Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Certification Report

Certificate Number: 2011/73

22 Mar 2011

Version 1.0

Amendment Record

Version	Date	Description
0.1	16/03/2011	Internal release.
0.2	21/03/2011	Extended review.
1.0	22/03/2011	Public release.

Executive Summary

1 Secure Objects incorporating Secure Envelopes is a data protection product that is designed to provide confidentiality and integrity controls for user data while in transit and at rest. Secure Objects incorporating Secure Envelopes is the Target of Evaluation (TOE).

2 This report describes the findings of the IT security evaluation of Cocoon Data's Secure Objects incorporating Secure Envelopes (SOSE), to the Common Criteria (CC) evaluation assurance level EAL 4 + ALC_FLR.1. The report concludes that the product has met the target assurance level of EAL 4 + ALC_FLR.1 and that the evaluation was conducted in accordance with the relevant criteria and the requirements of the Australasian Information Security Evaluation Program (AISEP). The evaluation was performed by stratsec AISEF and was completed in 7th March 2011.

3 With regard to the secure operation of the TOE, the Australasian Certification Authority (ACA) recommends that:

a) Users and administrators should be aware that the security of Secure Envelopes authentication data relies on SSL being enabled on each mail server in the communications channel. Therefore, each node in the communications channel between the end user and the SOES must have SSL enabled, or the authentication data will be sent in the clear.

b) Users and administrators should be aware that once a secure envelope has been successfully opened the contents may be extracted; as such the security of the envelope contents may no longer be under the control of the TOE

c) All software forming part of the TOE environment should be kept up to date with the latest security patches, antivirus, firewalls etc. Additionally all unused services should be disabled and a strong password policy should be enforced.

d) The SQL database schema file provided contains default passwords for database user accounts; it is recommended that these passwords be changed immediately after installation

e) In instances where the TOE is to be hosted by a 3rd party provider, it is recommended that the provider is assessed to ensure that their security complies with industry best practice whilst ensuring that data separation between customers is maintained.

4 This report includes information about the underlying security policies and architecture of the TOE, and information regarding the conduct of the evaluation.

5 It is the responsibility of the user to ensure that the TOE meets their requirements. For this reason, it is recommended that a prospective user of the TOE refer to the Security Target at Ref [1], and read this Certification Report prior to deciding whether to purchase the product.

Table of Contents

Chapter 1 - Introduction

1.1 Overview

6 This chapter contains information about the purpose of this document and how to identify the Target of Evaluation (TOE).

1.2 Purpose

7 The purpose of this Certification Report is to:

a) report the certification of results of the IT security evaluation of the TOE, Secure Objects incorporating Secure Envelopes, against the requirements of the Common Criteria (CC) evaluation assurance level EAL 4 + ALC_FLR.1, and

b) provide a source of detailed security information about the TOE for any interested parties.

8 This report should be read in conjunction with the TOE's Security Target (Ref [1]) which provides a full description of the security requirements and specifications that were used as the basis of the evaluation.

1.3 Identification

9 Table 1 provides identification details for the evaluation. For details of all components included in the evaluated configuration refer to section 2.6.1 Evaluated Configuration.

Table 1: Identification Information

Item	**Identifier**
Evaluation Scheme	Australasian Information Security Evaluation Program
TOE	Secure Objects incorporating Secure Envelopes
Software Version	Auth Server component: build 1.5.1.6 All other components: build 1.5.1.5
Security Target	Secure Objects using Secure Envelopes Security Target (EAL4+)
Evaluation Level	EAL 4 + ALC_FLR.1
Evaluation Technical Report	Secure Objects incorporating Secure Envelopes Evaluation Technical Report

Criteria	CC Version 3.1, July 2009, interpretations as of 9th July 2009.
Methodology	CCMB – 2009-07-004 Version 3.1, Revision 3, July 2009.
Conformance	CC Part 2 Conformant CC Part 3 Conformant
Developer	Cocoon Data
Evaluation Facility	stratsec Suite 1/50 Geils Court, Deakin ACT 2600, Australia

Chapter 2 - Target of Evaluation

2.1 Overview

10 This chapter contains information about the Target of Evaluation (TOE), including: a description of the TOE, functionality provided; its architecture components; the scope of evaluation; security policies; and its secure usage.

2.2 Description of the TOE

11 The TOE is called Secure Objects incorporating Secure Envelopes (SOSE) developed by Cocoon Data. 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.

12 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.

13 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.

2.3 Security Policy

14 This evaluation was performed at EAL4 augmented with ALC_FLR.1. There is no security policy model required for the TOE.

2.4 TOE Architecture

15 The TOE consists of the following major architectural components:

a) Secure Envelopes client;

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

c) The Random Number Generator (RNG) server.

2.4.1 Secure Envelopes Client

16 The Secure Envelopes client is the client application that is used by creators and recipients of secure objects, either to create new, or open previously created secure objects.

17 The Secure Envelopes client provides the only component of the TOE which provides for the actual use of secure objects. The Secure Envelope client is used to create secure objects which include attachments and are subsequently saved as an encrypted file (default suffix of .senv) which requires the Secure Envelopes client to open.

18 The Secure Envelopes client subsystem is composed of four individual components (user interface, core, cryptography shim and cryptography) see Figure 1 - User Environment.

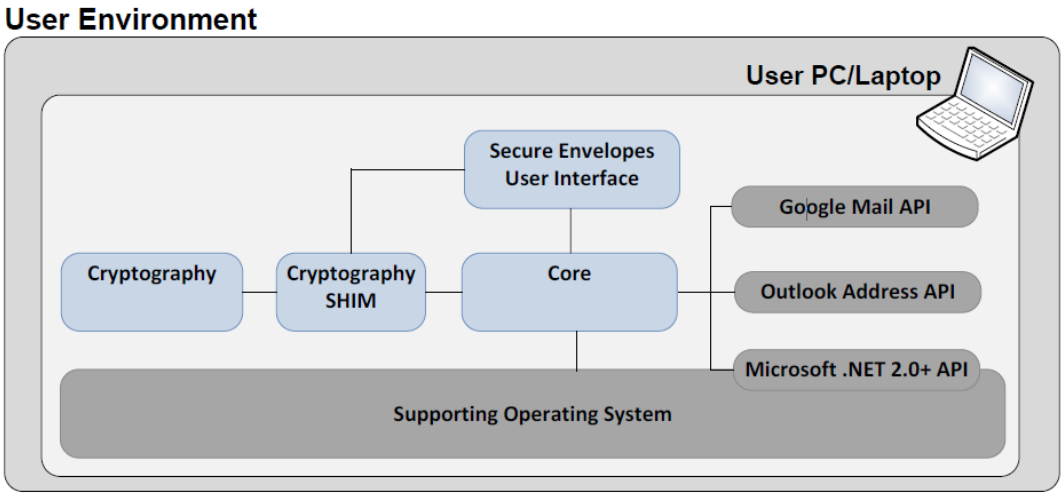

Figure 1 - User Environment

19 **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.

20 **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.

21 **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.

22 **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.

2.4.2 Secure Objects Enterprise Server

23 The SOES provides the main server functionality that is used for creating, managing and maintaining secure objects. The SOES provides interfaces which are used by both the Secure Envelopes client (to create or open secure objects) as well as by administrators and managers of previously created secure objects in order to manage the SOES, each individual user account and group, as well as update attributes specific to a secure object.

24 The SOES subsystem is comprised of six web servers (Gatekeeper, Auth, Template, Mngr, Admin and SAdmin) and two supporting libraries (data and web).

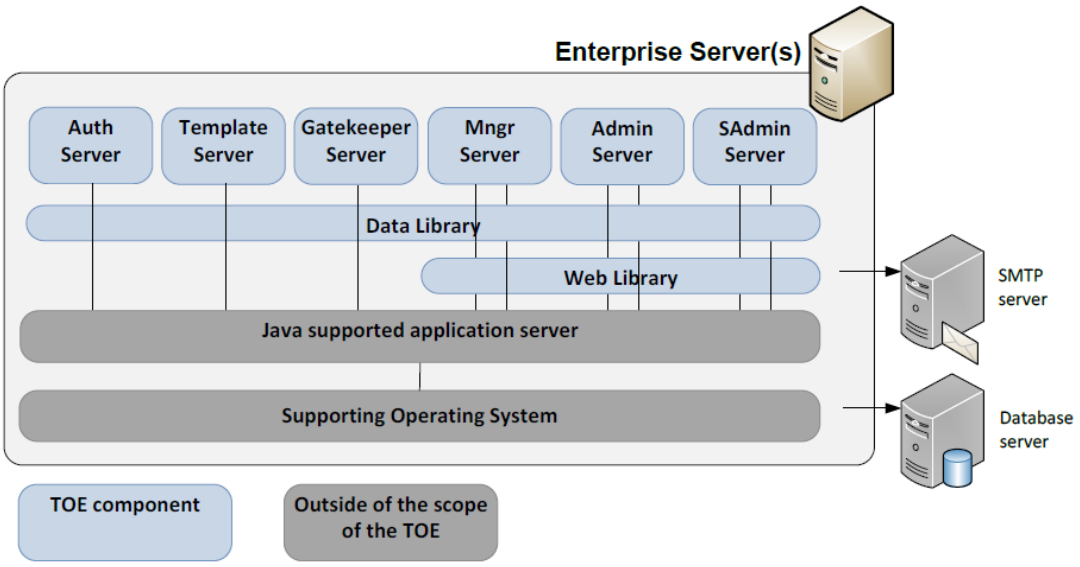

Figure 2 - Enterprise Server

25 **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.

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

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

28 **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.

29 **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.

30 **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.

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

32 **Web Library.** Provides common web functions to the manager, admin and super admin servers.

2.4.3 RNG Server

33 The RNG (random number generator) server provides the functionality to the SOES server to allow for pseudo-random number and cryptographic

key generation. This is comprised of six modules which are installed from a single RPM (Red hat Package Manager) package requiring a Java Virtual Machine to support this.

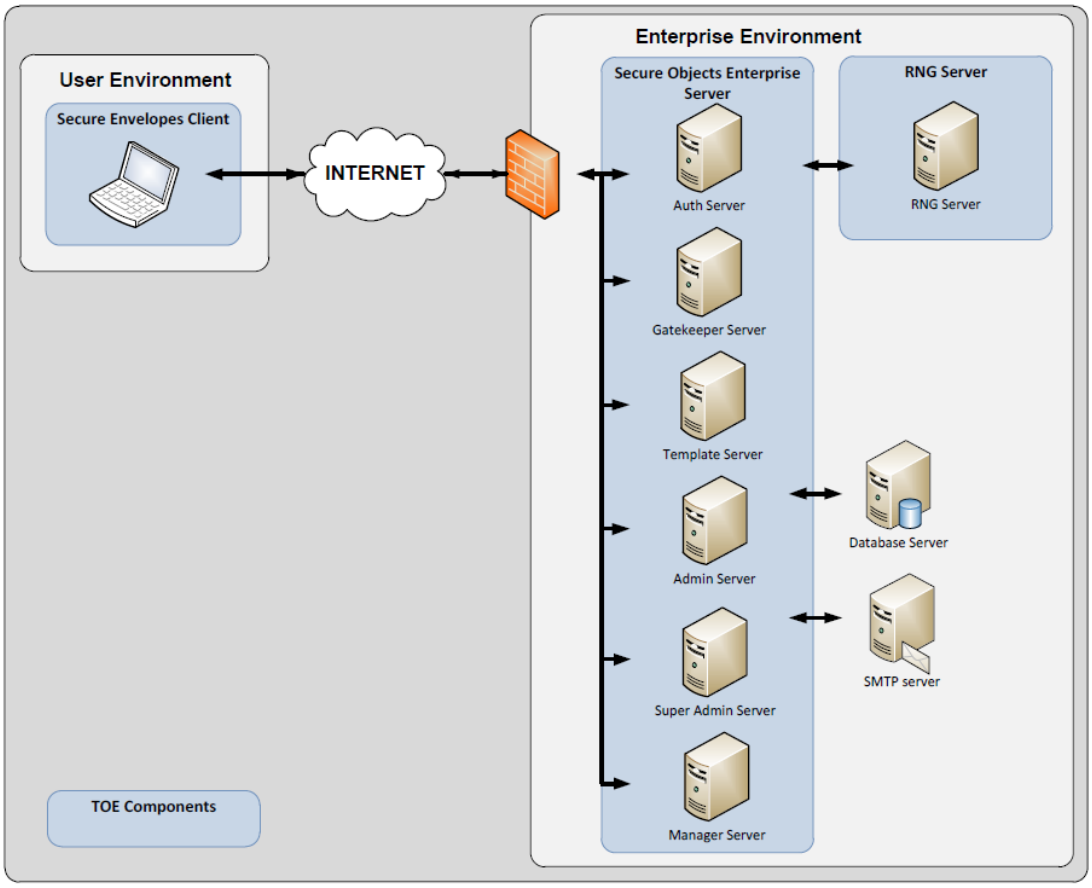

Figure 3 - Major components of the TOE

2.5 Clarification of Scope

34 The scope of the evaluation was limited to those claims made in the Security Target (Ref [1]).

2.5.1 Evaluated Functionality

35 The TOE provides the following evaluated security functionality:

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	**Generation of audit records.** The TOE has the capability to generate and centrally store audit records

capability to capture audit records for events of interest.	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.

2.5.2 Non-evaluated Functionality

36 Potential users of the TOE are advised that some functions and services have not been evaluated as part of the evaluation. Potential users of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration; Australian Government users should refer to Australian Government ICT Security Manual (ISM) (Ref [2]) for policy relating to using an evaluated product in an un-evaluated configuration. New Zealand Government users should consult the Government Communications Security Bureau (GCSB).

37 The functions and services that have not been included as part of the evaluation are provided below:

a) The database server;

b) SMTP server;

c) Java supported application server; and

d) The API's that enable Secure Envelopes to integrate with either Google Mail or Microsoft Outlook. See Figure 1 - User Environment

2.6 Usage

2.6.1 Evaluated Configuration

38 This section describes the configurations of the TOE that were included within scope of the evaluation. The assurance gained via evaluation applies specifically to the TOE in this defined evaluated configuration. Australian Government users should refer to ISM (Ref [2]) to ensure that configuration meet the minimum Australian Government policy requirements. New Zealand Government users should consult the Government Communications Security Bureau (GCSB).

39 The TOE is comprised of the following software components:

a) Secure Envelopes Client

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

c) The RNG server.

40 The TOE relies on the following hardware:

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.

41 Each component of the Secure Objects Enterprise server also requires:

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.

42 Please note that the RNG server runs on only a Linux operating system and does not need the java application server, only the Java run time environment.

2.6.2 Delivery procedures

43 When placing an order for the TOE, purchasers should make it clear to their supplier that they wish to receive the evaluated product.

44 Cocoon Data delivers the TOE to customers using one of the following methods, depending on the customers' requirements or preferred delivery method. The possible delivery methods are as follows:

a) Onsite delivery by an authorised Cocoon Data employee or authorised representative (storage media).

b) Customer pickup from Cocoon Data premises or from a Cocoon Data employee or authorised representative (storage media).

c) Registered post (CD).

d) Email or downloaded from the Cocoon Data website or an authorised website (software download).

2.6.3 Determining the Evaluated Configuration

45 Cocoon Data ensures that the finished TOE is securely transferred and retains its integrity until it reaches the customer either by personally delivering the finished TOE to the customer or by encrypting the TOE within a Secure Envelope (via the public non-evaluated version of Secure Objects and Secure Envelopes).

46 In order to open the Secure Envelope that the TOE is contained within, the customer must download and install the most recent copy of the public version of Secure Envelopes from the Cocoon Data website, and be able to access the public Secure Objects servers via the Internet.

47 If the TOE is to be delivered in person (either delivered onsite or picked up by the customer), the TOE does not need to be encrypted via a Secure Envelope. Any other method of delivery (by post, email or download) requires the use of a Secure Envelope to protect the TOE.

2.6.4 Documentation

48 It is important that the TOE is used in accordance with guidance documentation in order to ensure the secure usage. Please see Annex A.2 for a list of the documentation provided with the TOE.

2.6.5 Secure Usage

49 The evaluation of the TOE took into account certain assumptions about its operational environment. These assumptions must hold in order to ensure the security objectives of the TOE are met.

50 Assumptions are made in the following areas:

Assumption 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/physical 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 provided secure network protection.
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 servers and the SMTP Server, any intermediary SMTP 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.
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.

51 In addition, the following organisational security policies must be in place:

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

Chapter 3 - Evaluation

3.1 Overview

52 This chapter contains information about the procedures used in conducting the evaluation and the testing conducted as part of the evaluation.

3.2 Evaluation Procedures

53 The criteria against which the Target of Evaluation (TOE) has been evaluated are contained in the Common Criteria for Information Technology Security Evaluation (Refs [14], [15], [16]). The methodology used is described in the Common Methodology for Information Technology Security Evaluation (CEM) (Ref [17]). The evaluation was also carried out in accordance with the operational procedures of the Australasian Information Security Evaluation Program (AISEP) (Refs [18], [19], [20], [22]). In addition, the conditions outlined in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (Ref [22]) were also upheld.

3.3 Functional Testing

54 To gain confidence that the developer's testing was sufficient to ensure the correct operation of the TOE, the evaluators analysed the evidence of the developer's testing effort. This analysis included examining: test coverage; test plans and procedures; and expected and actual results. The evaluators drew upon this evidence to perform a sample of the developer tests in order to verify that the test results were consistent with those recorded by the developers. The evaluators conducted testing of the TOE during October 2010 and February 2011. The evaluators obtained test results consistent with expected test results documented in the developer test documentation.

3.4 Penetration Testing

55 The developer performed penetration tests on the TOE in order to identify any obvious vulnerability in the product and to show that the vulnerabilities were not exploitable in the intended environment of the TOE. The evaluators performed these tests to determine if the TOE is resistant to attacks performed by an attacker possessing enhanced-basic attack potential. The following factors have been taken into consideration during the penetration tests:

a) Time taken to identify and exploit;

b) Specialist technical expertise required;

c) Knowledge of the TOE design and operation;

d) Window of opportunity; and

e) IT hardware/software or other equipment required for exploitation.

56 The developers search for vulnerabilities also considered public domain sources for published vulnerability data related to the TOE and the contents of all TOE deliverables.

Chapter 4 - Certification

4.1 Overview

57 This chapter contains information about the result of the certification, an overview of the assurance provided by the level chosen, and recommendations made by the certifiers.

4.2 Certification Result

58 After due consideration of the conduct of the evaluation as witnessed by the certifiers, and of the Evaluation Technical Report (Ref [23]), the Australasian Certification Authority certifies the evaluation of Secure Objects incorporating Secure Envelopes performed by the Australasian Information Security Evaluation Facility, stratsec AISEF.

59 stratsec AISEF has found that Secure Objects incorporating Secure Envelopes upholds the claims made in the Security Target (Ref [1]) and has met the requirements of the Common Criteria (CC) evaluation assurance level EAL 4 + ALC_FLR.1.

60 Certification is not a guarantee of freedom from security vulnerabilities.

4.3 Assurance Level Information

61 EAL4 provides assurance by an analysis of the security functions, using a functional and complete interface specification, guidance documentation, the high-level and low-level design of the TOE, and a subset of the implementation, to understand the security behaviour. Assurance is additionally gained though an informal model of the TOE security policy.

62 The analysis is supported by independent testing of the TOE security functions, evidence of developer testing based on the functional specification and high-level design, selective independent confirmation of the developer test results, strength of function analysis, evidence of a developer search for obvious vulnerabilities, and an independent vulnerability analysis demonstrating resistance to penetration attackers with a low attack potential.

63 EAL4 also provides assurance though the use of development environment controls and additional TOE configuration management including automation, and evidence of secure delivery procedures. The development

environment assessment was conducted 10-11 March 2010 in Sydney, Australia.

64 ALC_FLR.1 is a class that is used to determine whether the developer has established flaw remediation procedures that describe the tracking of security flaws, the identification of corrective actions and the distribution of corrective action information to users. The evaluators examined the flaw remediation procedures and determined that the product complies with the ALC_FLR.1

4.4 Recommendations

65 Not all of the evaluated functionality present in the TOE may be suitable for Australian and New Zealand Government users. For further guidance, Australian Government users should refer to ISM (Ref [2]) and New Zealand Government users should consult the Government Communications Security Bureau (GCSB).

66 In addition to ensuring that the assumptions concerning the operational environment are fulfilled and the guidance document is followed (Ref [3]), the ACA also recommends that:

a) Users and administrators should be aware that the security of Secure Envelopes authentication data relies on SSL being enabled on each mail server in the communications channel. Therefore, each node in the communications channel between the end user and the SOES must have SSL enabled, or the authentication data will be sent in the clear.

b) Users and Administrators should be aware that once a secure envelope has been successfully opened the contents may be extracted; as such the security of the envelope contents may no longer be under the control of the TOE.

c) All software forming part of the TOE Environment should be kept up to date with the latest security patches, antivirus, firewalls etc. Additionally all unused services should be disabled and a strong password policy should be enforced.

d) The SQL database schema file provided contains default passwords for database user accounts; it is recommended that these passwords be changed immediately after installation.

e) In instances where the TOE is to be hosted by a third party provider, it is recommended that the provider is assessed to ensure that:

   i) they comply with relevant industry security standards; and

   ii) suitable data separation between customers at that site is maintained.

Annex A - References and Abbreviations

A.1 References

[1] Secure Objects incorporating Secure Envelopes Security Target EAL4+

[2] Australian Government Information Security Manual (ISM), November 2010, Defence Signals Directorate, (available at www.dsd.gov.au).

[3] Secure Objects incorporating Secure Envelopes 1.5.1 Security Target Version 1.3 .

[4] Secure Objects incorporating Secure Envelopes 1.5.1 Functional Specification Version 0.3

[5] Secure Objects incorporating Secure Envelopes 1.5.1 TOE Design Version 0.4

[6] Secure Objects incorporating Secure Envelopes 1.5.1 Security Architecture Version 0.3

[7] Secure Objects incorporating Secure Envelopes 1.5.1 Operational User Guidance Version 1.1

[8] Secure Objects incorporating Secure Envelopes 1.5.1 Preparative Procedures Version 1.2

[9] Secure Objects incorporating Secure Envelopes 1.5.1 Delivery Documentation Version 0.3

[10] Secure Objects incorporating Secure Envelopes 1.5.1 Configuration Management Processes and Procedures Version 0.6

[11] Secure Objects incorporating Secure Envelopes 1.5.1 Flaw Remediation Version 0.3

[12] Secure Objects incorporating Secure Envelopes 1.5.1 Life-Cycle Documentation Version 0.2

[13] Secure Objects incorporating Secure Envelopes 1.5.1 Security Testing Version 0.5

[14] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and General Model, version 3.1 Revision 3, July 2009, CCMB-2009-07-001.

[15] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, version 3.1 Revision 3, July 2009, CCMB-2009-07-002.

[16] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, version 3.1 Revision 3, July 2009, CCMB-2009-07-003.

[17] Common Methodology for Information Technology Security Evaluation, Evaluation methodology, July 2009, Version 3.1 Revision 3, CCMB-2009-07-004.

[18] AISEP Publication No. 1 – Program Policy, AP 1, Version 3.1, 29 September 2006, Defence Signals Directorate.

[19] AISEP Publication No. 2 – Certifier Guidance, AP 2. Version 3.1, 29 September 2006, Defence Signals Directorate.

[20] AISEP Publication No. 3 – Evaluator Guidance, AP 3. Version 3.1, 29 September 2006, Defence Signals Directorate.

[21] AISEP Publication No. 4 – Sponsor and Consumer Guidance, AP 4. Version 3.1, 29 September 2006, Defence Signals Directorate.

[22] Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, May 2000

[23] Secure Objects incorporating Secure Envelopes Evaluation Technical Report, EFS-T017-ETR.

A.2 Guidance Documentation provided with TOE:

Secure Envelopes Client guide v1.5.1.5.

SO 0001 Secure Objects - Setup v1.5.1.5.

SO 0002 Secure Objects - Server Installation v1.5.1.5.

SO 0003 Secure Objects - Installing the Server Applications.

SO 0004 Secure Objects - Setup Certificate for SSL v1.5.1.5.

SO 0005 Secure Objects - Database Guide v1.5.1.5.

SO 0006 Secure Objects - Customisation v1.5.1.5.

SO 0007 Secure Objects - Template Customisation v1.5.1.5.

SO 0008 Secure Objects - Client Customisation v1.5.1.5.

SO 0009 Secure Objects - Server Email Customisation v1.5.1.5.

SO 0010 Secure Objects - Server Text Customisation v1.5.1.5.

SO 0011 Secure Objects -Build Procedure v1.5.1.5.

SO 0012 Secure Objects - Server Build v1.5.1.5.

SO 0013 Secure Objects - Secure Envelopes Desktop Client Build.

WMC Administrator guide v1.5.1.5.

WMC Creator and Manager guide v1.5.1.5.

WMC Super Administrator guide v1.5.1.5.

A.3 Abbreviations

AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Program
CC	Common Criteria
CEM	Common Evaluation Methodology
DSD	Defence Signals Directorate
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GCSB	Government Communications Security Bureau
PP	Protection Profile
RNG	Random Number Generator
SaaS	Software-as-a-Service
SFP	Security Function Policy
SFR	Security Functional Requirements
SOSE	Secure Objects using Secure Envelopes
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy