managers can set the activity status (active/inactive) of the secure object and individual attachments, and optionally, the number of times a recipient can open the secure object, the period that the secure object can be opened, whether the attachment names can be seen or are hidden, and which individual users are permitted access to the contents of the secure object.

59 The Manager role for a specific secure object is granted in one of three ways:

a) The Creator specifies the email address of a user during the creation of the secure object that will be granted the Manager role;

b) All groups that the Creator is a member of are automatically granted the Manager role during the creation of a secure object. If the Creator does not belong to any groups, then no Managers will be assigned through this method; or

c) Once the secure object has been successfully created, users with the Manager role (as well as the secure object's Creator) can add additional Managers through the Manager Server web interface.

60 Only users that have been granted the Manager role by the Creator (during the secure object's creation) or via the Manager Server web interface can have their Manager rights removed.

61 Once a secure object has been created, the groups that are granted the Manager role through the Creator's group membership cannot be modified. Users must be a member of one of these groups at the time they attempt to access the Manager Server in order to be granted Manager rights to the secure object.

6.2.4.3 Centralised key management

62 The TOE provides a centralised key management capability that distributes and manages keys separately outside user data.

63 All the keys and information used to encrypt the files are generated and maintained on the Secure Objects Enterprise and RNG servers (only being passed to the Secure

Envelopes client when a user has been authenticated and authorised) and are not stored with the secure object.

6.3 Assurance measures

6.3.1 Overview

64 The following groups of assurance measures are applied to Secure Envelope to satisfy CC EAL4 assurance requirements:

a) Security Target,

b) Development,

c) Guidance documents,

d) Life cycle support,

e) Testing, and

f) Vulnerability analysis.

6.3.2 Security Target

65 This document provides the evidence for the Security Target to meet the ASE requirements of the Common Criteria.

6.3.3 Development

66 The design and security architecture of the Secure Envelopes product is contained within the following suite of development documents:

a) **Secure Objects incorporating Secure Envelopes Functional Specification.** The functional specification describes the security functionality of the TOE, and aligns with the security functional requirements specified in the ST. The functional specification also details the external interfaces to the TOE.

b) **Secure Objects incorporating Secure Envelopes Security Architecture.** Documentation that describes the mechanism implemented within the TOE to ensure that the security enforcing functions cannot be bypassed, that the TOE operates in a domain of its own control and that the security functionality is always invoked.

c) **Secure Objects incorporating Secure Envelopes TOE Design.** The design of Secure Objects, the RNG Server and Secure Envelopes components provides a description of the TSF in terms of subsystems and modules and relates these units to the functions that they provide.

d) **Secure Objects incorporating Secure Envelopes Correspondence Demonstration.** This document provides correspondence between the various representations provided for the EAL4 evaluation.

6.3.4 Guidance documents

67 Cocoon Data provides operational guidance on how to perform the TOE security functions and warnings to authorised administrators and users about actions that can compromise the security of the TOE.

68 Cocoon Data also provides documentation that provides guidance for initially installing and configuring all components of the TOE so that it is in a suitable and secure initial configuration.

69 Administrator guidance and preparatory information is documented in the Secure Object incorporating Secure Envelopes Administrator Guide.

70 User guidance is provided in the Secure Object incorporating Secure Envelopes Software User Guide.

6.3.5 Life cycle support

71 The Configuration Management (CM) measures applied by Cocoon Data ensure that Configuration Items (CIs) are uniquely identified, and that documented procedures are used to control and track changes that are made to the TOE.

72 Cocoon Data ensures changes to the implementation representation are controlled with the support of automated tools and that TOE associated CI modifications are properly controlled. Cocoon Data performs CM on the TOE implementation representation, design, tests, user and administrator guidance, the CM documentation, lifecycle documentation and vulnerability analysis.

73 Cocoon Data ensures that the TOE is uniquely referenced and labelled with this reference. Cocoon Data uses, and documents how they use, automated tools to support TOE generation.

74 Cocoon Data also implements a set of processes to ensure that design flaws are identified, managed and remediated.

6.3.6 Testing

75 The TOE has been tested by Cocoon Data to ensure that all security functional requirements have been implemented accurately within Secure Objects and Security Envelopes.

76 The Secure Objects incorporating Secure Envelopes testing evidence consists of the following documents:

a) **Test plan.** The test plan describes the form, content, and organization of test documentation. It also summarizes each of the test suites and includes high-level procedures for exercising the tests.

b) **Test procedures.** The test procedures include both documentation and an actual implemented test (if applicable). Test suites are organised around tests that share a common theme. The test suite documentation describes the purpose for the test suite, the set of test variations, procedures to successfully exercise the test, and expected results.

c) **Test results.** The results are captured for each test with summaries of the results in terms of total tests for each test suite. The results are matched against the expected results for each test.

6.3.7 Vulnerability analysis

77 All evidence identified will provide input into the vulnerability analysis effort. The TOE will be made available to the evaluators to conduct vulnerability testing.

7 Rationale

7.1 Overview

78 This section provides the rationale for completeness and consistency of the ST. The rationale addresses the following areas:

a) **Security objectives rationale.** Provides coverage for the security objectives for the TOE and the environment, ensuring that all threats and assumptions are effectively addressed.

b) **Security requirements rationale.** Provides justification for TOE assurance requirements, evidence that all dependencies have been addressed, specification of strength of function for all probabilistic mechanisms and demonstration that the IT requirements address the TOE and environment objectives.

c) **TOE summary specification rationale.** Provides evidence that the IT security functions and assurance measures are adequate to implement the security functional and assurance requirements.

7.2 Security objectives rationale

7.2.1 Security objectives for the TOE

Table 12 – Mapping of TOE security objectives to threats

Threats	Objective	Justification
T.USERDATA_COMM	O.USRDATA_COMM	The threat of monitoring communications between creator and recipient is mitigated by implementing mechanisms to preserve the confidentiality and integrity of transmitted TSF data.
T.USERDATA_REST	O.USRDATA_REST	The threat of interception is mitigated by implementing mechanisms to preserve the confidentiality and integrity of stored user data.
T.TSFDATA	O.TSFDATA	The threat of monitoring communications between the Secure Envelopes client and Secure Objects Enterprise Server (TOE Components) is mitigated by implementing mechanisms to preserve the confidentiality and integrity of transmitted TSF data.

Threats	Objective	Justification
T.ROLES	O.ROLES O.USER_AUTH O.AUDIT OSP.ACCOUNTABLE	The threat of unauthorised access to user data and TSF data by users is mitigated by: • O.USER_AUTH requires user authentication, preventing immediate access to data. • O.ROLES enables role based access control to assign roles based on their required level of access. • O.AUDIT provides a record of all events of interest associated with accessing Secure Objects. • OSP.ACCOUNTABLE holds users accountable for their actions.
T.MANAGEMENT	O.USER_AUTH O.ROLES O.MANAGEMENT OSP.ACCOUNTABLE	The threat of unauthorised modifications to security policy settings by users is mitigated by: • O.USER_AUTH requires user authentication, preventing immediate access to data. • O.ROLES enables role based access control to assign roles based on their required level of access. • O.MANAGEMENT limits the modification of security policy settings to the role of Administrator and Super Administrator. • OSP.ACCOUNTABLE holds users accountable for their actions.

7.2.2 Organisational Security Policies (OSPs)

Table 13 – Mapping of security objectives to OSPs

OSP	Objectives	Justification
OSP.ACCOUNTABLE	O.AUDIT O.ROLES	This organisational security policy is enforced by the following security objectives: • O.AUDIT provides the audit records required by the organisation to hold users accountable for their actions. • O.ROLES enables the organisation to distinguish if the action of a user was authorised or unauthorised based on level of access to TOE function.

7.2.3 Security objectives for the non-IT environment

Table 14 – Mapping of non-IT objectives to assumptions

Assumptions	Objectives	Justification
A.USAGE	OE.USAGE	This objective for the environment ensures that this assumption is upheld that the users will be made aware of the needs to follow guidance. This includes that attachments extracted from a secure object are not disclosed and distributed to anyone, and that Secure Envelopes continue to operate in the evaluated configuration.
A.ENTERPRISE	OE.ENTERPRISE	This objective for the environment ensures that the assumption is upheld that the Secure Objects Enterprise Server and RNG Server are appropriately protected from unauthorised physical access.
A.ADMIN	OE.ADMIN	This objective for the environments upholds the assumption that administration personnel shall not be careless, wilfully negligent, hostile and can be trusted to follow the administrator documentation.

7.2.4 Security objectives for the IT environment

Table 15 – Mapping of IT environment objectives to assumptions

Assumption	Objective	Justification
A.IT_ENTERPRISE	OE.IT_ENTERPRISE	This objective for the IT environment ensures that the assumption is upheld that the IT environment provides logical access controls to protect the Secure Objects Enterprise Server and RNG Server from unauthorized access.
A.COMMS	OE.COMMS	This objective for the IT environment ensures that the assumption is upheld that: • the IT environment provides an active network connection between the Secure Envelopes client and the Secure Objects Enterprise Server. • The IT environment provides an active network connection between the Secure Objects Enterprise Server and the RNG Server. • The IT environment provides an active network connection between the Secure Objects Enterprise Server and the SMTP Server. • The IT environment provides an active network connection between the SMTP Server and any intermediary SMTP servers.
A.COMMS_SECURE	OE.COMMS_SECURE	The objective for the IT environment ensures that the assumption is upheld that: • The communications between the Secure Objects Enterprise Server and both the database and SMTP Server is secure. • The communications between the SMTP Server and any intermediary SMTP servers is secure.
A.OS	OE.OS	The objective for the IT environment ensures that the assumption is upheld that the operating systems supporting individual TOE components protect these components from unauthorised access, modification or deletion.

A.TIME	OE.TIME	The objective for the IT environment ensures that the assumption is upheld that the IT environment (operating system supporting the Security Objects Enterprise Server) provides a reliable time service for use by the Secure Objects Enterprise Server.
A.SECRET	OE.SECRET	The objective for the IT environment ensures that the assumption is upheld that the IT environment (the Java application server supporting the Secure Objects Enterprise Server) provides a random alphanumeric character generator for use by the Secure Objects Enterprise Server to generate random 16 character, alphanumeric passwords.

7.3 Security requirements rationale

7.3.1 Dependency analysis

Table 16 – TOE SFR dependency demonstration

SFR	Dependency	Inclusion
FAU_GEN.1	FPT_STM.1 Reliable time stamps	FPT_STM.1
FAU_GEN.2	FAU_GEN.1 Audit data generation FIA_UID.1 Timing of identification	FAU_GEN.1 FIA_UID.1
FAU_SAR.1a	FAU_GEN.1 Audit data generation	FAU_GEN.1
FAU_SAR.1b	FAU_GEN.1 Audit data generation	FAU_GEN.1
FAU_SAR.1c	FAU_GEN.1 Audit data generation	FAU_GEN.1
FAU_SAR.1d	FAU_GEN.1 Audit data generation	FAU_GEN.1
FCS_CKM.1	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1 FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]	FCS_CKM.1

SFR	Dependency	Inclusion
FCS_COP.1a	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1 FCS_CKM.4
FCS_COP.1b	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1 FCS_CKM.4
FCS_COP.1c	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	None. The Secure Hashing Algorithm has no dependency on cryptographic keys.
FDP_ACC.1	FDP_ACF.1 Security attribute based access control	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation	FDP_ACC.1 FMT_MSA.3
FIA_ATD.1	No dependencies.	N/A
FIA_UAU.1	FIA_UID.1 Timing of identification	FIA_UID.1
FIA_UAU.4	No dependencies.	N/A

SFR	Dependency	Inclusion
FIA_UID.1	No dependencies.	N/A
FMT_MSA.1	[FDP_ACC.1 Subset access control, FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1
FMT_MSA.3	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA.1 FMT_SMR.1
FMT_SAE.1	FMT_SMR.1 Security roles FPT_STM.1 Reliable time stamps	FMT_SMR.1 FPT_STM.1
FMT_SMF.1	No dependencies.	N/A
FMT_SMR.1	FIA_UID.1 Timing of identification	FIA_UID.1
FPT_ITT.2	No dependencies.	N/A
FPT_STM.1	No dependencies.	N/A
FTP_TRP.1	No dependencies.	N/A

7.3.2 IT environment SFR dependency demonstration

Table 17 – IT environment SFR dependency demonstration

SFR	Dependency	Inclusion
FCS_CKM.1	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1 FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]	FCS_CKM.1
FIA_ATD.1	No dependencies.	N/A
FIA_UAU.1	FIA_UID.1 Timing of identification	FIA_UID.1
FIA_UID.1	No dependencies.	N/A
FPT_ITT.2	No dependencies.	N/A
FTP_TRP.1	No dependencies.	N/A

7.3.3 TOE IT requirements correspondence

Table 18 – Mapping TOE SFRs to objectives

Objective	SFRs	Demonstration
O.USRDATA_COMM	FCS_CKM.1 FCS_COP.1a FCS_COP.1b FCS_COP.1c FCS_CKM.4	FCS_CKM.1 provides cryptographic support through key generation that enables the implementation of cryptographic operations for secure communications between Creators and Recipients that have both confidentiality and integrity security properties. FCS_COP.1a provides the cryptographic operations to implement data encryption services. FCS_COP.1b provides the cryptographic operations to implement data encryption services. FCS_COP.1c provides cryptographic hashing operations to support data encryption services. FCS_CKM.4 provides a mechanism for securely disposing of cryptographic keys that have been generated by various components within the enterprise environment that communicate using cryptographic protection with the TOE. FCS_CKM.1, FCS_COP.1a, FCS_COP.1b, FCS_COP.1c and FCS_CKM.4 combine to ensure that the O.USRDATA_COMM objective is met.
O.USRDATA_REST	FCS_CKM.1 FCS_COP.1a FCS_COP.1b FCS_COP.1c FCS_CKM.4	FCS_CKM.1 provides cryptographic support through key generation that support data encryption. FCS_COP.1a provides the cryptographic operations to implement data encryption services. FCS_COP.1b provides the cryptographic operations to implement data encryption services. FCS_COP.1c provides cryptographic hashing operations to support data encryption services. FCS_CKM.4 provides a mechanism for securely disposing of cryptographic keys that have been generated. FCS_CKM.1, FCS_COP.1a, FCS_COP.1b, FCS_COP.1c and FCS_CKM.4 combine to ensure that the O.USRDATA_REST objective is met.
O.TSFDATA	FPT_ITT.2	FPT_ITT.2 provides the trusted path (SSL secured) between the Secure Envelopes client and the Secure

Objective	SFRs	Demonstration
		Objects Enterprise Server, protecting all TSF data in transit. FPT_ITT.2 ensures that the O.TSFDATA objective is met.
O.AUDIT	FAU_GEN.1 FAU_GEN.2 FAU_SAR.1a FAU_SAR.1b FAU_SAR.1c FAU_SAR.1d FPT_STM.1	FAU_GEN.1 provides the audit records that are generated for events associated with accessing Secure Objects. FAU_GEN.2 provides the capability to associate each audit record with the identity of a user that caused that event. FAU_SAR.1a provides the capability for the Creator to access and review all audit records relating to Secure Envelopes generated by the Creator. FAU_SAR.1b provides the capability for the Administrator to access and review audit records. FAU_SAR.1c provides the capability for the Manager to access and review all audit records that relate to the secure objects that the Managers has been assigned the Manager role for. FAU_SAR.1d provides the capability for the Super Administrator to access and review all audit records. FPT_STM.1 ensures that each audit record generated has a reliable time stamp provided. FAU_GEN.1, FAU_GEN.2, FAU_SAR.1a, FAU_SAR.1b, FAU_SAR.1c, FAU_SAR.1d and FPT_STM.1 combine to ensure that the O.AUDIT objective is met.
O.USER_AUTH	FIA_ATD.1 FIA_UAU.1 FIA_UAU.4	FIA_ATD.1 provides the set of security attributes that must be associated with a user to enable authentication. FIA_UAU.1 provides the capability for the TOE to be able to offer a number services prior to requiring a user authentication event. FIA_UAU.4 ensures that each authentication event does not reuse prior authentication data for the access of the secure object. FIA_ATD.1, FIA_UAU.1 and FIA_UAU.4 combine to ensure that the O.USER_AUTH objective is met.

Objective	SFRs	Demonstration
O.ROLES	FMT_SMR.1	FMT_SMR.1 provides a specification of the various roles that the TOE is required to recognize and apply.
O.MANAGEMENT	FDP_ACC.1 FDP_ACF.1 FMT_MSA.1 FMT_MSA.3 FMT_SAE.1 FMT_SMF.1 FMT_SMR.1	FDP_ACC.1 provides the basis for establishing the object control SFP within the TOE for controlling the configuration of each Secure Envelope. FDP_ACF.1 provides the object control SFP statements to support the implementation of Secure Envelopes configuration for the TOE. FMT_MSA.1 provides the restrictions for the object control SFP that are necessary for protecting the management and configuration of each Secure Envelope. FMT_MSA.3 provides restrictions and controls for managing security attributes associated with the object control SFP. FMT_SAE.1 ensures that the management of the expiration time for authentication data is restricted to no TOE maintained roles. FMT_SMF.1 ensures that the Administrator is capable of configuring security policy settings that cannot be modified by the end-user. FMT_SMR.1 provides a specification of the various roles that the TOE is required to recognise and apply, in particular the role of Administrator. FDP_ACC.1, FDP_ACF.1, FMT_MSA.1, FMT_MSA.3, FMT_SAE.1, FMT_SMF.1 and FMT_SMR.1 combine to ensure that the O.MANAGEMENT objective is met.

7.3.4 TOE assurance requirements

2 This ST contains the assurance requirements from the CC EAL4 assurance package augmented with ALC_FLR.1. This ST is based on good rigorous commercial development practices and has been developed for a general environment for a TOE that is readily available and does not require modification to meet the security needs of the environment specified in this ST.

3 The EAL chosen is based on the statement of the security environment (threats, organizational policies, assumptions) and the security objectives defined in this ST. The sufficiency of the EAL chosen is justified based on those aspects of the environment that have impact upon the assurance needed in the TOE. Specifically, that the TOE will not process information that requires protection from attackers possessing a high or moderate attack potential, and that protection from obvious vulnerabilities is required.

7.3.5 Demonstration of Mutual Support

4 The dependency analysis provided at Table 16 and the analyses provided in Table 17, Table 18 and Table 19 demonstrate that the IT security functions work together to satisfy the stated security functionality of the TOE.

5 The demonstration of the implementation of the majority of dependencies, and a suitable rationale for those dependencies that have not been implemented, demonstrates mutual support between security requirements, and therefore, the security functions and mechanisms that implement them.

7.4 TOE summary specification rationale

7.4.1 IT security functions

Table 19 – Mapping TOE SFRs to TOE security functions

SFR	Data protection	Object access audit	Object control	Security management	Demonstration
FAU_GEN.1		X			FAU_GEN.1 generates the audit records required for the object access audit function.
FAU_GEN.2		X			FAU_GEN.2 associates each audit event with the identity of the user that caused the evening required for the object access audit function.
FAU_SAR.1a		X			FAU_SAR.1a provides the Creator with the ability to access and review all audit records relating to Secure Objects generated by the Creator required for the object access audit function.
FAU_SAR.1b		X			FAU_SAR.1b provides the Administrator with the ability to access and review all generated audit records required for the object access audit function.
FAU_SAR.1c		X			FAU_SAR.1c provides the Manager with the ability to access and review all audit records relating to secure objects that the Manager has been assigned the Manager role for.
FAU_SAR.1d		X			FAU_SAR.1d provides the Super Administrator with the ability to access and review all generated audit records.
FCS_CKM.1	X				FCS_CKM.1 creates the cryptographic keys for each function that protects the data required by the data protection function.

SFR	Data protection	Object access audit	Object control	Security management	Demonstration
FCS_CKM.4	X				FCS_CKM.4 ensures that the cryptographic keys used to protect the data are securely destroyed, which is required by the data protection function.
FCS_COP.1a	X				FCS_COP.1a provides the cryptographic protection for TSF and/or user data required by the data protection function.
FCS_COP.1b	X				FCS_COP.1b provides the cryptographic protection for TSF and/or user data required by the data protection function.
FCS_COP.1c	X				FCS_COP.1c provides hashing functionality used to support the cryptographic protection for TSF and/or user data required by the data protection function.
FDP_ACC.1				X	FDP_ACC.1 provides the access controls for a Secure Envelope or Secure Objects required by the security management function.
FDP_ACF.1				X	FDP_ACF.1 provides the controls to align with the set of specific security policy rules identified in this requirement required by the security management function.
FIA_ATD.1		X	X		FIA_ATD.1 provides the attributes associated with a user that is required for the object access audit function and object control function.
FIA_UAU.1			X		FIA_UAU.1 states the functions that can be performed before a user is authenticated, that is required by the object control function.
FIA_UAU.4			X		FIA_UAU.4 provides the one-time generated authentication passcodes required by the object

SFR	Data protection	Object access audit	Object control	Security management	Demonstration
					control function.
FIA_UID.1			X		FIA_UID.1 provides for the receipt of a secure object prior to a user being identified, required by the object control function.
FMT_MSA.1				X	FMT_MSA.1 provides the specified management functionality for the object control function, required by the security management function.
FMT_MSA.3				X	FMT_MSA.3 ensures that static attributes are applied during initialisation of the Object Control SFP, required by the security management function.
FMT_SAE.1			X		FMT_SAE.1 restricts the configuration of the expiration time for authentication data to no roles maintained by the TOE.
FMT_SMF.1				X	FMT_SMF.1 implements the set of security management function provided for the TOE, required by the security management function.
FMT_SMR.1				X	FMT_SMR.1 implements the set of security roles established by FMT_SMR.1 requirement, required by the security management function.
FPT_ITT.2	X				FPT_ITT.2 establishes a secure connection between the Secure Objects Enterprise Server and Secure Envelopes client for data transfer, required by the data protection function.

SFR	Data protection	Object access audit	Object control	Security management	Demonstration
FPT_STM.1		X			FPT_STM.1 provides reliable time stamps required by the FAU_GEN.1 requirement, required by the object access audit function.
FTP_TRP.1				**X**	FTP_TRP.1 provides a secure channel between users and the web console interfaces of the Secure Objects Enterprise Server.

7.4.2 Assurance measures

Table 20 – Assurance measures rationale

Assurance requirement	Assurance measures	Demonstration
ADV_ARC.1 Security architecture description	Development	The development assurance measure provides all the necessary design documentation to support the effective detailed analysis of the TOE for an evaluation at EAL4. The security architecture description provides a detailed description of the TSF security architecture. The functional specification provides a detailed description of the security functions of the TOE. The design documentation provides a complete definition of the TSF, allowing for sufficient analysis to be performed.
ADV_FSP.4 Complete functional specification		
ADV_IMP.1 Implementation representation of the TSF		
ADV_TDS.3 Basic modular design		
AGD_OPE.1 Operational user guidance	Guidance documents	The operational user guidance documentation provides the guidance for end users, administrators and other parties who will utilise the TOE. These documents provide all the necessary instructions and direction for ensuring that the TOE is installed, configured, used and administered in a secure manner.
AGD_PRE.1 Preparative procedures		
ALC_CMC.4 Production support, acceptance procedures and automation	Life cycle support	The life cycle support measures provide the assurance that the TOE is developed and subsequently managed using a well defined and controlled approach. Configuration management measures provide the assurance that configured items are managed and maintained in a controlled manner, through the demonstration of well defined processes, procedures and requirements.
ALC_CMS.4 Problem tracking CM coverage		

Assurance requirement	Assurance measures	Demonstration
ALC_DEL.1 Delivery procedures		By placing the TOE and its components into this configuration management list provides assurance that the TOE components are only modified in a controlled manner with proper authorization. Employing sufficient security measures in the delivery process of the TOE to consumers ensures that the TOE is not tampered with prior to its receipt. Procedural, personnel and physical security related documentation is used to ensure that the confidentiality and integrity of the TOE and its design are maintained throughout the development life cycle. The life cycle support assurance measures provides a set of procedures aimed at the identifying, reporting and addressing security flaws or bugs that may appear in the TOE. An established development lifecycle methodology is employed to guide the development of the TOE. A set of well established development tools exist and are employed in the development of the TOE.
ALC_DVS.1 Identification of security measures		
ALC_LCD.1 Developer defined life-cycle model		
ALC_TAT.1 Well-defined development tools		
ALC_FLR.1 Basic flaw remediation		
ASE_CCL.1 Conformance claims	Security Target evaluation	Security Target evaluation assurance measures ensure that the claim to EAL4 (augmented with ALC_FLR.1) can be accurately appraised.
ASE_ECD.1 Extended components definition		
ASE_INT.1 ST Introduction		
ASE_OBJ.2 Security objectives		

Assurance requirement	Assurance measures	Demonstration
ASE_REQ.2 Derived security Requirements		
ASE_SPD.1 Security problem definition		
ASE_TSS.1 TOE summary specification		
ATE_COV.2 Analysis of coverage	Tests	The tests assurance measure ensures that the TOE has been appropriately tested for the claimed set of security functions. The test plans for the TOE identifies the set of security functions that are to be tested, the procedures for establishing the test environment and also for conducting the test cases. The results of the tests are also recorded to provide evidence of test results.
ATE_DPT.1 Testing: basic design		
ATE_FUN.1 Functional testing		
ATE_IND.2 Independent testing - sample		
AVA_VAN.3 Focused vulnerability analysis	Vulnerability assessment	The TOE will be made available for vulnerability analysis and penetration testing.