



Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Certification Report

Certificate Number: 2010/65

5 Feb 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 | 5/02/2010 | Public release. |

Executive Summary

- 1 Windows Mobile 6.5 is a compact operating system for use on Smartphones enabling users to extend their corporate Windows desktop to mobile devices in a secure manner. Windows Mobile 6.5 is the Target of Evaluation (TOE).
- 2 The core functionality of the TOE includes:
- a) **Device data protection.** The TOE provides the capability to protect data at rest and in transit.
 - b) **Device application control.** The TOE provides the capability to only permit trusted applications to be installed and executed on the Mobile Device.
 - c) **Secure enterprise access.** The TOE provides the capability to securely connect the TOE to trusted Enterprise assets and facilitate data transfer.
 - d) **Device access control.** The TOE has inbuilt security mechanisms that can be enabled to provide controlled access to the Mobile Device.
 - e) **Device security management.** The TOE has configurable security policies that establish which actions a user or application may take.
- 3 This report describes the findings of the IT security evaluation of Microsoft Corporation's Windows Mobile 6.5, to the Common Criteria (CC) evaluation assurance level EAL4 + ALC_FLR.1. The report concludes that the product has met the target assurance level of EAL4 + 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 (AISEP). The evaluation was performed by stratsec and was completed on 22 December 2009.
- 4 The TOE forms the software part of a software and hardware 'composed evaluation' product. The TOE evaluation technical report (ETR) (Ref [1]) provides composition guidance for an Original Equipment Manufacturer (OEM) to meet in developing a hardware component for a composed product.
- 5 The OEM is the primary customer of the operating system. Microsoft provides the OEM with security updates and they are expected to pass them on to the end users.
- 6 The TOE User for the composed product is the end user. The end user administrator should ensure that the TOE is used in a composed product evaluated to EAL4+.
- 7 With regard to the secure operation of the TOE, the Australasian Certification Authority (ACA) recommends that:
- a) The administrator ensures that no applications are installed which will allow the user to change the security areas of the registry.

- b) The administrator reviews the certificates in the Software Publishing Certificate (SPC), privileged and unprivileged certificate stores and removes any certificates that are not required. This action prevents unwanted, signed applications from being installed on the TOE. Note: some certificates are required for the TOE to operate, and the administrator should verify that the TOE can function without the certificates that are removed during provisioning.
- c) The administrator ensures that users are aware of the importance of running the TOE in the evaluated configuration. In the event of a device wipe, the mobile device should be returned to the administrator for reconfiguration.
- d) The administrator advises users against using the device as a primary data store. This is because data on the device and storage card is encrypted, and the keys stored on the device are destroyed during a device wipe.
- e) The administrator sets the lockout time on a device to reflect the criticality of the data stored on a mobile device. The reduction in lockout time reduces the chances of an attacker gaining access to a device in an unlocked state.
- f) The administrator sets mobile device policy to encrypt all areas of the device that may contain user data.
- g) The administrator ensures that the SD card and local device encryption is enabled prior to users placing any files into internal stores or SD media.
- h) The administrator lock down all unrequired physical ports on mobile devices to reduce the risk of vulnerabilities in OEM hardware and firmware.
- i) The administrator considers disabling the use of the Bluetooth radio in order to prevent exploitation of publically published weaknesses in the Bluetooth key pairing process.

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

9 It is the responsibility of the user to ensure that the TOE meets their requirements. For this reason, 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. It is recommended that a prospective user of the TOE refer to the Security Target at Ref [2], and read this Certification Report prior to deciding whether to use the product.

Table of Contents

| | |
|--|-----------|
| CHAPTER 1 - INTRODUCTION | 1 |
| 1.1 OVERVIEW | 1 |
| 1.2 PURPOSE..... | 1 |
| 1.3 IDENTIFICATION | 1 |
| CHAPTER 2 - TARGET OF EVALUATION | 2 |
| 2.1 OVERVIEW | 2 |
| 2.2 DESCRIPTION OF THE TOE | 2 |
| 2.3 TOE ARCHITECTURE..... | 3 |
| 2.4 CLARIFICATION OF SCOPE | 4 |
| 2.4.1 <i>Evaluated Functionality</i> | 4 |
| 2.4.2 <i>Non-evaluated Functionality</i> | 5 |
| 2.4.3 <i>TOE for Composition</i> | 6 |
| 2.4.4 <i>TOE User</i> | 6 |
| 2.5 USAGE..... | 6 |
| 2.5.1 <i>Evaluated Configuration</i> | 6 |
| 2.5.2 <i>Delivery procedures</i> | 7 |
| 2.5.3 <i>Determining the Evaluated Configuration</i> | 9 |
| 2.5.4 <i>Documentation</i> | 10 |
| 2.5.5 <i>Secure Usage</i> | 10 |
| CHAPTER 3 - EVALUATION | 11 |
| 3.1 OVERVIEW | 11 |
| 3.2 EVALUATION PROCEDURES | 11 |
| 3.3 FUNCTIONAL TESTING..... | 12 |
| 3.4 PENETRATION TESTING | 12 |
| CHAPTER 4 - CERTIFICATION..... | 12 |
| 4.1 OVERVIEW | 12 |
| 4.2 CERTIFICATION RESULT | 13 |
| 4.3 ASSURANCE LEVEL INFORMATION | 13 |
| 4.4 RECOMMENDATIONS | 13 |
| ANNEX A - REFERENCES AND ABBREVIATIONS | 15 |
| A.1 REFERENCES | 15 |
| A.2 ABBREVIATIONS..... | 16 |

Chapter 1 - Introduction

1.1 Overview

10 This chapter contains information about the purpose of this document and how to identify the TOE.

1.2 Purpose

11 The purpose of this Certification Report is to:

- a) report the certification of results of the IT security evaluation of the TOE, Windows Mobile 6.5, against the requirements of Common Criteria evaluation assurance level EAL4 + ALC_FLR.1; and
- b) provide a source of detailed security information about the TOE for any interested parties.

12 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

13 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 | Windows Mobile 6.5 |
| Software Version | Windows Mobile 6.5 Standard (Build 21849 AKU 5.0.63) Windows Mobile 6.5 Professional (Build 21854 AKU 5.0.80) |
| Security Target | Windows Mobile 6.5 EAL4+ Security Target v1.0, July 2009 |
| Evaluation Level | EAL4 + ALC_FLR.1 |
| Evaluation Technical Report | Windows Mobile 6.1 EAL4+ Evaluation Technical Report v1.0, January 2010 |
| Criteria | Common Criteria for Information Technology (IT) Security Evaluation, Version 3.1 Revision 3, July 2009, with interpretations as of 6 March 2008 |
| Methodology | Common Methodology for Information Technology Security Evaluation, Evaluation methodology, July 2009, Version 3.1 Revision 3, CCMB-2009-07-004 |
| Conformance | Common Criteria Part 2 extended. |

| | |
|-----------------------|---|
| | Common Criteria Part 3 conformant, EAL4 augmented with ALC_FLR.1. |
| Sponsor and Developer | Microsoft Corporation 1 Microsoft Way, Redmond WA 98052-8300 USA |
| Evaluation Facility | stratsec Suite 1/50 Geils Court, Deakin ACT |

Chapter 2 - Target of Evaluation

2.1 Overview

- 14 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

- 15 The TOE is Windows Mobile 6.5 developed by Microsoft Corporation.
- 16 The TOE is a compact operating system for use on Smartphones enabling users to securely extend their corporate Windows desktop to mobile devices.
- 17 Windows Mobile 6.5 provides the basis for establishing a secure enterprise mobile messaging solution that can securely synchronize and access Line of Business (LOB) applications and services, including Microsoft Exchange to access email, contacts, tasks and calendar and other corporate applications that may be only accessible from within the enterprise network.
- 18 Windows Mobile powered devices can be centrally managed through the System Center Mobile Device Manager (SCMDM). Windows Mobile 6.5 supports the standards needed to allow the client to establish an authenticated and encrypted communications channel to MDM Gateway Server for enterprise management.
- 19 The inclusion of the SCMDM client application in Windows Mobile 6.5 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. Enterprise administrators can lock down many areas of the Windows Mobile Smartphones, including certain communications and device functionality, while exercising significant control over the software to be installed on devices.
- 20 Windows Mobile 6.5 has a seamless user experience across cellular or Wi-Fi data connections to the enterprise network. SCMDM provides a single point for security-enhanced, behind-the-firewall access to corporate data and LOB applications for Windows Mobile. Enterprise Administrators can facilitate security over public wireless networks

through a Mobile VPN link. The VPN link secures wireless communications between the Windows Mobile 6.5 powered mobile device and corporate servers through an SSL encrypted tunnel.

21 Figure 1 illustrates the claimed security functionality for Windows Mobile.

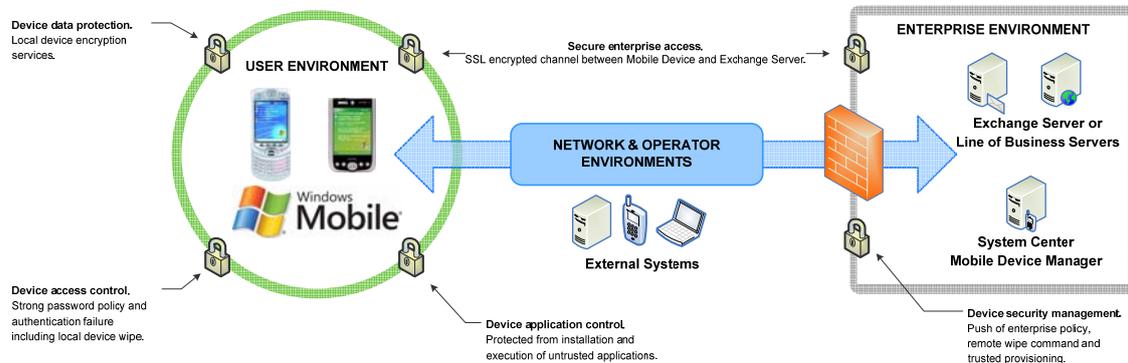


Figure 1 – Windows Mobile 6.5 security architecture

2.3 TOE Architecture

22 Windows Mobile 6.5 is a compact operating system combined with a suite of basic applications for mobile devices based on the Microsoft Win32 API.

23 The base operating system components have been developed from the Windows CE 5.0 (version 5.2) source code. Enhancements and additions are made to the operating system to make it specific to Windows Mobile and then additional applications and features are also added through additional Windows Mobile specific source.

24 The Windows Mobile 6.5 architecture has the following distinct layers (see Figure 1 below):

- a) **Windows Mobile layer.** A layer of code that has been specifically developed to implement Windows Mobile specific functionality and applications.
- b) **Operating system layer.** Based on the Windows CE 5.0 operating system which is used as the basis for Windows Mobile 6.5. This includes core operating system functionality such as the kernel, device management and file system management.
- c) **OEM adaptation layer.** A layer of code that resides between the operating system kernel and the hardware of Mobile Device. It facilitates communication between the operating system and the hardware and includes code to handle interrupts, timers, and generic I/O control codes (IOCTLs).

25 The diagram below demonstrates that the Common Criteria EAL4+ evaluation of Windows Mobile has focused on the Windows Mobile and Windows CE components and has placed the OEM adaptation layer (OAL) and hardware outside the scope of this base evaluation.

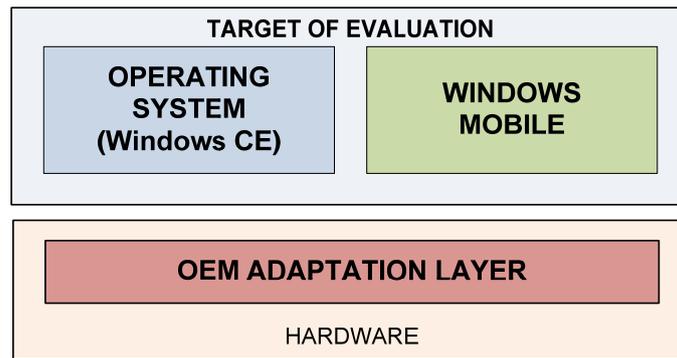


Figure 2 – Windows Mobile 6.5 architectural design layers

2.4 Clarification of Scope

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

2.4.1 Evaluated Functionality

27 The TOE provides the following evaluated security functionality:

Table 1 – Windows Mobile security features

| Security function | TOE security feature |
|---|--|
| Device data protection. The TOE provides the capability to protect data at rest. | Sensitive Data Protection. The TOE supports 128-bit AES encryption of data stored locally on the Mobile Device and also on removable storage cards. |
| | S/MIME support. The TOE provides additional protection features for e-mail messages, whether in transit between device and server or at rest. |
| | Certified cryptographic module. The TOE includes a FIPS validated cryptographic module enabling applications to make use of inbuilt cryptographic operations. |
| Secure enterprise access. The TOE provides the capability to securely connect trusted enterprise assets and facilitate secure data transfer. | SSL/TLS channel encryption. The TOE supports SSL/TLS encryption enabling sensitive data to be transmitted between the device and server, over-the-air or through a wired connection. |
| | Mobile VPN. Incorporating secure key exchange (IKEv2), an IPSec VPN tunnel can be established between the TOE and the enterprise gateway, providing protection for information communicated between the TOE and Line of Business (LOB) servers within the trusted enterprise. |

| Security function | TOE security feature |
|--|---|
| | Enterprise Authentication. The TOE provides the capability to support enterprise authentication mechanisms. |
| Device application control. The TOE provides the capability to control the installation and execution of applications 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 Mobile Device. |
| | Controlled application execution. The TOE implements code execution control to only permit applications signed with a trusted certificate to be executed on the Mobile Device. |
| Device access control. The TOE has capability to provide controlled access to information and functionality of the Mobile Device. | Device authentication and lock. The TOE implements functionality that requires the Mobile User to enter a password to gain access to the Mobile Device. |
| | Local device wipe. The TOE can be configured to perform a local device wipe after a specified number of incorrect login attempts by the Mobile User on the Mobile Device. |
| | Trusted provisioning. The TOE implements protection mechanisms to ensure that provisioning and configuration data can only be accepted by the Mobile Device from a trusted source. |
| Device security management. The TOE has configurable security and management policies that enable enterprise management of the Mobile Device. | Security roles and policies. The TOE maintains multiple management roles and implements a suite of security policies which determine access to resources on the Mobile Device. |
| | Remote wipe. The TOE can be configured to accept a command from a management server to remotely wipe the Mobile Device. |
| | Device management policies. The TOE supports a range of mobile device management capabilities which can be instilled by the Enterprise Administrator through Server Center Mobile Device Manager (SCMDM) 2008. |

2.4.2 Non-evaluated Functionality

28 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).

29 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.

30 The mobile device handset does not form part of the TOE. Potential users should note that the security functionality provided by the TOE is independent of the handset hardware platform.

2.4.3 TOE for Composition

31 The TOE forms the software part of a software and hardware ‘composed evaluation’ product. The TOE ETR (Ref [1]) provides composition guidance for an OEM to meet in developing a hardware component for a composed product. The ETR is a controlled document and is available from the ACA or Microsoft to Microsoft-approved OEMs.

2.4.4 TOE User

32 The OEM is the primary customer of the operating system. Microsoft provides the OEM with security updates and they are expected to pass them on to the end users.

2.5 Usage

2.5.1 Evaluated Configuration

33 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. Additionally, 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.

34 The evaluated configuration is provided in the Windows Mobile 6.5 “EAL4+” Enterprise Administrator, OEM and User Guidance Supplements (Refs [4],[5] and [6]). The principal policies that are applied to the TOE in the evaluated configuration are:

- a) Minimum Password Length and complexity Requirements;
- b) Storage card encryption;
- c) Device Encryption;
- d) Local device wipe after a configurable number of unsuccessful authentication attempts;
- e) S/MIME settings, 3DES/SHA1;
- f) Applications must be signed to be installed or to run;
- g) Mobile operator message and provisioning services SI, SL and OMA-CP are disabled; and
- h) Device password required for Desktop ActiveSync.

35 The TOE is required to be used on a mobile device evaluated to EAL4 which complies with the requirements stated in the Windows Mobile 6.5 ETR for composition (Ref [1]). OEMs and evaluators of the composite product should refer to this ETR for an explanation of the functions that the OS relies on, and which must be implemented by the OEM.

2.5.2 Delivery procedures

36 The delivery process to the OEM comprises the following distinct stages:

- a) **Final development.** Specific actions taken during the final development stages to ensure that the TOE is ready for release.
- b) **Release to manufacturer.** The initial release to the OEMs for review and incorporation into mobile platforms. Development of specific applications and underlying software and hardware for integration with the TOE.
- c) **Official release via Microsoft OEM Online.** Once all integration and testing efforts have occurred the official release is provided through the Microsoft OEM Online (MOO) capability.

37 Post official release delivery to the OEM the following additional phases also occur:

- a) **Mobile operator customization.** Implementation of Mobile Operator applications and service offerings for use by end consumers of the Mobile Device.
- b) **Delivery to mobile user.** Final delivery to the end consumers of the TOE and Windows Mobile powered devices.

2.5.2.1 Final development

38 In the final stages of the develop phase, Windows Mobile Feature Teams (developers of the various features that comprise the Windows Mobile OS) are responsible for definition of test cases to validate that all feature requirements have been satisfied. During this phase the Adaptation Kit Update (AKU), or specific version of the TOE, is produced for testing. Feature requirements, test cases and the AKU for release testing pass into the RTM phase.

2.5.2.2 Release to manufacturer (RTM)

39 In the RTM phase, test requirements and test cases are loaded into the Logo Test Kit (LTK) access database. Test cases are executed against the AKU intended for release. Test Case 5000 includes verification of the CRC for each component (executable and dynamic link library) comprising the WM operating system. Other test cases validate the correct functional behaviour of the Windows Mobile operating system features (including security features). Following execution of LTK against the AKU, results are logged and the following outcomes implemented:

- a) **If testing passes.** The AKU can be released to Microsoft-approved OEM for integration; or
- b) **If testing has failed.** Manual verification of failed tests is conducted to confirm whether test cases are incorrect, or that the AKU tested feature does not meet the requirement. Where it is confirmed that the test case is incorrect, it may be determined (by code analysis or other manual verification methods) that the AKU still meets the feature requirements. In this case, an AKU may be released to market. If testing confirmed that feature requirements have not been met, the AKU is not released to market and feature teams may make changes to the feature. In this case a new AKU would result.

2.5.2.3 Microsoft OEM Online

40 The Microsoft OEM Online <https://www.microsoftoem.com> is a confidential and controlled site that is subject to legal agreements and bindings. Only licensed OEMs are permitted to access this site and collect products that they are licensed to access. At a minimum an OEM must have a Customer's Non-Disclosure Agreement ("NDA") with Microsoft, and one or more of the following:

- a) a Microsoft Business Terms Document For OEM Customers;
- b) a Microsoft OEM Business Terms Document for Embedded Systems ("BTDE");
- c) a Microsoft OEM Embedded Systems License Agreement for Reference Platform Devices, an OEM Customer License Agreement, or a Microsoft OEM Distribution Agreement For Software Products For Embedded Systems (each an "Embedded Agreement");
- d) an MSLI OEM Online Site Agreement ("Site Agreement");
- e) a Microsoft OEM Distributor Channel Agreement ("OEM Distributor Channel Agreement")

41 At this point licensed OEMs are permitted to access the finalised versions of the Windows Mobile operating system for installation on their specific Windows Mobile powered devices.

2.5.2.4 Mobile operator customization

42 In the mobile operator customization phase, Mobile Operators perform final customization of the mobile device.

- 43 This customization 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.
- 44 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 RTM Phase.
- 45 It is possible for an enterprise customer to bypass the Mobile Operator and negotiate provisioning of mobile devices directly from an OEM. In this case, this phase of delivery is not used.
- 46 There are no specific delivery responsibilities or approvals in this phase related to the Windows Mobile Operating System. The responsibilities and approvals within this phase are based on commercial arrangements between the OEM and the Mobile Operators.

2.5.2.5 Delivery to the enterprise administrator or end user

- 47 The Windows Mobile 6.5 Security Target (Ref. [2]) includes assumptions that both the OEM and Mobile Operators are trusted to not alter/modify the security enforcing functions. With these assumptions in mind, the Enterprise Administrator or Mobile User can have assurance that the mobile device and operating system have not been altered if the manufacturers shrink wrapped packaging is intact.
- 48 The Enterprise Administrator or Mobile User is encouraged to check the shrink wrapping of the delivered Mobile Device. If there are signs of tampering or damage then the manufacturer should be contacted.
- 49 The Enterprise Administrator or Mobile User must acquire the relevant evaluation guidance supplements from the Microsoft TechNet website (<http://technet.microsoft.com/en-us/ee441336.aspx>) so that Windows Mobile powered devices are administered and used in a controlled manner and in accordance with the evaluated configuration.
- 50 The following documents can be obtained from Microsoft TechNet:
- a) WM6.5 EAL4+ Enterprise Administrator Guidance Supplement (Ref. [5]), and
 - b) WM6.5 EAL4+ User Guidance Supplement (Ref. [6]).

2.5.3 Determining the Evaluated Configuration

- 51 The TOE is labelled with the unique reference and can be reviewed by the end-user by completing the following steps:
- 52 For **Windows Mobile 6.5 Professional**:
- a) Go to Start > Settings

- b) Select the System tab
- c) Select the About to open the About window

53 For **Windows Mobile 6.5 Standard**:

- a) Go to Start > Settings
- b) Select About to open the About window

54 Device information is then displayed:

- a) Marketing description – In this case it is **Windows Mobile 6.5**.
- b) Window CE Operating system version – **OS 5.2.21849**.
- c) AKU build – **Build 21849 AKU 5.0.63**

2.5.4 Documentation

55 OEMs will be required to supply relevant evaluation guidance supplements to the enterprise administrator and end user so that Windows Mobile powered devices are administered and used in a controlled manner and in accordance with the evaluated configuration.

56 The following documents need to be distributed by the OEM:

- a) WM6.5 EAL4+ Enterprise Administrator Guidance Supplement (Ref. [5]); and
- b) WM6.5 EAL4+ User Guidance Supplement (Ref. [6]).

57 Other guidance is referenced from these documents and should be followed where there is no contradiction. In the case of a contradiction, the order of authority is:

- a) The DSD Consumer Guide (for Australian and New Zealand users) where one is available;
- b) This Certification Report;
- c) The guidance documentation listed above in Paragraph 56; and
- d) Any subsequent referenced guidance documentation.

2.5.5 Secure Usage

58 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 2 - Assumptions

| Identifier | Assumption statement |
|------------------|---|
| A.USAGE | Mobile Users are trusted to: <ul style="list-style-type: none"> a) follow user guidance; b) ensure that the TOE continues to operate in the evaluated configuration; c) only permit ActiveSync connections between the Mobile Device and trusted computing devices; and d) 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. |
| A.IT_ENTERPRISE | The Active Directory Server and all LOB Servers are located within the enterprise boundary and are protected from unauthorized logical/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.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 System Center Mobile Device Manager and LOB Servers and the Mobile Device. |
| A.SEC_POLICY | The IT environment will implement System Center Mobile Device Manager for managing devices and establishing enterprise policy. |

Chapter 3 - Evaluation

3.1 Overview

59 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

60 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 (Refs [7], [8], [9]). The methodology used is described in the Common Methodology for Information Technology Security Evaluation Version 3.1 (CEM) (Ref

[10]). The evaluation was carried out in accordance with the operational procedures of the Australasian Information Security Evaluation Program (AISEP) (Refs [11], [12], [13] and [14]). In addition, the conditions outlined in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (Ref [15]) were also upheld.

3.3 Functional Testing

61 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

62 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 tests:

- 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.

63 The results of the penetration testing note that a number of additional vulnerabilities exist that are dependent on an attacker having access to the underlying hardware and related interfaces. Access to the underlying hardware is out of scope of this evaluation; however must be considered when the TOE is used in composition with OEM hardware. Due to the nature of mobile devices, the opportunity for an attacker to access a lost or stolen device is greatly increased.

Chapter 4 - Certification

4.1 Overview

64 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

65 After due consideration of the conduct of the evaluation as witnessed by
the certifiers, and of the Evaluation Technical Report (Ref [1]), the
Australasian Certification Authority certifies the evaluation of Windows
Mobile 6.5 performed by the Australasian Information Security Evaluation
Facility, stratsec.

66 stratsec has found that Windows Mobile 6.5 upholds the claims made in
the Security Target (Ref [2]) and has met the requirements of the Common
Criteria (CC) evaluation assurance level EAL4 + ALC_FLR.1.

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

4.3 Assurance Level Information

68 EAL4 provides assurance by a full security target 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.

69 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 a vulnerability analysis demonstrating resistance
to penetration attackers with an Enhanced-Basic attack potential.

70 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

71 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).

72 In addition to ensuring that the assumptions concerning the operational
environment are fulfilled and the guidance document is followed (Refs [4],
[5] and [6]), the ACA also recommends that:

- a) The administrator ensures that no applications are installed which will
allow the user to change the security areas of the registry.
- b) The administrator reviews the certificates in the Software Provider
Certificate (SPC), privileged and unprivileged certificate stores and
removes any certificates that are not required. This action prevents
unwanted, signed applications from being installed on the TOE.
Note: some certificates are required for the TOE to operate, and the
administrator should verify that the TOE can function without the
certificates that are removed during provisioning.

- c) The administrator ensures that users are aware of the importance of running the TOE in the evaluated configuration. In event of a device wipe, the mobile device should be returned to the administrator for reconfiguration.
- d) The administrator advises users against using the device as a primary data store. This is because data on the device and storage card is encrypted, and the keys stored on the device are destroyed during a device wipe.
- e) The administrator sets the lockout time on a device to reflect the criticality of the data stored on a mobile device. The reduction in lockout time reduces the chances of an attacker gaining access to a device in an unlocked state.
- f) The administrator sets mobile device policy to encrypt all areas of the device that may contain user data.
- g) The administrator ensures that SD card and local device encryption is enabled prior to users placing any files into internal stores or SD media.
- h) The administrator lock down all unrequired physical ports on mobile devices to reduce the risk of vulnerabilities in OEM hardware and firmware.
- i) The administrator consider disabling the use of the Bluetooth radio in order to prevent exploitation of well know weaknesses in the Bluetooth key pairing process.

Annex A - References and Abbreviations

A.1 References

- [1] Windows Mobile 6.5 EAL4+ Evaluation Technical Report 1.0, January 2010
- [2] Windows Mobile 6.5 EAL4+ Common Criteria Evaluation Security Target version 1.0, July 2009
- [3] Australian Government ICT Security Manual (ISM), December 2008, Defence Signals Directorate, (available at www.dsd.gov.au).
- [4] Windows Mobile 6.5 EAL4+ OEM Guidance Supplement version 1.0, January 2010
- [5] WM6.5_EAL4+ Enterprise Administrator Guidance Supplement 1.0, January 2010
- [6] Windows Mobile 6.5 User Guide Supplement version 1.0, January 2010
- [7] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model (CC), Version 3.1, Revision 3, July 2009, CCMB-2009-07-001
- [8] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components (CC), Version 3.1, Revision 3, July 2009, CCMB-2009-07-002
- [9] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components (CC), Version 3.1, Revision 3, July 2009, CCMB-2009-07-003
- [10] Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1 Revision 3, July 2009, CCMB-2009-07-004
- [11] AISEP Publication No. 1 – Program Policy, AP 1, Version 3.1, 29 September 2006, Defence Signals Directorate.
- [12] AISEP Publication No. 2 – Certifier Guidance, AP 2. Version 3.1, 29 September 2006, Defence Signals Directorate.
- [13] AISEP Publication No. 3 – Evaluator Guidance, AP 3. Version 3.1, 29 September 2006, Defence Signals Directorate.
- [14] AISEP Publication No. 4 – Sponsor and Consumer Guidance, AP 4. Version 3.1, 29 September 2006, Defence Signals Directorate.
- [15] Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, May 2000

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 |
| ETR | Evaluation Technical Report |
| FLR | Flaw Remediation |
| GCSB | Government Communications Security Bureau |
| IOCTL | Input Output Control |
| LOB | Line Of Business |
| OAL | OEM Adaptation Layer |
| OEM | Original Equipment Manufacturer |
| PP | Protection Profile |
| SCMDM | System Center Mobile Device Manager |
| SD | Secure Digital |
| SFP | Security Function Policy |
| SFR | Security Functional Requirements |
| SPC | Software Publishing Certificate |
| SSL | Secure Socket Layer |
| ST | Security Target |
| TOE | Target of Evaluation |
| TSF | TOE Security Functions |
| TSP | TOE Security Policy |
| VPN | Virtual Private Network |