Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Certification Report

Certificate Number: 2009/52

30 April 2009

Version 1.0

Amendment Record

Version	Date	Description
1.0	30/04/2009	Public release.

Executive Summary

1 The Target of Evaluation (TOE) is the Eaglehawk SBX Enigma Version 4.2.4, a server–based, object oriented data access and management application designed to protect an organisations valuable information assets. The core SBX Enigma functions include identification and authentication, role based management, access control, secure data storage and security audit capabilities.

2 This report describes the findings of the IT security evaluation of the TOE to Common Criteria (CC) evaluation assurance level EAL 2+. The report concludes that the product has met the target assurance level of EAL 2+ 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 and was completed on 9 April 2009.

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

a) use it only in its evaluated configuration; and

b) balance the 'need to know' restrictions with the need for availability of business information across their organisation.

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, Eaglehawk SBX Enigma Version 4.2.4, against the requirements of the Common Criteria (CC) evaluation assurance level EAL 2+ 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	Eaglehawk SBX Enigma Version 4.2.4
Software Version	SBX Enigma Version 4.2.4
Security Target	Eaglehawk SBX Enigma EAL2+ Common Criteria Evaluation Security Target; ST documentation number: TDG6014-ASE-001; Version E.0, 21 November 2008.
Evaluation Level	EAL 2+
Evaluation Technical Report	Evaluation Technical Report for Eaglehawk SBX Enigma v4.2.4, 14 April 2009
Criteria	CC Version 3.1, Revision 2, September 2007 with interpretations as of 2008-05-26.

Methodology	Common Criteria, Common Methodology for Information Technology Security Evaluation September 2007 version 3.1 Revision 2 with interpretations as of 4 April 2007
Conformance	Common Criteria Part 2 Conformant Common Criteria Part 3 Augmented with Basic Flaw Remediation
Sponsor/Developer	Eaglehawk Limited, PO Box 1913, Hamilton HM HX, Bermuda
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 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 the Eaglehawk SBX Enigma Version 4.2.4 developed by Eaglehawk Limited. Its primary role is to grant system architects complete discretion and control over what information gets protected and who can access it.

12 SBX Enigma™ is server-based data security software that provides a virtual lockbox designed to protect an organisation's most valuable information assets. It is an object oriented data management system. Core SBX Enigma™ functions include: identification and authentication; role based management; access control; secure data storage and comprehensive security audit capabilities instantly available to support client applications through the SBX application program interface (API). Regardless of data type or location, SBX Enigma™ enables an organisation to protect any of its information assets, ranging from enterprise applications, to service-oriented architecture (SOA) services, to discrete data components such as encryption keys or personally identifiable information (PII). SBX functions are highly configurable and enable an organisation to address its specific data security requirements in a manner best suited to its unique environment. SBX Enigma™ readily integrates with and strengthens

existing applications and security frameworks, providing a direct path to address such issues as securely sharing information between organisations and need-to-know protection of high-value data.

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

2.3 Security Policy

14 As this evaluation was conducted at EAL2 a security policy model was not required.

2.4 TOE Architecture

15 The TOE's major architectural components are described in the Security Target (Ref [1]).

16 The developer's architectural design identifies the following components of the TOE:

a) audit registry (enterprise audit registry);

b) system user registry (admin users);

c) metadata registry encompassing the following metadata components:

- standard groups (field definitions);
- enterprise groups (entity group fields) and
- templates (entity groups, data groups);

d) organisation registry encompassing the following components:

- data elements objects;
- organisation audit registry (client apps)and
- organisation user register(admin users).

2.5 Clarification of Scope

17 The scope of the evaluation was limited to those claims made in the Security Target (Ref [1]). The scope of the evaluation includes only the SBX Enigma application hosted on Windows Server 2003 in a virtual machine. The virtual machine and Windows Server 2003 were not included in this evaluation. The application is accessible via a thin client

application that is installed with the TOE or via a documented API. The thin client software was not included in the scope of the evaluation. The TOE provides functionality to generate checksums for TOE generated audit records. It does not perform integrity checking on these records once they are stored externally. The checksum generation is not included in the scope of the TOE. The TOE does not counter the threat of information disclosure by authorised users. Users are explicitly trusted to use the TOE in a secure manner and ensure that the TOE is in the evaluated configuration.

2.5.1 Evaluated Functionality

18 The TOE evaluated security functionality is described in detail in the Security Target (Ref ([1]).The security functions are:

a) security audit;

b) cryptographic support;

c) user data protection;

d) identification and authentication;

e) security management and

f) TOE access. Assignment or removal of access rights to metadata and data element objects.

2.5.2 Non-evaluated Functionality and Services

19 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 Information and Communications Technology Security Manual (ISM) 2008(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).

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

a) computing platform hardware ;

b) bios firmware;

c) Microsoft Windows Server 2003;

d) Microsoft SQL Server;

e) Apache Tomcat 5.x;

f) Eaglehawk Falcon VS virtual machine and

g) Eaglehawk remote thin client.

2.6 Usage

2.6.1 Evaluated Configuration

21 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 the defined evaluated configuration. Australian government users should refer to the ISM (Ref [2]) to ensure that the configuration meets the minimum Australian government policy requirements. New Zealand government users should consult the Government Communications Security Bureau (GCSB).

22 The TOE is comprised of the following software component:

a) SBX Enigma Version 4.2.4

23 The TOE relies on the hardware identified in the Security Target (Ref [1]).

24 The evaluated configuration of the TOE is detailed in user documentation (ref [3],[4] and [5]). The evaluated configuration of the TOE is based on a default installation of the TOE from the installation medium. The installation script by default installs the TOE to C:\Eaglehawk. This installation path may be changed at installation time without affecting the evaluated configuration. The other user input required is to specify the start menu folder to create (or confirm the use of the default). After the product has been installed, the licence file (LICENSE_NAME).lcs must be copied into the folder C:\Eaglehawk\NAS\Binary\Release\Admin\ (if default path is selected during install). To ensure the correct operation of SSL, a valid X.509 certificate (renamed to rapserver.pem) must be placed in the same directory. The TOE requires an email service to be configured for user account change notifications. The evaluated configuration does not use the default third party SMTP service. To configure the TOE to use an internal mail server, the file named mailparameters.txt (located in Eaglehawk\NAS\data\Application\EH_Registries\TextFiles) must be edited. The first five lines of this file are the five parameters that can be edited as follows: Line 1 – Specify the outgoing SMTP mail server e.g. mail.abc-corp.com. Line 2 – Specify the senders email address i.e., the “From” address that will appear on outgoing emails to Users e.g. enigma@abc-corp.com. Lines 3 & 4 – The senders mail system log-on details (User Name & Password) e.g. enigma-admin agoodpassword. Note that the password is not encrypted in this file. Line 5 – The correct response (true or false) to the question “Is user authentication required?” If the SMTP server does not require user authentication, lines 3 and 4 may contain arbitrary text. NOTE: The file format must not be changed.

25 For a portion of the evaluator testing, SSL was disabled. If SSL is disabled, alternate network confidentiality controls (e.g. IPSec ESP) must be deployed to ensure the evaluated configuration is maintained.

2.6.2 Delivery procedures

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

27 The Installshield package comprising the SBX Enigma release and associated installation and guidance documentation are retrieved from the configuration management system (Visual SourceSafe) and copied to the installation medium. The generated copy of the installation medium is then tested to ensure that the medium and install image is not corrupted. The distribution medium is labelled with the product identifier and version number. It is then packaged into a slip case type container (which is also labelled with the TOE name and version number.) Three uniquely numbered tamper evident seals are applied to the exterior of the slip case to assist detection of tampering in transit. The three seals have sequential numbers.

28 The developer then forwards the sealed container to the customer using a commercial delivery carrier. Transit packaging is applied by the carrier. Following shipment of the media, the developer notifies the customer via email of the shipment details (carrier, tracking number, date of shipment, URL for online despatch tracking.) The email will also describe the application of tamper evident seals and specify the serial numbers of the seals used. Additional information is included to provide guidance to the customer on the detection of tampering and steps to take in the event of suspected tampering. If required, the licence file for the TOE will also be attached to this email.

2.6.3 Determining the Evaluated Configuration

29 The evaluated product is initially verified by examination of the distribution medium label to ensure that the product version number is 4.2.4. The installation file should be named Eaglehawk-sbxEnigma-4.2.4.exe. During the initial post install configuration, this version number is also displayed by the software.

2.6.4 Documentation

30 It is important that the TOE is used in accordance with guidance documentation in order to ensure secure usage. The following documentation is provided with the TOE:

a) *User Documentation Volume 1.7 Installation & Enterprise Setup*. (Ref [3]).

b) *User Documentation Volume 2.4 Establishing Organizations.* (Ref [4]).

c) *User Documentation Volume 3.4 Creating an Organization's Role-Based User Framework* (Ref [5]).

d) *Technical Reference 1.5 Audit Registry* (Ref [6]).

e) *Technical Reference 2.4 Metadata* (Ref [7]).

f) *Technical Reference 3.4 SBX Application Program Interface (API)*(Ref[8]).

g) *Technical Reference 4.3 Access Control* (Ref [9]).

2.6.5 Secure Usage

31 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.

32 The following assumptions were made:

a) administrators and managers are educated in respect to their responsibilities, security functionality under their control and the benefits/protection of successful implementation;

b) all SBX Enigma™ data that traverses a network is protected from disclosure to unauthorised parties;

c) administrators are non-hostile, appropriately trained, and follow all administrator guidance;

d) there are no general purpose computing capabilities (e.g., compilers or user applications) available on SBX Enigma™ servers;

e) the underlying OS has been evaluated and provides a level of trust and

f) it is assumed that appropriate physical security is provided within the domain for the value of the IT assets protected by the TOE and for the value of the stored, processed, and transmitted information.

Chapter 3 - Evaluation

3.1 Overview

33 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

34 The criteria against which the Target of Evaluation (TOE) has been evaluated are contained in the Common Criteria for Information Technology Security Evaluation (Refs [10], [11] and [12]). The methodology used is described in the Common Methodology for Information Technology Security Evaluation (CEM) (Ref [13]). The evaluation was also carried out in accordance with the operational procedures of the Australasian Information Security Evaluation Program (AISEP) (Refs [14],[15],[16] and [17]). In addition, the conditions outlined in the *ARRANGEMENT on the Recognition of Common Criteria Certificates in the field of Information Technology Security* (Ref [18]) were also upheld.

3.3 Functional Testing

35 To gain confidence that the developer's testing was sufficient to ensure the correct operation of the TOE, the evaluators analysed the evidence (Ref [19]) 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.

3.4 Penetration Testing

36 The developer performed a vulnerability analysis of 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. This analysis included a search for possible vulnerability sources in publicly available information. The evaluators performed penetration tests to determine whether the TOE was vulnerable to attack by attackers with a basic or enhanced basic attack potential.

Chapter 4 - Certification

4.1 Overview

37 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

38 After due consideration of the conduct of the evaluation as witnessed by the certifiers and of the Evaluation Technical Report (Ref[20]), the Australasian Certification Authority certifies the evaluation of Eaglehawk SBX Enigma Version 4.2.4 performed by the Australasian Information Security Evaluation Facility, stratsec.

39 stratsec has found that Eaglehawk SBX Enigma Version 4.2.4 upholds the claims made in the Security Target (Ref[1]) and has met the requirements of the Common Criteria (CC) evaluation assurance level EAL 2+.

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

4.3 Assurance Level Information

41 EAL2 provides assurance by an analysis of the security functions, using a functional and interface specification, guidance documentation and the high-level design of the TOE, to understand the security behaviour.

42 The analysis is supported by independent testing of the TOE security functions, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results and evidence of a developer search for obvious vulnerabilities (e.g. those in the public domain).

43 EAL2 also provides assurance through a configuration list for the TOE and evidence of secure delivery procedures.

4.4 Recommendations

44 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 the ISM (Ref [2]) and New Zealand Government users should consult the Government Communications Security Bureau (GCSB).

45 In addition to ensuring that the assumptions concerning the operational environment are fulfilled and the guidance document is followed

(Ref[3],[4] and [5]), the ACA also recommends that users and administrators:

a) balance the ‘need to know’ restrictions with the need for availability of business information within their organisation.

46 The TOE provides the capability to generate and store checksums of audit data stored in external databases. It does not provide any capability to detect changes to the audit data. The TOE operator is expected to provide suitable controls over access to the audit records and to perform integrity checking.

Annex A - References and Abbreviations

A.1 References

[1] Eaglehawk SBX Enigma™ EAL2+ Common Criteria Evaluation Security Target.

[2] Australian Government Information and Communications Technology Security Manual (ISM), 2008, Defence Signals Directorate, (available at www.dsd.gov.au).

[3] User Documentation Volume 1.7 Installation & Enterprise setup , version 7, Q1 2009

[4] User Documentation Volume 2.4 Establishing Organizations, version 4, Q1 2009

[5] User Documentation Volume 3.4 Creating an Organisation's Role Based User Framework, version 4, Q1 2009

[6] Technical Reference 1.5 Audit registry, version 5, Q1 2009

[7] Technical Reference 2.4 Metadata, version 4, Q1 2009

[8] Technical Reference 3.4 SBX Application Program Interface.(API) version 4, Q1 2009

[9] Technical Reference 4.3 Access Control, Q1 2009

[10] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model (CC), Version 3.1, Revision 1, September 2007, CCMB-2006-09-001, Incorporated with interpretations as of 2008-05-26

[11] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components (CC), Version 3.1, Revision 2 , September 2007, CCMB-2007-09-002, Incorporated with interpretations as of 2008-05-26

[12] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements (CC), Version 3.1, Revision 2, September 2007, CCMB-2007-09-003, Incorporated with interpretations as of 2008-05-26

[13] Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1, Revision 2 September 2007, CCMB-2007-09-004 Incorporated with interpretations as of 2008-05-26

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

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

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

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

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

[19] Eaglehawk SBX Enigma Development Evidence, version 3.6, 3 February 2009.

[20] Evaluation Technical Report for Eaglehawk SBX Enigma v4.2.4, 14 April 2009

A.2 Abbreviations

AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Program
API	Application Program Interface
CC	Common Criteria
CEM	Common Evaluation Methodology
DSD	Defence Signals Directorate
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GCSB	Government Communications Security Bureau
PII	Personally Identifiable Information
PP	Protection Profile
SFP	Security Function Policy
SFR	Security Functional Requirements
SOA	Service-Oriented Architecture
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy