Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Certification Report

Certificate Number: 2009/58

17 September 2009

Version 1.0

Amendment Record

Version	Date	Description
1.0	17 Sep 2009	Public release.

Executive Summary

1 System Center Mobile Device Manager 2008 is a product that is designed to provide a secure management and monitoring solution for Windows Mobile-powered devices. System Center Mobile Device Manager 2008 is the Target of Evaluation (TOE).

2 The core functionality of the TOE includes:

a) **Device security management.** The TOE provides administrators with the capability to enrol and manage Windows Mobile devices.

b) **Device configuration management.** The TOE provides administrators with the capability to review the configuration of Windows Mobile devices and distribute software to the devices.

c) **Mobile VPN capability.** The TOE implements standards-based communications so that Mobile Users can securely access the enterprise environment.

d) **SCMDM Management.** The TOE controls access so that only authorised administrators can perform device management functions and ensures that all communication between MDM components is secure.

3 This report describes the findings of the IT security evaluation of Microsoft Corporation's System Center Mobile Device Manager 2008, to the Common Criteria (CC) evaluation assurance level EAL4 augmented with ALC_FLR.3 (EAL4+). The report concludes that the product has met the target assurance level of EAL4+ and that the evaluation was conducted in accordance with Common Criteria and Australasian Information Security Evaluation Program (AISEP) requirements. The evaluation was performed by stratsec and was completed on 20 July 2009.

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

a) administrators ensure that the TOE is operated in the evaluated configuration and that assumptions concerning the TOE security environment (Ref [1]) are fulfilled;

b) administrators operate the TOE according to the administrator guidance document (Ref [2]); and

c) administrators maintain the underlying environment in a secure manner so that the integrity of the TOE security functions is preserved.

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

1 INTRODUCTION 1

1.1 OVERVIEW 1
1.2 PURPOSE 1
1.3 IDENTIFICATION 1

2 TARGET OF EVALUATION 2

2.1 OVERVIEW 2
2.2 DESCRIPTION OF THE TOE 2
2.3 TOE ARCHITECTURE 4
2.4 CLARIFICATION OF SCOPE 4
2.4.1 Evaluated Functionality 5
2.4.2 Non-evaluated Functionality 6
2.5 USAGE 6
2.5.1 Evaluated Configuration 6
2.5.2 Delivery procedures 7
2.5.3 Determining the Evaluated Configuration 7
2.5.4 Documentation 8
2.5.5 Secure Usage 9

3 EVALUATION 10

3.1 OVERVIEW 10
3.2 EVALUATION PROCEDURES 10
3.3 FUNCTIONAL TESTING 10
3.4 PENETRATION TESTING 10

4 CERTIFICATION 11

4.1 OVERVIEW 11
4.2 CERTIFICATION RESULT 11
4.3 ASSURANCE LEVEL INFORMATION 11
4.4 RECOMMENDATIONS 12

ANNEX A - REFERENCES AND ABBREVIATIONS 13

A.1 REFERENCES 13
A.2 ABBREVIATIONS 15

1 Introduction

1.1 Overview

7 This chapter contains information about the purpose of this document and how to identify the 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, System Center Mobile Device Manager 2008, against the requirements of the Common Criteria (CC) evaluation assurance level EAL4+, 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 2.5.1 Evaluated Configuration.

Table 1: Identification Information

Item	**Identifier**
Evaluation Scheme	Australasian Information Security Evaluation Program
TOE	System Center Mobile Device Manager 2008
Software Version	System Center Mobile Device Manager 2008 with KB950135, KB951311 and KB951840 hotfixes
Security Target	System Center Mobile Device Manager 2008 Security Target, Version 1.2, 30 June 2009
Evaluation Level	EAL4
Evaluation Technical Report	Evaluation Technical Report for System Center Mobile Device Manager 2008, Version 1.3, 01 September 2009
Criteria	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2, September 2007, with interpretations as of 29 May 2008

Methodology	Common Methodology for Information Technology Security Evaluation, Evaluation methodology, September 2007, Version 3.1 Revision 2, CCMB-2007-09-004
Conformance	Common Criteria Part 2 conformant. Common Criteria Part 3 conformant, EAL4 augmented with ALC_FLR.3.
Sponsor/Developer	Microsoft Corporation 1 Microsoft Way, Redmond WA 98052-8300 USA
Evaluation Facility	stratsec Suite 1, 50 Geils Court, Deakin, ACT 2600, Australia

2 Target of Evaluation

2.1 Overview

11 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

12 The TOE is the System Center Mobile Device Manager 2008 (SCMDM, also referred to as MDM) developed by Microsoft Corporation.

13 The TOE is an enterprise server solution designed to provide a secure management and monitoring solution for Windows Mobile-powered devices. The TOE empowers administrators to provide secure data and network access for their mobile workforce, while retaining a high degree of control over their mobile device usage.

14 The TOE provides a security management platform for Windows Mobile phones with over 130 policies and settings and built-in mechanisms that help prevent the misuse of corporate data. Administrators can lock down many areas of the Windows Mobile Smartphone’s and Pocket PCs, including certain communications and device functionality, application installation and execution settings and more. The TOE can be used to manage security on all Windows Mobile devices across the enterprise network, from an enterprise wide perspective down to individual Windows Mobile devices and users.

15 The TOE is a simple and comprehensive solution for distributing software to Windows Mobile devices and maintaining an inventory of devices in a complex organisational environment. The TOE enables cost-effective device enrollment through over-the-air (OTA) provisioning and

bootstrapping and helps administrators streamline device management through role–based administration, MMC snap-ins, and Microsoft Windows PowerShell™ cmdlets. Comprehensive reporting tools within Mobile Device Manager provide IT professionals with improved visibility of devices and helps reduce the cost and complexity of managing devices within a corporate network.

16 The TOE is designed to facilitate a seamless user experience across cellular or Wi-Fi data connections. The solution provides a single point for security–enhanced, behind-the-firewall access to corporate data and line of business (LOB) applications. With the TOE, administrators can facilitate security over public wireless networks through a Mobile virtual private network (VPN) link. The VPN link secures wireless communications between a Windows Mobile device and corporate servers through an SSL–encrypted tunnel, underpinned by an IPsec encrypted tunnel between the Windows Mobile device and MDM gateway. This dual layered combination of IPsec and SSL encryption, both implementing mutual certificate based authentication lends a definite edge over other systems that generally use a single security barrier. With features such as fast reconnect and session persistence, Mobile VPN also helps maintain connectivity whilst reducing bandwidth overheads.

17 Figure 1 illustrates a typical enterprise environment incorporating the TOE.

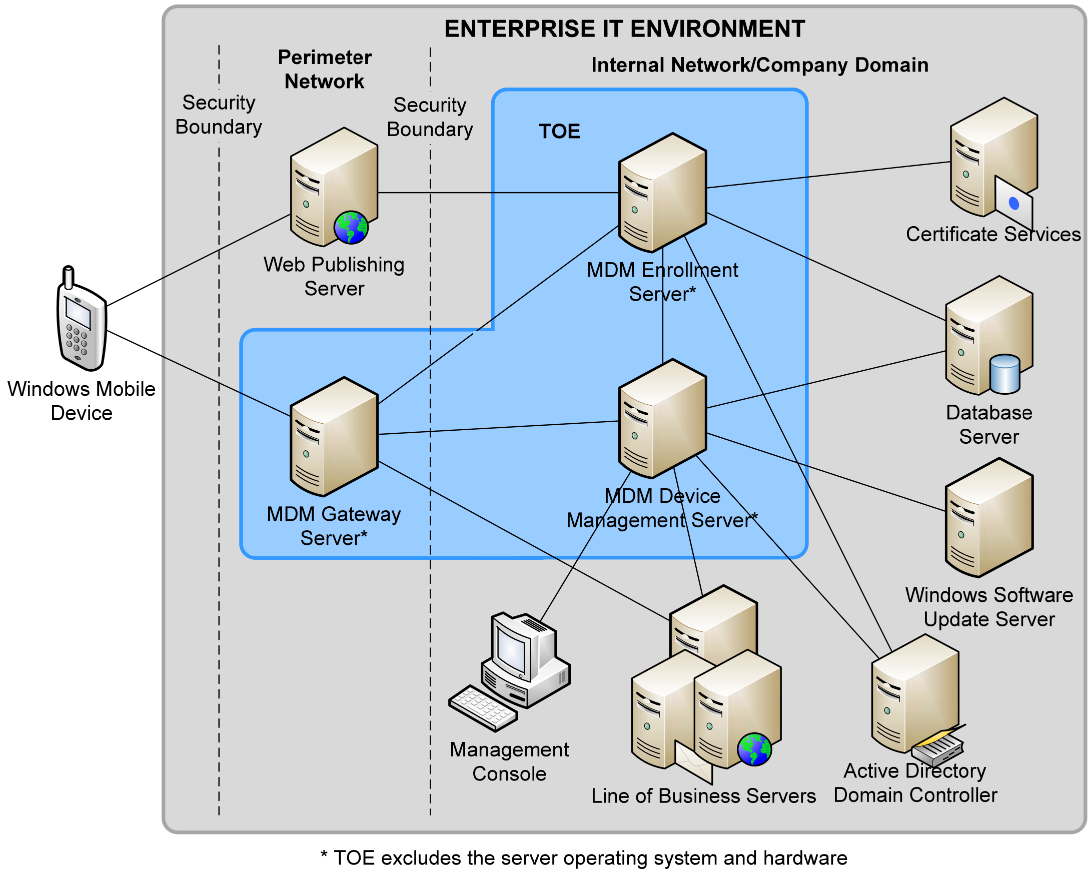

Figure 1 – SCMDM Environment

2.3 TOE Architecture

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

19 The TOE comprises the three server roles that make up the System Center Mobile Device Manager 2008. The TOE exists within an enterprise operating environment and is supported through communications with a number of enterprise resources that are not within the scope of the TOE.

20 The TOE does not include the server operating system and hardware for the three SCMDM server roles. The TOE comprises the SCMDM software components that are installed and operate within the environment provided by the underlying Microsoft Windows server operating system and greater enterprise IT environment.

21 The Developer's Architectural Design identifies the following components of the TOE:

a) The MDM Enrollment server.

- Provides an over-the-air (OTA) process for requesting and retrieving certificates for mobile devices and for creating the Active Directory objects through which the device itself may be considered domain joined. The Enrollment server essentially acts as a proxy that enforces a set of security mandates and requirements on connecting devices through a set of checks and validations to permit them to be enrolled into the domain.

b) The MDM Device Management server.

- Provides the central administration point for devices and Device Management servers. MDM Device Management server transforms enterprise data and commands into Open Mobile Alliance Device Management (OMA DM) compliant commands that are sent to the Mobile Device.

c) The MDM Gateway server.

- Facilitates connectivity between the Mobile Device and the MDM Device Management server (as well as Line-of-business servers if configured) once the device has been successfully enrolled. The Gateway server terminates the IPSec VPN (Mobile VPN) established between the Mobile Device and enterprise and routes traffic accordingly.

2.4 Clarification of Scope

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

2.4.1 Evaluated Functionality

The TOE provides the following evaluated security functionality:

Table 1 - SCMDM Security Features

TOE security function	TOE security feature
Device security management. The TOE provides administrators with the capability to enroll and manage Windows Mobile devices.	**Device enrollment.** The TOE provides the capability to securely enroll a Windows Mobile device to build a trust relationship.
	Managing security policies. The TOE provides the capability to configure and enforce security policy settings on managed Windows Mobile devices.
	Managing device block. The TOE provides the capability to block a managed Windows Mobile device from establishing a VPN and accessing the enterprise network.
	Performing remote device wipe. An administrator can issue a command to wipe a managed Windows Mobile device in the event that the device may have been compromised.
Device configuration management. The TOE provides administrators with the capability to review the configuration of Windows Mobile devices and distribute software to the devices.	**Software Distribution.** The TOE has the ability to distribute software packages and updates to Windows Mobile devices.
	Managing device inventory. The TOE provides the capability to view different types of current information on managed Windows Mobile devices.
Mobile VPN capability. The TOE implements standards-based communications so that Mobile Users can securely access the enterprise environment.	**Implementing IPsec capability.** The TOE implements standard IPsec ESP to provide encryption communications between itself and a managed Windows Mobile device.
	Facilitating secure enterprise access. The TOE supports mutual certificate authenticated, SSL encrypted communications between Windows Mobile devices and enterprise services and MDM administration servers.
	Line of business access control. The TOE provides administrators with the capability to define the enterprise LOB servers that Windows Mobile devices can connect to.
SCMDM Management. The TOE controls access so that only authorized administrators can	**Implementing role-based access control.** The TOE applies roles to authorized administrators to control access to the range of device management functions.

TOE security function	TOE security feature
perform device management functions and ensures that all communication between MDM components is secure.	**Transferring data internally securely.** The TOE implements a trusted communications path between the physically separate components of the TOE.

2.4.2 Non-evaluated Functionality

23 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 [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).

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

a) Server operating systems and hardware;

b) Windows Mobile devices and MDM client software;

c) Database server;

d) Windows Software Update Server (WSUS);

e) Certificate services;

f) Active directory domain service;

g) Line Of Business (LOB) application servers;

h) Web publishing server;

i) Management console;

j) Internet Information Services (IIS); and

k) Group Policy Management Console (GPMC) and Group Policy extensions.

2.5 Usage

2.5.1 Evaluated Configuration

25 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 [3]) for

guidance on Australian Government policy requirements. New Zealand Government users should consult the GCSB.

26 The evaluated configuration is based on a default installation of the TOE from the installation medium. The installation script by default installs the TOE to C:\Program Files\System Center Mobile Device Manager. This installation path may be changed at install time without affecting the evaluated configuration. The only other user input required is to specify the start menu folder to create (or confirm the use of the default). The evaluated configuration is described in greater detail in the Installation and Administration Guide (Ref [2]).

2.5.2 Delivery procedures

27 The TOE (and associated hotfix update) is only available to end-users by means of download from the Microsoft website, no physical media (for the Volume License version which is the TOE) is currently provided. The package files are available from the Microsoft website for secure (SCMDM install file) or unsecure (hotfix files) download.

2.5.3 Determining the Evaluated Configuration

2.5.3.1 SCMDM Installation File

28 The end user should perform the following steps:

a) Right click the downloaded file and select properties.

b) Click on the Digital Signatures tab.

c) Confirm that the file has been signed by Microsoft Corporation.

d) Verify that the certification path is correct by performing the following:

1. Under the Digital Signatures tab, click on Microsoft Corporation and then the Details button.

2. Click on View Certificate.

3. Click on the Certification Path and confirm that the path stems from the Microsoft Root Authority.

2.5.3.2 KB951840 Hotfix File (Includes KB950135 and KB951311)

29 The end user should perform the following steps:

a) Right click the downloaded update file and select properties.

b) Click on the Digital Signatures tab.

c) Confirm that the file has been signed by Microsoft Corporation.

d) Verify that the certification path is correct by performing the following:

1. Under the Digital Signatures tab, click on Microsoft Corporation and then the Details button.

2. Click on View Certificate.

3. Click on the Certification Path and confirm that the path stems from the Microsoft Root Authority.

2.5.3.3 Confirm version of TOE

30 Once each of the server components have been installed with the necessary software go to the MCC console (MMC.exe) on the MDM Server perform the following:

a) Open File > Add/Remove Snap-in

b) Select the Mobile Device Manager snap-in and go to the Server key and check that each server role has the following version information:

1. Enrollment Server – Version 1.0 (Build 2300.0)

2. Device Management Server – Version 1.0 (Build 2300.6)

3. Gateway Server – Version 1.0 (Build 2300.6)

2.5.4 Documentation

31 It is important that the TOE is used in accordance with guidance documentation in order to ensure secure use of the product. The following documentation is provided with the TOE:

a) System Center Mobile Device Manager 2008 Installation and Administrator Guide (Ref [2]).

b) Architecture Guide for System Center Mobile Device Manager 2008 (Ref [4])

c) Deployment Guide for System Centre Mobile Device Manager 2008 (Ref [5])

d) Planning Guide for System Center Mobile Device Manager 2008 (Ref [6])

e) Security Considerations in Mobile Device Manager (Ref [7])

2.5.5 Secure Usage

32 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.

33 The following assumptions were made:

Table 2 - SCMDM Assumptions

Identifier	Assumption statement
A.IT_AUTH	The IT environment will provide a mechanism for authenticating Mobile Users when accessing enterprise applications, data and services.
A.IT_CERT	The IT environment will provide certificate services for the TOE and line of business servers to support certificate provisioning and secure channel establishment with managed Windows Mobile devices.
A.IT_CHANNEL	The IT environment will provide the client-side of a secure channel between the MDM Gateway Server and the managed Windows Mobile device.
A.ENTERPRISE	The MDM Device Management Server, MDM Enrollment Server, Domain Controller, Database Server, Certificate Services, Windows Server Updates Services and Administration Console are located within the enterprise boundary (company domain) and are protected from unauthorized logical and physical access.
A.PERIMETER	The MDM Gateway Server and Web Publishing Server are located within the perimeter network and are protected from unauthorized physical access. These servers are also protected from unauthorized logical access, however are considered more prone to compromise than servers that reside within the company domain (as assumed in A.ENTERPRISE) as they reside in a perimeter environment that is exposed to the Internet.
A.ADMIN	Administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by administrator documentation.

3 Evaluation

3.1 Overview

34 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

35 The criteria against which the TOE has been evaluated are contained in the Common Criteria for Information Technology Security Evaluation Version 3.1 (Refs [8], [9], [10]). The methodology used is described in the Common Methodology for Information Technology Security Evaluation version 3.1 (CEM) (Ref [11]). The evaluation was carried out in accordance with the operational procedures of the Australasian Information Security Evaluation Program (AISEP) (Refs [12], [13], [14], [15]). In addition, the conditions outlined in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (Ref [16]) were also upheld.

3.3 Functional Testing

36 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 confirmed that the actual test results were consistent with the expected test results.

3.4 Penetration Testing

37 Penetration testing was conducted based on an independent vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design, security architecture description, implementation representation as well as available public information. The evaluators used these tests to determine that 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 testing:

a) Time taken to identify and exploit (elapsed time);

b) Specialist technical expertise required (specialist expertise);

c) Knowledge of the TOE design and operation (knowledge of the TOE);

d) Window of opportunity; and

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

38 The analysis conducted by the evaluators and the subsequent testing effort indicated that the TOE will resist an attacker with Enhanced Basic potential. This is consistent with the requirements of the EAL 4+ ALC_FLR.3 assurance level.

4 Certification

4.1 Overview

39 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

40 After due consideration of the conduct of the evaluation as witnessed by the certifiers, and of the Evaluation Technical Report (Ref [17]), the Australasian Certification Authority certifies the evaluation of System Center Mobile Device Manager 2008 performed by the Australasian Information Security Evaluation Facility, stratsec.

41 stratsec has found that System Center Mobile Device Manager 2008 upholds the claims made in the Security Target (Ref [1]) and has met the requirements of the Common Criteria (CC) evaluation assurance level EAL4+.

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

4.3 Assurance Level Information

43 EAL4 provides assurance by a full security target (ST) and an analysis of the security functions in that ST, using a functional and complete interface specification, guidance documentation, a description of the basic modular design of the TOE and a subset of the implementation to understand the security behaviour.

44 The analysis is supported by independent testing of the TOE security functions, evidence of developer testing based on the functional specification and TOE design, selective independent confirmation of the developer test results, and an independent vulnerability analysis demonstrating resistance to penetration attackers with an Enhanced-Basic attack potential.

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

4.4 Recommendations

46 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 GCSB.

47 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:

a) administrators ensure that the TOE is operated in the evaluated configuration and that assumptions concerning the TOE security environment (Ref [1]) are fulfilled;

b) administrators operate the TOE according to the administrator guidance document (Ref [2]); and

c) administrators maintain the underlying environment in a secure manner so that the integrity of the TOE security functions is preserved.

Annex A - References and Abbreviations

A.1 References

[1] System Center Mobile Device Manager 2008 Security Target, Version 1.2, 30 June 2009

[2] System Center Mobile Device Manager 2008 Installation and Administrator Guide version 1.0, June 2009

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

[4] Architecture Guide for System Center Mobile Device Manager 2008, Microsoft, 1-April-2008, SCMDM08Architecture.doc.

[5] Deployment Guide for System Center Mobile Device Manager 2008, Microsoft, 1-April-2008, SCMDM08Deployment.doc.

[6] Planning Guide for System Center Mobile Device Manager, Microsoft, 1-April-2008, SCMDM08Planning.doc.

[7] Security Considerations in Mobile Device Manager, Microsoft, 1-April-2008, SecurityConsid_MDM.doc.

[8] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model (CC), Version 3.1, Revision 1, September 2006, CCMB-2006-09-001, Incorporated with interpretations as of 2008-05-29

[9] 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 2008-05-29

[10] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components (CC), Version 3.1, Revision 2, September 2007, CCMB-2007-09-003, Incorporated with interpretations as of 2008-05-29

[11] Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1, Revision 2 September 2007, CCMB-2007-09-004 Incorporated with interpretations as of 2008-05-29

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

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

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

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

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

[17] Evaluation Technical Report for System Center Mobile Device Manager 2008, Version 1.3, 01 September 2009

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
CCMB	Common Criteria Maintenance Board
CEM	Common Evaluation Methodology
DSD	Defence Signals Directorate
EAL	Evaluation Assurance Level
ESP	Encapsulating Security Payload
ETR	Evaluation Technical Report
FLR	Flaw Remediation
GCSB	Government Communications Security Bureau
GPMC	Group Policy Management Console
IIS	Internet Information Service
IPsec	Internet protocol Security
ISM	Information Security Manual
LOB	Line Of Business
MDM	Mobile Device Manager
MMC	Microsoft Management Console
OMA DM	Open Mobile Alliance Device Management
OTA	Over-The-Air
PP	Protection Profile
ROQ	Release Only Quality
SCMDM	System Center Mobile Device Manager
SFP	Security Function Policy
SFR	Security Functional Requirements
SQL	Structured Query Language
SSL	Secure Socket Layer
ST	Security Target
SSL	Secure Socket Layer
TOE	Target of Evaluation

TSF	TOE Security Functions
TSP	TOE Security Policy
VPN	Virtual Private Network
WSUS	Windows Software Update Server