Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Certification Report

Certificate Number: 2010/67

02 Jul 2010

Version 1.0

Commonwealth of Australia 2010.

Reproduction is authorised provided
that the report is copied in its entirety.

Amendment Record

Version	Date	Description
1.0	02/07/2010	Public release

Executive Summary

1 The Target of Evaluation (TOE) is the OCA Incident Manager Version 1.1 which is a product that is designed to coordinate communication between clients during an incident and provide a central repository of audit data. The TOE allows the owners of the systems to avoid separate logistic and security arrangements for communication between the parties while maintaining the control of the visibility to others.

2 This report describes the findings of the IT security evaluation of Noggin Pty Ltd's OCA Incident Manager Version 1.1, to the Common Criteria (CC) evaluation assurance level EAL2 augmented with ALC_FLR.1. The report concludes that the product has met the target assurance level of EAL2 augmented with ALC_FLR.1 and that the evaluation was conducted in accordance with the Common Criteria and the requirements of the Australasian Information Security Evaluation Program (AISEP). The evaluation was performed by stratsec and was completed on 24 June 2010.

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

a) use it only in its evaluated configuration;

b) use cryptographic implementations approved by the TOE administrators and comply with the Australian Information Security Manual (ISM) (Ref [1]) and other Australian Government regulations;

c) use SHA-1, AES with 256-bit keys and RSA with 2048 bit keys to encrypt the email attachments using S/MIME protocol. In accordance with the ISM, the cryptographic keys used should be those generated and distributed to the clients by the TOE; and

d) ensure strict adherence to the delivery procedures.

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 (Ref [2]) 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, OCA Incident Manager Version 1.1, against the requirements of the Common Criteria (CC) evaluation assurance level EAL2 augmented with 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 [2]) 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	OCA Incident Manager Version 1.1
Software Version	1.1.0.0
Security Target	Noggin OCA Incident Manager Security Target, June 2010
Evaluation Level	EAL2 augmented with ALC_FLR.1
Evaluation Technical Report	Evaluation Technical Report for OCA Incident Manager, Version 1.1, 24 June 2010.
Criteria	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3, July 2009.

Methodology	Common Methodology for Information Technology Security Evaluation, Evaluation methodology, Version 3.1 Revision 3, July 2009, CCMB-2009-07-004.
Conformance	Common Criteria Part 2 conformant. Common Criteria Part 3 augmented with Basic Flaw Remediation (ALC_FLR.1).
Sponsor/Developer	Noggin Pty Ltd Level 8, 28 Foveaux St, Surrey Hills NSW, 2010, Australia
Evaluation Facility	stratsec Deakin House, 1/50 Geils Ct, 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 it's secure usage.

2.2 Description of the TOE

11 The TOE is OCA Incident Manager Version 1.1 developed by Noggin Pty Ltd. The primary role of the TOE is to coordinate communication between clients and provide a central repository of audit data.

12 In an emergency scenario, a number of clients, owned and operated by different organisations need to communicate in a reliable manner. Establishing communication directly between the organisations would be inefficient and the complexity of coordination would significantly complicate the management of security within the systems in which the clients reside.

13 The TOE provides a central point of communication and a repository of contacts to simplify the interconnection of systems. It allows the owners of the clients and the systems they reside in to avoid separate logistic and security arrangements for communication between different parties while maintaining the control of the visibility to others.

14 The essential security features of the TOE include protection and filtering of communication between clients, provision of a central depository of audit records, and ensuring that the system configuration remains authentic so that only authorised alterations are allowed. The TOE software relies on a physically secure environment, a reliable time source and cryptographic functionality to secure communications channels. The TOE environment is assumed not to contain vulnerabilities that could be used to bypass TOE access controls.

2.3 Security Policy

15 The TOE Security Policy (TSP) is a set of rules that defines how the information within the TOE is managed and protected. The Security Target (Ref [2]) contains no explicit security policy statements.

2.4 TOE Architecture

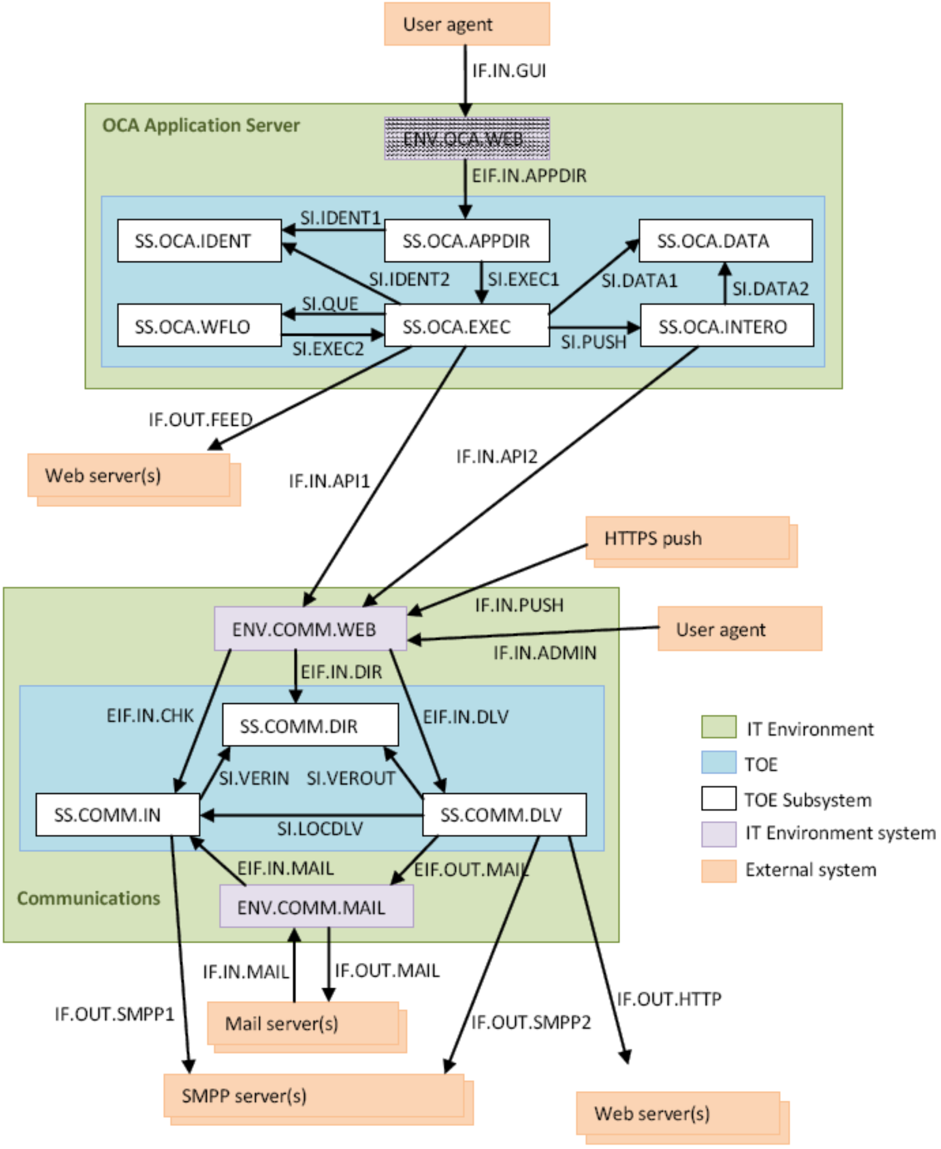

Figure 1 - TOE Subsystems

16 The OCA Application Server part of the TOE consists of the following major architectural components:

a) Identification and Authentication subsystem (SS.OCA.IDENT);

b) Application Director subsystem (SS.OCA.APPDIR);

c) Operation Execution subsystem (SS.OCA.EXEC);

d) Interoperability subsystem (SS.OCA.INTEROP);

e) Workflow subsystem (SS.OCA.WFLO); and

f) Data Management subsystem (SS.OCA.DATA).

17 The Communications Gateway part of the TOE consists of the following major architectural components:

a) Communication Delivery subsystem (SS.COMM.DLV);

b) Inbound Communication subsystem (SS.COMM.IN); and

c) OCA Connect Directory subsystem (SS.COMM.DIR).

2.5 Clarification of Scope

18 The scope of the evaluation was limited to those claims made in the Security Target (Ref [2]).

2.5.1 Evaluated Functionality

19 The TOE provides the following evaluated security functionality:

a) secure interoperation – the TOE intermediates all communication between interconnected clients and only allows traffic that is acceptable according to the traffic filtering and information flow control rules established by the administrators. Messages are authenticated prior to being relayed to their recipients. Participants define what resources are accessible to the TOE and also define the criteria for access;

b) authentication – the TOE requires identification and authentication prior to user access. The TOE maps users to roles (defined by the system administrator) which determine the security profile and access permissions that are associated with the user;

c) access control – the TOE implements a two dimensional multilevel security environment. Assets must have a security classification (for reading and for writing) associated with them. A security classification level may be sub-divided into compartments for more granular access control. Users are assigned a clearance level which is used in conjunction with the asset’s classification to determine a user’s access authorisation; and

d) security event monitoring – the TOE collects audit data from security relevant events and provides authorised administrators with the capability to review the audit data to monitor the usage of a product and detect potential security flaws.

2.5.2 Non-evaluated Functionality and Services.

20 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 Security Manual

(ISM) (Ref [1]) 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).

21 Secondary authentication, including email and SMS was not tested as part of this evaluation.

2.6 Usage

2.6.1 Evaluated Configuration

22 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 these defined evaluated configuration(s). Australian Government users should refer to the ISM (Ref [1]) to ensure that configuration(s) meet the minimum Australian Government policy requirements. New Zealand Government users should consult the GCSB.

23 The TOE is comprised of the following software components:

a) OCA Incident Manager v1.1 Application software

b) OCA Incident Manager v1.1 Communications Gateway software

24 The TOE relies on the following hardware:

a) Communications Gateway

b) Generic X86 architecture hardware used to host the TOE.

25 The evaluated configuration consisted of an out-of-the-box install of the OCA server component with post-installation configuration performed to integrate with the OCA Communications Gateway device.

26 The setup of the OCA server requires the install of the OCA server component with the bootable DVD disk. Upon successful completion of the install, the user is required to create certificates for secure communication and configure components such as the access control mechanisms and visible interfaces in accordance with the operations and preparative procedures. Once finished, the TOE can be considered to be in its configured state.

27 The TOE requires that minimum key lengths and cryptographic algorithms used by clients are set and enforced by the administrators prior to accepting registrations by the OCA Connect. These were implemented in accordance with the preparative procedures. The following specific configurations were made to the TOE:

a) Remove secondary authentication;

b) Set maximum of login attempts before accounts are suspended;

c) Set required password strength [high];

d) Set password expiry; and

e) Disable user initiated password resets and reset resends. An administrator is called if assistance is required.

2.6.2 Delivery procedures

28 When placing an order for the TOE, purchasers should make it clear to their supplier that they wish to receive the EPL listed version. They should then receive version 1.1.0.0.

29 The OCA Incident Manager is delivered by Noggin in two parts: the OCA application and the communications gateway. Note that the customer may require delivery of both or only one of these parts depending on the nature of the implementation. The delivery will be carried out or personally supervised by a Noggin staff member or an authorised agent such as a secure person-to-person courier service only.

30 Prior to delivery, Noggin will send the receiver a delivery document stating: the identity of the nominated person (customer) receiving the TOE; the identity of the authorised Noggin employee or agent delivering the TOE; the time and location of the delivery; and the list of deliverables. The delivery document is issued to the receiver with an OpenPGP signature. Verification resources are available from the website https://www.noggin.com.au/gpg/.

31 The receiving party must:

a) Provide the deliverer proof of identity for verification;

b) Verify the deliverer’s identity;

c) Check and accept the deliverables;

d) Sign two copies of the delivery document; and

e) Retain one copy for proof of delivery.

32 The delivering party must:

a) Provide the receiver proof of identity for verification;

b) Verify the receiver’s identity;

c) Provide the deliverables;

d) Sign two copies of the delivery document; and

e) Retain one copy for proof of delivery.

2.6.3 Determining the Evaluated Configuration

33 The OCA application part of the TOE is delivered as software on physical media, such as a DVD. The installer must verify all physical media before proceeding with the installation. OpenPGP signatures and SHA-256 checksums can be obtained via the internet at https://www.noggin.com.au/gpg/ for verification of the following deliverables:

a) The CentOS 5.4 OCA kickstart DVD; and

b) The CentOS 5.4 source code DVD (not required for installation).

34 The evaluated version is OCA Incident Manager v1.1. When identifying versions of the OCA Incident Manager, the version number 1.1.0.0 is the same as 1.1. The final two parts of the version number are reserved for future patches.

35 The use of version 1.1.0.0 can be verified as follows:

a) The OCA kickstart DVD media has OCA Incident Manager v1.1.0.0 on the label;

b) The OCA Application, when logged in via the web interface, displays OCA Incident Manager v1.1.0.0 on the footer of the main screen; and

c) The OCA Communications Gateway, when logged in via the web interface, displays OCA Incident Manager v1.1.0.0 on the footer of the main screen.

2.6.4 Documentation

36 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) Online help files (Ref [3]).

2.6.5 Secure Usage

37 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:

a) The TOE resides in a physically secure premises governed by appropriate physical, procedural and administrative security arrangements that ensure only legitimate and authorised administrators can gain physical access to the TOE or the immediate IT support required by the TOE;

b) The TOE is only operated in accordance with an underlying operating system that is configured to implement a reliable NTP daemon associated to a trustworthy NTP service so that the resulting time stamps provided for use by the TOE are of sufficient quality to facilitate generation of audit records;

c) The clients associated to the TOE and using the TOE to relay encrypted email attachments between each other, implement cryptographic keys and cryptographic functions so that the confidentiality, authenticity or integrity of the messages cannot be compromised when outside the TOE. Additionally, the environment will provide the necessary cryptographic components to protect the integrity and confidentiality of data; and

d) All administrators are assumed to be competent, to follow all guidance, and will maintain the security posture of the environment supporting the TOE.

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

a) The key lengths and cryptographic algorithms used by clients are set and enforced by the administrators prior to accepting registrations in the OCA vault;

b) The cryptographic implementations must be approved by the TOE administrators and comply with the Australian Information Security Manual (ISM) (Ref [1]); and

c) The clients must use SHA-1, AES with 256-bit keys and RSA with 2048 bit keys to encrypt the email attachments using S/MIME protocol. In accordance with the ISM, the cryptographic keys used should be those generated and distributed to the clients by the TOE.

Chapter 3 - Evaluation

3.1 Overview

39 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

40 The criteria against which the Target of Evaluation (TOE) has been evaluated are contained in the Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 3 (Refs [4], [5] and [6]). The methodology used is described in the Common Methodology for Information Technology Security Evaluation Version 3.1 Revision 3 (CEM) (Ref [7]). The evaluation was carried out in accordance with the operational procedures of the Australasian Information Security Evaluation Program (AISEP) (Refs [8], [9], [10] and [11]). In addition, the conditions outlined in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (Ref [12]) were also upheld.

3.3 Functional Testing

41 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 areas tested were secure interoperation, user authentication, 2D-MLS access control and security audit.

3.4 Penetration Testing

42 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.

43 The evaluators identified twelve potential vulnerabilities and nine of these were tested to determine whether the TOE was vulnerable to attack by attackers with a basic attack potential. Through testing, the evaluators found that the TOE was protected against these vulnerabilities.

44 Three vulnerabilities were not tested by the evaluators:

a) **Password brute force attack** – countered by enforced password complexity and suspension of account after three failed attempts. This was not tested as the attack potential calculations indicated that it was beyond a basic attack potential, based on the time required to calculate a password.

b) **Session hijacking** – not tested as the window of opportunity and knowledge required to execute this vulnerability are beyond a basic attack potential. This was verified when testing for communications interception.

c) **Failure to restrict URL access** – restrictions placed on URL access were partially verified in functional testing. Additional verification was incorporated into other tests.

Chapter 4 - Certification

4.1 Overview

45 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

46 After due consideration of the conduct of the evaluation as witnessed by the certifiers and of the Evaluation Technical Report (Ref [13]), the Australasian Certification Authority certifies the evaluation of OCA Incident Manager Version 1.1 performed by the Australasian Information Security Evaluation Facility, stratsec.

47 stratsec has found that OCA Incident Manager Version 1.1 upholds the claims made in the Security Target (Ref [2]) and has met the requirements of the Common Criteria (CC) evaluation assurance level EAL2 augmented with ALC_FLR.1.

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

4.3 Assurance Level Information

49 EAL2 provides assurance by a full security target and an analysis of the SFRs in that ST, using a functional and interface specification, guidance documentation and a basic description of the architecture of the TOE, to understand the security behaviour.

50 The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, security architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with a basic attack potential.

51 EAL2 also provides assurance through use of a configuration management system and evidence of secure delivery procedures.

4.4 Recommendations

52 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 [1]) and New Zealand Government users should consult the GCSB.

53 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) The TOE is used only in its evaluated configuration;

b) The use of cryptographic implementations approved by the TOE administrators and comply with the Australian Information Security Manual (ISM) and other Australian Government regulations;

c) The use of SHA-1, AES with 256-bit keys and RSA with 2048 bit keys to encrypt the email attachments using S/MIME protocol. In accordance with the ISM, the cryptographic keys used should be those generated and distributed to the clients by the TOE; and

d) Users and administrators ensure strict adherence to the delivery procedures.

Annex A - References and Abbreviations

A.1 References

[1] Australian Government Information Security Manual (ISM), Sept 2009, Defence Signals Directorate, (available at www.dsd.gov.au).

[2] Noggin OCA Incident Manager Version 1.1, Security Target Version 1.0, June 2010.

[3] Preparatory, Guidance and Online User Documentation, OCA Incident Manager v1.1, Noggin Pty Ltd.

[4] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model July 2009 Version 3.1 Revision 3 Final CCMB-2009-07-001.

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

[6] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components July 2009 Version 3.1 Revision 3 Final CCMB-2009-07-003.

[7] Common Methodology for Information Technology Security Evaluation (CEM) July 2009 Version 3.1 Revision 3 Final CCMB-2009-07-004

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

[9] AISEP Publication No. 2 – Certifier Guidance, AP 2. Version 3.3, 29 September 2007, Defence Signals Directorate.

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

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

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

[13] Evaluation Technical Report for OCA Incident Manager Version 1.1, 24 June 2010.

A.2 Abbreviations

ACA	Australasian Certification Authority
AES	Advanced Encryption Standard
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
ISM	Australian Government Information Security Manual
NTP	Network Time Protocol
OCA	Organise, Communicate, Act
OSP	Organisational Security Policy
PP	Protection Profile
RSA	Rivest, Shamir, Adleman public key encryption algorithm
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirements
SHA-1	Secure Hash Algorithm #1
S/MIME	Secure / Multipurpose Internet Mail Extensions
SSL	Secure Socket Layer
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy