Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Certification Report

Certificate Number: 2010/68

15 September 2010

Version 1.1

Amendment Record

Version	Date	Description
0.1	03/08/2010	Internal release.
0.2	04/08/2010	Extended review.
1.1	15/09/2010	Public release.

Executive Summary

1 The target of evaluation (TOE) is the Microsoft Exchange Server 2010 Enterprise (English) 64-bit. This is an e-mail and collaboration server that provides secure access to personal and shared data for a variety of clients using various protocols. Microsoft Exchange Server 2010 Enterprise (English) 64-bit is the Target of Evaluation (TOE).

2 The core functionality of the TOE includes:

a) **Flow Control**. The TOE provides filtering of mail traffic;

b) **Security Management**. This provides administrative functionality for the TOE; and

c) **Mobile Device Management**. The TOE has the ability to remotely manage Windows Mobile devices.

3 This report describes the findings of the IT security evaluation of Microsoft Corporation's Microsoft Exchange Server 2010 Enterprise (English) 64-bit to the Common Criteria (CC) evaluation assurance level EAL1 augmented with ALC_FLR.3. The report concludes that the product has met the target assurance level of EAL1 augmented with ALC_FLR.3 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 21 July 2010.

4 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;

b) operate it in accordance to the guidance documentation;

c) must not allow the TOE to be publically available until it is in the configured state; and

d) should have a thorough understanding of how the environment must be set up. The administrator should be familiar with requirements, integration into existing architectures and the application of certificate authorities.

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

6 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

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

1.2 Purpose

8 The purpose of this Certification Report is to:

a) report the certification of results of the IT security evaluation of the TOE, Microsoft Exchange Server 2010 Enterprise (English) 64-bit, against the requirements of the Common Criteria (CC) evaluation assurance level EAL1 augmented with ALC_FLR.3; and

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

9 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

10 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.

11 **Table 1: Identification Information**

Item	Identifier
Evaluation Scheme	Australasian Information Security Evaluation Program
TOE	Microsoft Exchange Server 2010 Enterprise (English) 64-bit
Software Version	2010 RTM (Build number 14.00.0639.021)
Security Target	Microsoft Exchange 2010 Security Target
Evaluation Level	EAL1 augmented with ALC_FLR.3
Evaluation Technical Report	Evaluation Technical Report for Microsoft Exchange 2010
Criteria	Common Criteria for Information Technology (IT) Security Evaluation, Version 3.1, revision 3 July 2009, CCMB-2009-07-003.

Methodology	Common Methodology, for Information Technology Security Evaluation, Evaluation methodology, July 2009, Version 3.1 Revision 3 CCMB-2009-07-004.
Conformance	CC Part 2 conformant CC Part 3 conformant augmented with Systematic Flaw Remediation (ALC_FLR.3)
Sponsor/Developer	Microsoft Corporation 1 Microsoft Way Redmond, WA 98052
Evaluation Facility	stratsec Deakin House, 1/50 Geils Ct, Deakin ACT 2600, Australia

Chapter 2 - Target of Evaluation

2.1 Overview

12 This chapter contains information about the 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

13 The TOE is called Microsoft Exchange Server 2010 Enterprise (English) 64-bit developed by Microsoft Corporation. This is an e-mail and collaboration server that provides secure access to personal and shared data for a variety of clients using various protocols. Exchange clients include internal or external phones and faxes, personal computers running Outlook client and Outlook web application and smart phones using Exchange Active Sync. As detailed in Figure 1 - diagram of the TOE, the areas that comprise of the TOE are:

a) Mailbox server role;

b) Client Access server role;

c) Unified Messaging server role;

d) Hub Transport server role; and

e) Edge Transport server role including:
   (i) mail flow and
   (ii) filtering

2.3 Security Policy

14 The TOE Security Policy (TSP) is a set of rules that defines how the information within the TOE is managed and protected. The TSP is defined in the Security Target (Ref [1]). A summary of the TSP is provided below:

a) **Connection filtering**. The TOE protects from unwanted spam or Unsolicited Commercial E-mail (UCE) by blocking messages from specified IP addresses;

b) **Message filtering**. The TOE filters potential spam messages based on administrator configured SMTP filters, including local and third party block/allow lists;

c) **Attachment filtering**. This provides a mechanism to filter potentially harmful attachments from external networks;

d) **Transport filtering**. The TOE allows the administrator to define mail policies to prevent specific internal external users from emailing each other;

e) **Access control**. This protects mailboxes and public folders from unauthorized access;

f) **Identification and authentication**. This provides identification and authentication mechanism for the Outlook Voice Access functionality in cases where Outlook Voice Access is not secured by the use of the transport layer security protocol;

g) **Distribution group restriction**. Requires users sending mail to a distribution group to be successfully authenticated and to be authorised; and

h) **Remote device wipe**. An administrator can issue a command to wipe a Windows Mobile device in the event that the device may have been compromised.

2.4 TOE Architecture

15 The TOE comprises software installed on Windows servers and its related guidance documentation. An installation of the TOE can be found in Figure 1 - diagram of the TOE and consists of the server roles components identified.

16 The TOE consists of the following major architectural components:

a) **Mailbox server role.** The Mailbox server role hosts mailbox and public folder databases. The administrator manages e-mail lifecycle folders and policies from a Mailbox server. The Mailbox server role, in conjunction with the environment, provides access control for users, mail, fax and voice messages;

b) **Client Access server role.** This is the server that hosts the client protocols. The Client Access server also exposes a Web Services interface for application developers. The Client Access server role accepts connections to the Exchange 2010 server from messaging clients;

c) **Unified Messaging server role.** This combines voice messaging, fax, calendaring and email, which are accessible from a telephone or computer. Exchange Server 2010 Unified Messaging integrates Exchange Server with telephony networks and brings Unified Messaging features to the core of Exchange Server. Outlook Voice Access (OVA) is a feature of the Unified Messaging role and lets users access their mailbox using telephone communications;

d) **Hub Transport server role.** This is the mail routing server that routes mail within the Exchange organisation. The Hub Transport server role handles all mail flow inside the organisation, applies transport rules, applies journaling policies and delivers messages to the recipient's mailbox. Messages that are sent to the internet are relayed by the Hub Transport server to the Edge Transport server role that is deployed in the perimeter network;

e) **Edge Transport server role.** This is the mail routing server that sits at the perimeter of the network topology and routes mail into and out of the Exchange organisation. The Edge Transport server role handles the following scenarios:

i) **Mail flow** - The Edge Transport server role accepts mail coming into the Exchange Server 2010 organisation from the internet and routes all outbound messages to the internet.

ii) **Filtering** - The Edge Transport server role helps protect the Exchange Server 2010 organisation from spam by filtering inbound messages as they arrive and before they are delivered to the internal private network.

17 All roles, with the exception of the Edge Transport server, can be installed on a single machine; for reasons of performance, in medium and large organisation installations, these roles may be installed on more than one physical server. The TOE roles communicate in the same way, whether they are installed on one server or many servers. More information about the installation of the TOE will be provided in the related guidance documents ref [2].

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

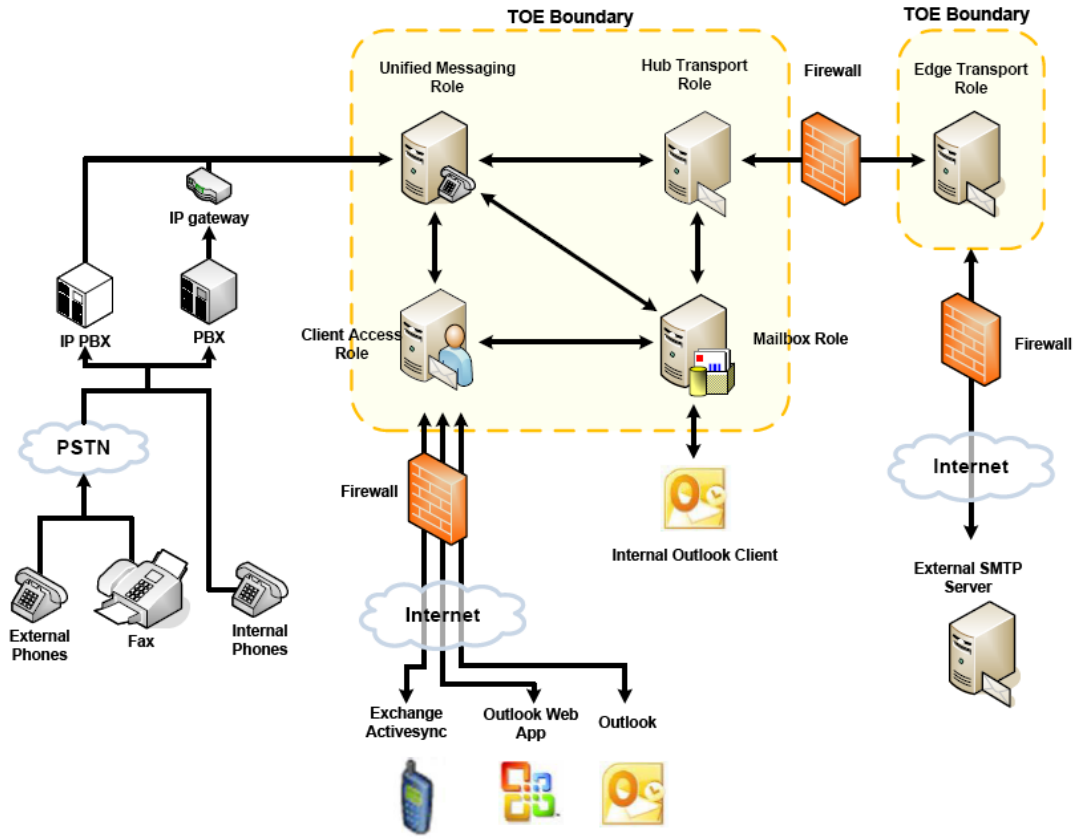

Figure 1 - diagram of the TOE

2.5 Clarification of Scope

19 The scope of the evaluation was limited to those claims made in the Security Target (Ref [1]). The assurance package for the evaluation of the TOE is Evaluation Assurance Level 1 (EAL1) augmented with Systematic Flaw Remediation (ALC_FLR.3).

20 EAL1 provides a basic level of assurance by a limited security target and an analysis of the SFRs in that ST using a functional and interface specification and guidance documentation, to understand the security behaviour.

21 The TOE offers its services for users via protocols including:

a) RPC for applications like Outlook 2010;

b) SMTP for generic clients and servers sending e-mail to the TOE;

c) HTTP for web browsers (using Outlook web access) and for Active Sync clients;

d) RPC tunnelled over http;

e) Web Services Application Programming Interface (API) for in-house applications; and

f) SIP/RTP for Outlook Voice Access (OVA).

22 The scope of the TOE ends at the interfaces where it provides its services and does not include any functionality of any client.

2.5.1 Evaluated Functionality

23 The TOE provides the following evaluated security functionality:

a) **Flow control**: connection filtering, message filtering, attachment filtering and transport filtering;

b) **Security management**: access control, identification and authentication, distribution group restriction and mailbox and public folder quota; and

c) **Mobile device management**: managing security policies and performing remote device wipe.

2.5.2 Non-evaluated Functionality

24 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 [3]) 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).

25 The following protocols are included in the Exchange product, but outside the logical scope of the TOE: IMAP4 and POP3.

26 Also, all clients that can be used to connect to the TOE are not addressed during the evaluation. For features of the TOE that rely on the use of external lists for filtering of email messages it should be noted that the way these external lists are complied and transferred to the TOE are out of scope of the evaluation.

2.6 Usage

2.6.1 Evaluated Configuration

27 The evaluated configuration is described in the guidance documentation Ref [2]. All required configurations are set during the post installation tasks or by use of administrator accessible functions. Australian Government users should refer to the ISM (Ref [3]) to ensure that the configurations meet the minimum Australian Government policy requirements. New Zealand Government users should consult the Government Communications Security Bureau (GCSB).

28 The product installation has been performed across three phases:

a) Environment preparation- installing the Active Directory server with DNS and installing Windows 2008 across the TOE servers;

b) Installing the server roles. This involves installing the mailbox, the Hub Transport server, the Edge Transport server and the Client Access server with the unified messaging role. For each role, a guided installation was performed.

c) Post installation. This involves configuring the TOE to its evaluated configuration.

2.6.2 Preparing the environment

29 Before the installation of the TOE, the operating system has to be installed on each machine.

30 The supported operating system is Windows Server 2008 R2 Standard and Enterprise Edition ([3]). The following software must also be installed on all Exchange servers:

a) Microsoft .NET Framework Version 4. http://www.microsoft.com/downloads/details.aspx?FamilyID=9cfb2d51-5ff4-4491-b0e5-b386f32c0992&displaylang=en

b) Microsoft Windows PowerShell v2.0 and Windows Remote Management (WinRM) 2.0. For download information, see Microsoft Knowledge Base article 968929, Windows Management

Framework (Windows PowerShell 2.0, WinRM 2.0 and BITS 4.0). http://support.microsoft.com/kb/968929

c) Microsoft Windows Installer 4.5 (or above) http://go.microsoft.com/fwlink/?LinkId=151819.

31 Exchange Server 2010 requires that you do not have the Network News Transfer Protocol (NNTP) service or the Simple Mail Transfer Protocol (SMTP) service installed.

32 Active directory is another requirement of the TOE environment. In order to install Active Directory, a DNS server needs to be set up. This can be done automatically during the installation of Active Directory.

33 For preparation of Active Directory and domains for Exchange 2010, refer to:

a) Microsoft Exchange 2010 Help: Exchange Server 2010>Planning and Deployment>Planning for Exchange 2010> Planning Active Directory for the preparation of Active Directory and domains for Exchange 2010.
Online: http://technet.microsoft.com/en-us/library/bb125224.aspx

34 An IP gateway is required in the environment. For information about the IP/VoIP gateways to use with the Unified Messaging server role, refer to:

a) Microsoft Exchange 2010 Help: Exchange Server 2010>Unified Messaging>Understanding Unified Messaging>Understanding Unified Messaging Components>Understanding Unified Messaging IP Gateways.
Online: http://technet.microsoft.com/en-us/library/bb123890.aspx

35 Finally, any internet connection to a server role needs to be appropriately secured by a firewall. The evaluators have used Microsoft ISA 2006 as the configured firewall.

36 For the use of the Microsoft Server 2010 Setup wizard to perform an installation of Exchange 2010, refer to:

a) Microsoft Exchange 2010 Help: Exchange Server 2010>Planning and Deployment>Deploying Exchange 2010>New Installation of Exchange 2010>Install Exchange Server 2010.
Online: http://technet.microsoft.com/en-us/library/bb124778.aspx

2.6.3 Product Key configuration

37 Logon to the server with an account that has local administrative access and has been delegated the exchange organisation administrator role.

a) Start the **exchange management** console.

b) In the console tree, expand **server configuration**.

c) In the result pane, select the server that you want to license.

d) In the action pane, under the server name, click **enter product key**. The **enter product key** wizard appears.

e) On the **enter product key** page, type the product key for the exchange server and then click enter.

f) Restart the **Microsoft Exchange information store** service so that the change is applied.

2.6.4 Delivery procedures

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

39 Exchange Server 2010 Enterprise Edition is available in a retail box with certificate of authenticity (COA) label on a box.

40 There is a **product version number** and for each executable there is a **file version number**. When the product is shipped, these version numbers will be the same, though they will be in a different format and the same number may be displayed in different formats. During development, some files may be revised and therefore have a different **file version number** as that number includes the rev or revision number.

2.6.5 Determining the Evaluated Configuration

41 There are two methods to examine the version of an instance of Exchange Server 2010, from the properties of the executable file and from the Exchange 2010 administrative console. Either can be used to determine the version number of an instance of Exchange Server. Note that a version number in the format “14.x.y.z” can also be read as “version 14.x (build y.z)”. Both versions are equivalent.

42 The file version number or the product version number 14.x.y.z verifies that the instance corresponds to the evaluated version named in the ST “Exchange Server 2010”. The numbers “14.x” in the file version number and the product version number both indicate Exchange Server 2010.

43 The version numbering scheme of the executable parts of the TOE is defined as following: Exchange Server is labelled 14.x.y.z.

44 To see the Exchange version, from the Exchange Management shell, enter the Cmdlet “get-ExchangeServer | fl” and check “AdminDisplayVersion” for the version number of Exchange Server 2010 and “Edition” for the product version.

45 When “AdminDisplayVersion” equals “version 14.0 (build 639.21)” and “edition” equals “Enterprise” the correct version of the TOE has been installed.

2.6.6 Documentation

46 It is important that the TOE is used in accordance with guidance documentation in order to ensure the secure usage. The following documentation is provided by the developer to ensure secure use of the product.

a) Microsoft Exchange 2010 help ref [2]; and

b) E14_EAL1_AGD_Guidance_Documentation

2.6.7 Secure Usage

47 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.

48 The setup of the environment is to be done to security best practice;

49 In order to reach the evaluated configuration, the following settings are applied:

a) The environment requires an active directory controller, a firewall, a PBX server with SIP enabled, separate servers for each role and a network to facilitate communications between all of these.

b) Restricting access to the operating platforms to administrators only;

c) Implementation of a PIN based authentication mechanism for Outlook;

d) Voice Access;

e) Enable encryption between clients and the server;

f) Configure the outlook address book;

g) Configure public access (if required);

h) Setting up the edge server subscription for data replication between the transport servers;

i) Restrict access to distribution groups as required;

j) Implement message filtering;

k) Implement connection filtering;

l) Implement attachment filtering;

m) Implement transport filtering; and

n) Implement device policies.

Chapter 3 - Evaluation

3.1 Overview

50 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

51 The criteria against which the Target of Evaluation (TOE) has been evaluated is contained in the Common Criteria for Information Technology Security Evaluation (Refs [4], [5], [6]). The methodology used is described in the Common Methodology for Information Technology Security Evaluation (CEM) (Ref [7]). The evaluation was also 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

52 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 SMTP service access rules and attachment filter rules, Powershell admin rights, voice access PIN restrictions, active sync device connectivity and active directory distribution.

3.4 Penetration Testing

53 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.

54 The evaluators identified potential vulnerabilities and 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.

VULNERABILITY	*TEST / JUSTIFICATION*
SMTP fuzzing	The evaluators observed in the process of evaluation that there is a publically facing SMTP interface as a part of the evaluated configuration. The evaluators would like to assess the interfaces vulnerability to malformed data.
Microsoft Security Bulletin MS10-024(CVE-2010-0025)	The vulnerability could allow denial of service attack if an attacker sent a specially crafted DNS response to a computer running the SMTP service. This meant to be addressed through applying patches in accordance with flaw remediation procedures.
General vulnerability scan	The evaluators will perform a general scan of the environment for threats of a basic attack potential.

55 The results of the tests did not identify any vulnerabilities with a basic attack potential.

Chapter 4 - Certification

4.1 Overview

56 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

57 After due consideration of the conduct of the evaluation as witnessed by the certifiers and of the Evaluation Technical Report (Ref [14]), the Australasian Certification Authority certifies the evaluation of Microsoft Exchange Server 2010 Enterprise (English) 64-bit performed by the Australasian Information Security Evaluation Facility, stratsec.

58 stratsec has found that Microsoft Exchange Server 2010 Enterprise (English) 64-bit upholds the claims made in the Security Target (Ref [1]) and has met the requirements of the Common Criteria (CC) evaluation assurance level EAL1 augmented with ALC_FLR.3.

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

4.3 Assurance Level Information

60 EAL1 provides a basic level of assurance by an analysis of the security functions using a functional and interface specification and guidance documentation, to understand the security behaviour.

61 The analysis is supported by independent testing of the TOE security functions.

4.4 Recommendations

62 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 [3]) and New Zealand Government users should consult the Government Communications Security Bureau (GCSB).

63 In addition to ensuring that the assumptions concerning the operational environment are fulfilled and the guidance document is followed (Ref [2]). The ACA also recommends that users and administrators should consider the following points when deploying Microsoft Exchange 2010:

a) The administrator must not allow the TOE to be publically available until it is in its configured state; and

b) The administrator should have a thorough understanding of how the environment must be set up. The administrator should be familiar with requirements, integration into existing architectures and the application of certificate authorities.

Annex A - References and Abbreviations

A.1 References

[1] Microsoft Exchange 2010 Security Target v0.5 30 May 2010.

[2] Microsoft Exchange Server 2010 (available at: http://technet.microsoft.com/en-us/library/bb124558.aspx)

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

[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] Microsoft Exchange 2010 Help (available at: http://technet.microsoft.com/en-au/library/aa996058(EXCHG.80).aspx)

[14] Evaluation Technical Report for Microsoft Exchange 2010 Version 1.0, 5 July 2010.

A.2 Abbreviations

AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Program
API	Application Programming 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
HTTP	Hypertext Transfer Protocol
IMAP4	Internet Message Access Protocol 4
OVA	Outlook Voice Access
POP3	Post Office Protocol 3
PP	Protection Profile
RPC	Remote Procedure Call
RTP	Real Time Protocol
SFP	Security Function Policy
SFR	Security Functional Requirements
SIP	Session Initiation Protocol
SMTP	Simple Mail Transport Protocol
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy