Australasian Information Security Evaluation Program

Certification Report

Certificate Number: 2008/45

10 March 2008

Version 1.0

Amendment Record

Version	Date	Description
1.0	10/03/2008	Public release.

Executive Summary

1 Windows Mobile 5.0 with Messaging and Security Feature Pack (MSFP) is a compact operating system for use on Pocket PCs and Smartphones enabling users to extend their corporate Windows desktop to mobile devices in a secure manner. Windows Mobile 5.0 with MSFP is the Target of Evaluation (TOE).

2 This report describes the findings of the IT security evaluation of Microsoft Corporation's Windows Mobile 5.0 with MSFP, to the Common Criteria Evaluation Assurance Level 2 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 relevant criteria and the requirements of the Australasian Information Security Evaluation Program. The evaluation was performed by stratsec and was completed on 10 March 2008.

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

a) are aware that information stored on external storage cards is not protected;

b) review the security of default applications;

c) consider the necessity of pre-installed certificates contained within the certificate stores;

d) maintain awareness of the evaluated configuration;

e) not accept Service Indicator or Service Loader provisioning messages they are not expecting; and

f) not install applications with identified security vulnerabilities.

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 [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, Windows Mobile 5.0 with Messaging and Security Feature Pack (MSFP), against the requirements of the Common Criteria (CC) Evaluation Assurance Level (EAL) 2 augmented with basic flaw remediation (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 [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 2.5.1 Evaluated Configuration.

Table 1: Identification Information

Item	Identifier
Evaluation Scheme	Australasian Information Security Evaluation Program (AISEP)
TOE	Windows Mobile Version 5.0 with MSFP (derived from Windows CE 5.1) which includes the following editions: • Windows Mobile 5.0 MSFP for Smartphones; and • Windows Mobile 5.0 MSFP for Pocket PC Phones
Software Version	This evaluation includes the following Adaptation Kit Updates (AKUs): • Build 14847 AKU 2.0 • Build 14914 AKU 2.1 • Build 14928 AKU 2.2

	• Build 14929 AKU 2.2.1 • Build 14932 AKU 2.2.2 • Build 14955 AKU 2.3 • Build 14957 AKU 2.3.1 • Build 14959 AKU 2.3.2 • Build 14960 AKU 2.4 • Build 14967 AKU 2.5 • Build 14989 AKU 2.6 • Build 14992 AKU 2.6.1 • Build 14994 AKU 2.6.2 • Build 14995 AKU 2.6.3 • Build 15096 AKU 3.0 • Build 15097 AKU 3.0.1 • Build 15314 AKU 3.1 • Build 15633 AKU 3.2 • Build 15671 AKU 3.3 • Build 15673 AKU 3.3.1 • Build 15359 AKU 3.4 • Build 15361 AKU 3.4.1 • Build 15362 AKU 3.4.2 • Build 15363 AKU 3.43 • Build 15704 AKU 3.5 • Build 15705 AKU 3.5.1 • Build 15706 AKU 3.5.2
Security Target	Windows Mobile 5.0 MSFP Security Target 1.0, 25 February 2008
Evaluation Level	EAL2 augmented with ALC_FLR.1
Evaluation Technical Report	Evaluation Technical Report for Windows Mobile 5.0 MSFP, 1.0, 03 March 2008
Criteria	CC Version 2.3, August 2005, with interpretations as of 18 July 2005
Methodology	CEM-99/045 Version 2.3, August 2005 with interpretations as of 18 July 2005
Conformance	Part 2 extended

	Part 3 conformant, augmented with basic flaw remediation (ALC_FLR.1)
Developer	Microsoft Corporation 1 Microsoft Way, Redmond WA 98052-8300 USA
Evaluation Facility	stratsec Suit 1/50 Geils Court, Deakin, ACT 2600

Chapter 2 - Target of Evaluation

2.1 Overview

10 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

11 The TOE is Windows Mobile 5.0 with MSFP developed by Microsoft Corporation.

12 The TOE is a single user operating system designed for use with Smartphones and Pocket PC devices. The intended method of use of the TOE is as a mobile messaging solution that allows users to stay connected to their email, contacts and calendar whilst away from their enterprise workstation.

13 The TOE operates in a specific operational environment, the ***user environment***, and is supported by capabilities that exist within the ***operator*** and ***enterprise environments***. This configuration is depicted in Figure 1 below.

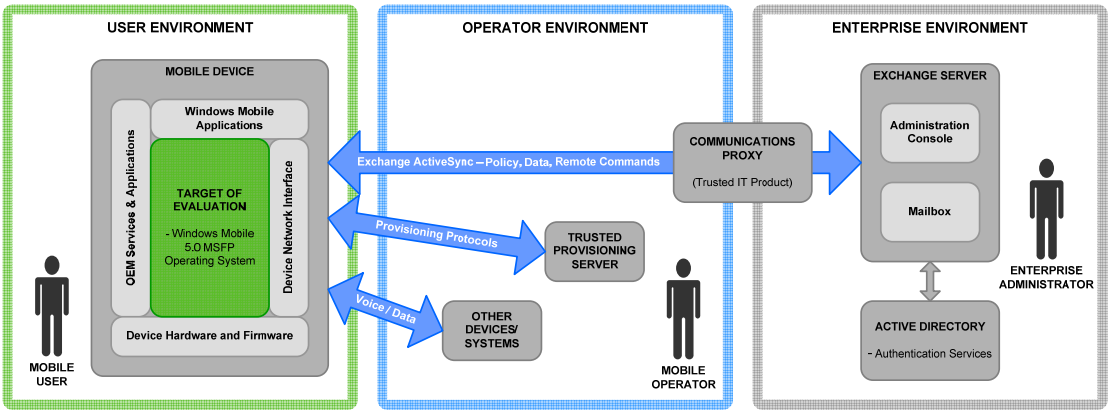

Figure 1: The TOE operating environment

14 Further details on the TOE and its operating environment are provided in the Security Target [1].

2.3 TOE Architecture

15 Windows Mobile 5.0 with MSFP is made up of three layers namely the Application layer, Operating System layer, and Original Equipment Manufacturer (OEM) layer. Figure 2 provides a diagrammatic representation of the Windows Mobile architecture. The TOE is defined as the Operating Systems Layer and consists of the following major architectural components:

a) Shell services subsystem

b) Remote connectivity subsystem

c) Core subsystem

d) Kernel subsystem

e) Security policy engine subsystem

f) Authentication services subsystem

g) Cryptographic services subsystem

h) Graphics, Windowing and Events Subsystem

i) Device manager subsystem

j) Storage manager subsystem

k) Communications and networking subsystem

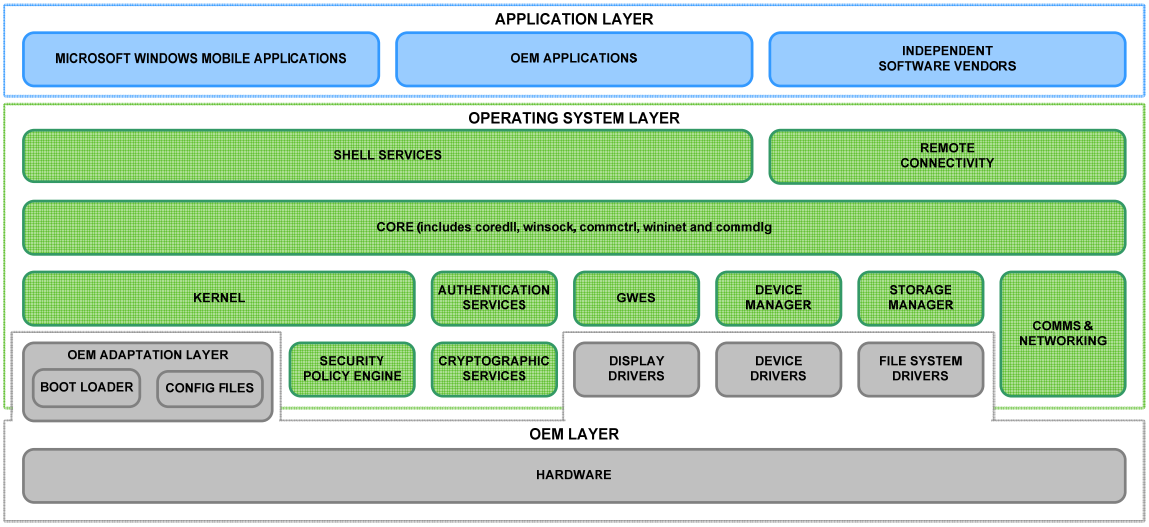

Figure 2: TOE Architecture

2.4 Clarification of Scope

16 The scope of the evaluation was limited to those claims made in the Security Target [1].

2.4.1 Evaluated Functionality

17 The TOE provides the following evaluated security functionality:

Table 2: Evaluated Security Functionality

Security function	TOE security feature
Device data protection. The TOE provides the capability to protect data in transit.	**SSL/TLS channel encryption**. Secure Sockets Layer (SSL)/Transport Layer Security (TLS) encrypts data transmitted between the device and server, over-the-air or through a wired connection.
	Certified cryptographic module. The TOE includes a certified FIPS validated cryptographic module. Applications can make use of cryptographic modules to perform cryptographic operations.
Device application control. The TOE provides the capability to only permit trusted applications to be installed and executed on the mobile device.	**Controlled application installation**. The TOE can be configured to only permit applications signed with a trusted certificate to be installed on the operating system.
	Controlled application execution. Code execution control allows the device to be locked so that only applications signed with a trusted certificate can run.
Secure enterprise access. The TOE provides the capability to securely synchronise data items with the Mobile User's Exchange Mailbox.	**Secure channel**. Windows Mobile establishes a secure channel for communicating with another trusted IT product.
	Synchronization of Mailbox Items. Mobile users can apply the secure channel to synchronise their emails, tasks, calendar and contacts with their enterprise mailbox.
Device configuration control. The TOE provides the capability to protect against modification by un-trusted systems.	**Exchange ActiveSync Mailbox Policy.** The Enterprise Administrator can use the secure channel to push down an enterprise policy for the Mobile Device.
	Trusted provisioning. Windows Mobile can implement secure communications with a trusted source that has the ability to provide provisioning and configuration data.
	Local configuration control. The authenticated user has the ability to locally manage specific configurations and settings.

Security function	TOE security feature
Device access control. The TOE has inbuilt security mechanisms that can be enabled to provide controlled access to the Mobile Device.	**Device authentication and lock.** Windows Mobile can be configured to require a password to gain access to the Mobile Device, however, it is possible to receive incoming calls and to make emergency calls without authenticating.
	Local device wipe. Windows Mobile can be configured to perform a local device wipe after a specified number of incorrect login attempts. **Note:** This feature only wipes TOE Security Functions (TSF) and user data on the Mobile Device. Data is not wiped from installed removable storage cards.
Device security management. The TOE has configurable security policies that establish which actions a user or application may take.	**Security roles.** Windows Mobile maintains multiple management roles which determine access to device resources.
	Security policies. Security policies establish the foundation configuration for the Mobile Device. They can be set to configure low-level device configuration policies and also implement enterprise password policy.
	Remote wipe. The Enterprise Administrator can issue a command to wipe a managed device if it has been lost or stolen. **Note:** This feature only wipes TSF and user data on the Mobile Device. Data is not wiped from installed removable storage cards.

2.4.2 Non-evaluated Functionality

18 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 Technology Security Manual (ACSI 33) [2] for policy relating to using an evaluated product in an unevaluated configuration. New Zealand Government users should consult the Government Communications Security Bureau (GCSB).

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

a) Application Layer which includes:

i) Microsoft Windows Mobile applications,

ii) OEM applications, and

iii) applications provided by independent software vendors.

b) OEM Layer which includes:

   i) drivers,

   ii) boot loader,

   iii) OEM configuration files, and

   iv) hardware.

20 While the actual mobile device does not form part of the TOE, potential users should note that the security functionality provided by the TOE is independent of the device that the operating system is installed upon.

2.5 Usage

2.5.1 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 these defined evaluated configuration(s). Australian Government users should refer to ACSI 33 [2] to ensure that configuration meets the minimum Australian Government policy requirements. New Zealand Government users should consult the GCSB.

22 The evaluated configuration is provided in the Installation and Administrator Guide [3]. The key policies that are applied to the TOE in the evaluated configuration are:

a) minimum password length and complexity requirements;

b) local device wipe after maximum unsuccessful authentication attempts;

c) encryption and signing settings;

d) applications must be signed to be installed or to run;

e) client provisioning settings; and

f) device password required for Desktop ActiveSync.

2.5.2 Delivery procedures

23 The end customer does not purchase the TOE directly from the developer. Windows Mobile 5.0 with MSFP is sold pre-installed on the device. A customer can purchase a device that contains the TOE in two ways: from the OEM or from a network provider.

24 The TOE has either two or three delivery stages depending on where the customer purchases the device.

2.5.2.1 OEM

25 An OEM obtains the TOE directly from the developer and can develop images for deployment onto their mobile devices. The OEM development activities add functionality to the handset including:

a) drivers to support the specific hardware components of the mobile device;

b) device specific applications that may use Windows Mobile operating system resources; and/or

c) device configuration settings as requested by Mobile Operators, or by enterprise customers.

26 Once the OEMs have completed development and integration with a specific AKU, OEMs are required to either:

a) submit their developed OEM image to a National Standards Testing Lab for independent verification and validation; or

b) self certify that the developed OEM image satisfies the Logo Test Kit (LTK).

27 The LTK includes a test case that performs a Cyclic Redundancy Check (CRC) of all Microsoft developed components that can be used to verify the integrity of the Windows Mobile operating system.

28 Note: The OEMs are trusted not to deliberately make changes to the TOE. (See A.DELIVERY in the Security Target [1]).

2.5.2.2 Network provider

29 In the mobile operator customisation phase, Mobile Operators perform final customisation of the mobile device.

30 This customisation of the mobile device may include:

a) installation of mobile operator specific applications;

b) setting of mobile device themes;

c) configuration of functionality to allow device management within the mobile operator network; and/or

d) device configuration (within the limitation of the mobile operator(s) security role) on behalf of customers.

31 Mobile Operators can make use of the CRC verification tool to determine whether the Windows Mobile operating system image provided by an OEM is the same as that released by Microsoft in the release to manufacturer Phase.

32 Note: The network operators are trusted not to deliberately make changes to the TOE. (See A.DELIVERY in the Security Target [1]).

2.5.2.3 End user

33 It is possible for an enterprise customer to bypass the Mobile Operator and negotiate provisioning of mobile devices directly from an OEM. In either case, the following procedures must be followed.

34 The Enterprise Administrator or Mobile User can have assurance that the mobile device and operating system have not been altered if the manufacturer's shrink-wrapped packaging is intact.

35 The Enterprise Administrator or Mobile User must check the shrink-wrapping of the delivered Mobile Device. If there are signs of tampering or damage then the manufacturer should be contacted.

2.5.3 Verifying the Evaluated Product

36 The Enterprise Administrator or Mobile User must check that the AKU of the received product matches one of the versions contained in the introduction of this report. This can be done by selecting "Settings -> About" from the main Windows Menu.

2.5.4 Documentation

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

a) Windows Mobile 5.0 MSFP Installation and Administrator Guide, version 1.0 [3]; and

b) Windows Mobile 5.0 MSFP & 6 User Guide Supplement, version 1.1 [4].

38 Other guidance is referenced from these documents and should be followed where there is no contradiction. In the case of a contradiction, the above references are considered to be authoritative.

39 To gain access to the relevant evaluation guidance the Enterprise Administrator can request access to the Windows Mobile 6 LTK Beta program, which provides controlled and secure access to the Microsoft Connect website where evaluation documentation and information is posted. The site provides both identification and authentication for controlling access and encryption using SSL for all access to Microsoft Connect.

40 Additionally, access to the Windows Mobile 6 LTK Beta program is only provided on a case-by-case basis. Enterprise Administrators must contact their local Microsoft office to request access to this program.

41 Once the Enterprise Administrator has been provided with access to the program, the Enterprise Administrator will need to go to the Microsoft Connect site and register. Once a Connect profile is established, the Windows Mobile team will be able to activate individuals in the Windows LTK Preview program.

42 To register on Connect, the following steps must be used.

a) Go to http://connect.microsoft.com.

b) Click “Sign In” and log in with your Windows Live ID Passport account.

c) Select “Manage Your Connect Profile”.

d) Accept the “Terms and Conditions”.

e) Fill out the Registration screen. Note: You MUST select YES to the question “I would like to be contacted about participating in other MS Beta programs”.

f) Click Submit.

43 Once this is completed a member of the Windows Mobile team will contact the individual to determine that they have a valid external record and need to access the evaluation guidance documentation.

2.5.5 Secure Usage

44 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.

Table 3: Secure Usage Assumptions

Assumption Identifier	Assumption Description
A.USAGE	Mobile Users are trusted to: • follow user guidance, • ensure that the TOE continues to operate in the evaluated configuration, • only permit ActiveSync connections between the Mobile Device and trusted computing devices, and • store the Mobile Device when not in use in a physically protected area that is appropriate for the information processed by the TOE.
A.DELIVERY	The security enforcing components of the TOE will not be modified by either the Mobile Operator or the manufacturer of the Mobile Device during the delivery process.

Assumption Identifier	Assumption Description
A.IT_ENTERPRISE	The Enterprise Exchange Server and Active Directory Server are located within the enterprise boundary and are protected from unauthorised logical/physical access.
A.IT_MOBILE	The Trusted Provisioning Server is located within the Mobile Operators network boundary and is protected from unauthorised logical and physical access.
A.ADMIN	The Enterprise Administrator is not careless, wilfully negligent, or hostile, and will follow and abide by the instructions provided by administrator documentation.
A.OPERATOR	The Mobile Operator will not transmit configuration messages that undermine the security objectives of the TOE.
A.I&A_ENTERPRISE	The IT environment will provide mechanisms for authenticating Mobile Users when accessing their mailbox and other resources within the corporate network.
A.COMMS_ENT	The IT environment will provide the server-side of a secure channel between the Enterprise Exchange Server and the Mobile Device.
A.COMMS_NET	The IT environment will provide the server-side of a secure channel between the Trusted Provisioning Server and the Mobile Device.
A.SEC_POLICY	The IT environment will provide a mechanism for setting enterprise policy and pushing it to the Mobile Device.

Chapter 3 - Evaluation

3.1 Overview

45 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

46 The criteria against which the TOE has been evaluated are contained in the Common Criteria for Information Technology Security Evaluation [5][6][7]. The methodology used is described in the Common Methodology for Information Technology Security Evaluation (CEM) [8]. The evaluation was also carried out in accordance with the operational procedures of the AISEP [9][10][11][12]. In addition, the conditions outlined in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security [13] were also upheld.

3.3 Functional Testing

47 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.

3.4 Penetration Testing

48 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.

49 Of the vulnerabilities examined, the evaluators deemed that two vulnerabilities exist but are not exploitable in the intended environment. These residual vulnerabilities are:

a) An attacker could attempt to read the contents of the internal memory of a TOE device in order to compromise user or TOE Security Function data. In this scenario, an attacker would be required to locate and remove the internal memory chip(s) from the TOE device and utilise specialised equipment in order to inspect the contents of the memory.

b) The TOE operates on portable devices that are intended to allow users to access office automation tools whilst away from their enterprise workstation. By their nature, such devices are subject to being lost, or physically stolen. It is possible that an attacker may access User data of a lost or stolen device by interacting with the user interface. While the device has a lockout, the device could be stolen/found within the timeout period.

Chapter 4 - Certification

4.1 Overview

50 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

51 After due consideration of the conduct of the evaluation as witnessed by the certifiers, and of the Evaluation Technical Report [14], the

Australasian Certification Authority (ACA) certifies the evaluation of Windows Mobile 5.0 with MSFP performed by the Australasian Information Security Evaluation Facility (AISEF), stratsec.

52 The stratsec AISEF has found that Windows Mobile 5.0 with MSFP upholds the claims made in the Security Target [1] and has met the requirements of the CC EAL2 augmented with ALC_FLR.1.

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

4.3 Assurance Level Information

54 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.

55 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, strength of function analysis, and evidence of a developer search for obvious vulnerabilities (e.g. those in the public domain).

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

4.4 Recommendations

57 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 ACSI 33 [2] and New Zealand Government users should consult the GCSB.

58 In addition to ensuring that the assumptions concerning the operational environment are fulfilled and the guidance document is followed [3][4], the ACA also recommends the following for users and administrators.

a) The administrator must ensure that users are aware that data stored on external storage cards is not protected and should advise users against storing sensitive data on external media.

b) The administrator should review the applications included in the default image and determine whether they allow the user to change the security areas of the registry.

c) The administrator should consider the necessity of all pre-installed certificates contained within the certificate stores. While specific OEM and Mobile Operator certificates may be required to ensure that the TOE boots and operates correctly, there may be no requirements to have other pre-installed certificates on the TOE.

d) The administrator should ensure that users are aware of the importance of running the TOE in the evaluated configuration, and ensure that they return for reconfiguration following a device wipe.

e) The administrator should advise users not to accept Service Indicator or Service Loader messages that they are not expecting.

f) The administrator should advise users against installing Resco Photo Viewer versions 4.11 and 6.01.

Annex A - References and Abbreviations

A.1 References

[1] Windows Mobile 5.0 MSFP Security Target 1.0, 25 February 2008, Microsoft Corporation.

[2] Australian Government Information and Communications Technology Security Manual (ACSI 33), September 2007, Defence Signals Directorate, (available at www.dsd.gov.au).

[3] Windows Mobile 5.0 MSFP Installation and Administrator Guide, version 1.1, 25 February 2008, Microsoft Corporation

[4] Windows Mobile 5.0 MSFP & 6 User Guide Supplement, version 1.0, 07 February 2008, Microsoft Corporation

[5] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model (CC), Version 2.1, August 1999, CCIMB-99-031, Incorporated with interpretations as of 2003-12-31

[6] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements (CC), Version 2.1, August 1999, CCIMB-99-032, Incorporate with interpretations as of 2003-12-31

[7] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements (CC), Version 2.1, August 1999, CCIMB-99-033, Incorporate with interpretations as of 2003-12-31

[8] Common Methodology for Information Technology Security Evaluation (CEM), Version 1.0, August 1999, CEM-99/045, Incorporated with interpretations as of 2003-12-31

[9] AISEP Publication No. 1 – Program Policy, AP 1, Version 3.1, 29 December 2006, Australian Certification Authority, Defence Signals Directorate.

[10] AISEP Publication No. 2 – Certifier Guidance, AP 2. Version 3.0, 21 February 2006, Australian Certification Authority, Defence Signals Directorate.

[11] AISEP Publication No. 3 – Evaluator Guidance, AP 3. Version 3.1, 29 September, Australian Certification Authority, Defence Signals Directorate

[12] AISEP Publication No. 4 – Sponsor and Consumer Guidance, AP 4. Version 3.1, 29 September, Australian Certification Authority, Defence Signals Directorate

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

[14] Evaluation Technical Report for Windows Mobile 5.0 MSFP 1.0, 03 March 2008, stratsec.

A.2 Abbreviations

ACA	Australasian Certification Authority
AISEP	Australasian Information Security Evaluation Program
AKU	Adaptation Kit Update
CC	Common Criteria
CEM	Common Evaluation Methodology
CRC	Cyclic Redundancy Check
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standard
GCSB	Government Communications Security Bureau
LTK	Logo Test Kit
IT	Information Technology
MMS	Multimedia Messaging Service
MSFP	Messaging and Security Feature Pack
OEM	Original Equipment Manufacturer
S/MIME	Secure/Multi-purpose Internet Mail Extensions
SMS	Short Messaging Service
SSL	Secure Sockets Layer
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functions
USB	Universal Serial Bus