Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Certification Report

Certificate Number: 2008/48

06 AUG 2008

Version 1.0

Amendment Record

Version	Date	Description
1.0	06/08/2008	Public release.

Executive Summary

1 Windows Mobile 6.1 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 6.1 is the Target of Evaluation (TOE).

2 Windows Mobile 6.1 extends and strengthens the core security features of the Windows Mobile 6 operating system by:

a) Enabling management of the mobile device with the System Center Mobile Device Manager (SCMDM) client application;

b) Providing a 'double-enveloped' (IPSec and SSL), secure Mobile VPN capability between the Mobile Device and the trusted enterprise; and

c) Encrypting locally stored data.

3 This report describes the findings of the IT security evaluation of Microsoft Corporation's Windows Mobile 6.1, to the Common Criteria Evaluation Assurance Level 2 augmented with basic flaw remediation (ALC_FLR.1). The report concludes that the product has met the target assurance level of EAL 2 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 (AISEP). The evaluation was performed by stratsec and was completed on 30 July 2008.

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

a) Review the security of default applications;

b) Consider the necessity of pre-installed certificates contained within the certificate stores;

c) Maintain the awareness of the evaluated configuration; and

d) Avoid using the device as a primary data store;

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 [1], and read this Certification Report prior to deciding whether to purchase the product.

Table of Contents

Chapter 1 - Introduction

1.1 Overview

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

1.2 Purpose

8 The purpose of this Certification Report is to:

a) report the certification of results of the IT security evaluation of the TOE, Windows Mobile 6.1, against the requirements of the Common Criteria (CC) evaluation assurance level EAL 2 augmented with ALC_FLR.1, 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 [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	Windows Mobile 6.1, which includes the following editions: • Windows Mobile 6.1 Standard; • Windows Mobile 6.1 Professional; and • Windows Mobile 6.1 Classic.
Software Version	This evaluation includes the following Adaptation Kit Updates (AKUs): • Build 19212 AKU 1.0.3; • Build 19214 AKU 1.0.4; and • Build 19581 AKU 1.1.1.
Security Target	Windows Mobile 6.1 Security Target v1.0, 22 July 2008
Evaluation Level	EAL 2 augmented with ALC_FLR.1
Evaluation Technical Report	Evaluation Technical Report for Windows Mobile 6.1 v1.0, 25 July 2008
Criteria	Common Criteria for Information Technology (IT) Security Evaluation, version 2.3, August 2005.
Methodology	CEM version 2.3, August 2005.
Conformance	CC Part 2 Extended, Part 2: Security functional requirements, version 2.3, August 2005. CC Part 3 Conformant: Security assurance requirements, version 2.3, August 2005.
Sponsor and Developer	Microsoft Corporation 1 Microsoft Way, Redmond WA 98052-8300 USA
Evaluation Facility	stratsec Suit 1/50 Geils Court, Deakin ACT

Chapter 2 - Target of Evaluation

2.1 Overview

11 This chapter contains information about the Target of Evaluation (TOE), including: a description of functionality provided; its architecture components; the scope of evaluation; security policies; and its secure usage.

2.2 Description of the TOE

12 The TOE is Windows Mobile 6.1 developed by Microsoft Corporation.

13 The TOE is a single user operating system designed for use with Smartphone and PocketPC 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.

14 The TOE operates in a specific operational environment, the ***user environment***, and is supported by capabilities that exist within the ***operator*** and ***enterprise environments***. The relationships between the TOE and relevant elements within each of the operating environments are depicted in Figure 1.

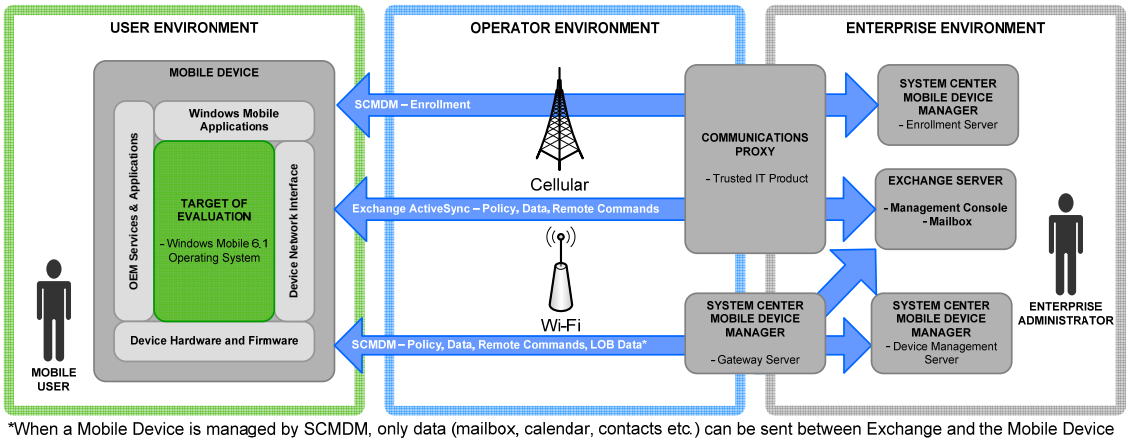

Figure 1 – The TOE operating environment

15 The TOE has the Windows Mobile 6 core security features and extends those capabilities. A description of the TOE security features are as follows.

16 The TOE may be managed through either Enterprise Exchange Server or the System Center Mobile Device Manager (SCMDM). Use of the SCMDM client application on Windows Mobile 6.1 enables management of the Mobile device through SCMDM.

17 Use of Windows Mobile 6.1 with Exchange allows secure communication of the TOE with Line Of Business (LOB) or infrastructure servers over an SSL/TLS tunnel.

18 Alternatively, use of Windows Mobile 6.1 with an SCMDM allows both a secure Mobile VPN using IPSec and an SSL/TLS tunnel to be established. In this configuration, information communicated between the TOE and the trusted enterprise receives 'double enveloped' protection.

19 The TOE supports 128-bit AES encryption of data stored locally on the Mobile Device and on removable storage cards.

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

2.3 TOE Architecture

21 Windows Mobile 6.1 is made up of three layers, namely the Application layer, Operating System layer, and OEM layer, shown in Figure 2. Of these layers, the security functions are implemented by the Operating System layer. The TOE is defined as the Operating System 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 Subsystems (GWES);

i) Device manager subsystem;

j) Storage manager subsystem; and

k) Communications and networking subsystem.

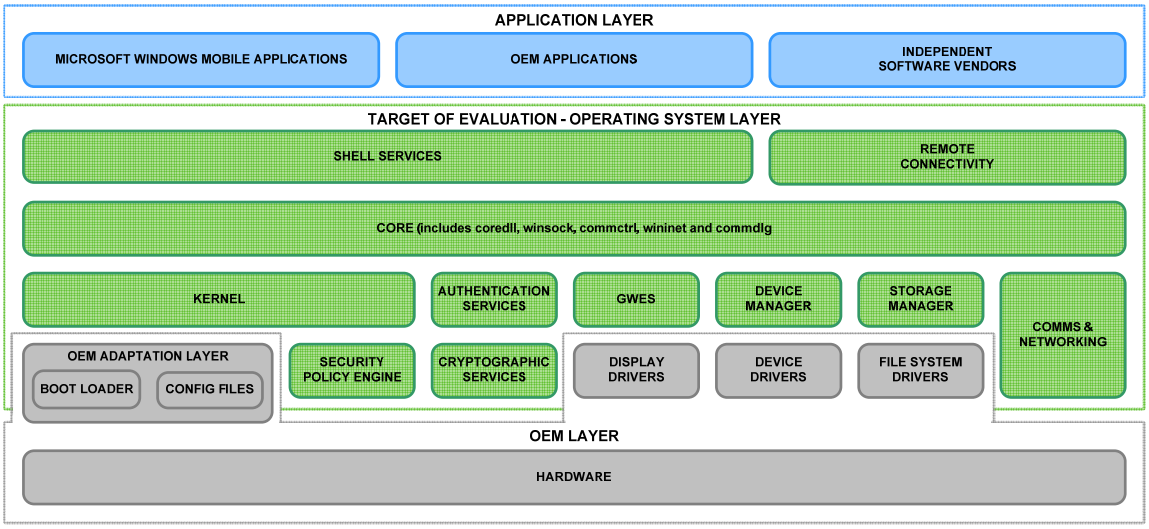

Figure 2 – The TOE architecture

2.4 Clarification of Scope

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

2.4.1 Evaluated Functionality

23 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 at rest and in transit.	**SSL/TLS channel encryption.** SSL/TLS encrypts data transmitted between the device and server, over-the-air or through a wired connection.
	S/MIME support. S/MIME provides additional protection features for e-mail messages, whether in transit between device and server or at rest. S/MIME uses an authentication process which verifies that messages were not tampered.
	Sensitive Data Protection. Windows Mobile 6.1 supports 128-bit AES encryption of data stored locally on the Mobile Device.
	Certified cryptographic module. Windows Mobile includes a certified FIPS validated cryptographic module. Applications can make use of cryptographic modules to perform cryptographic operations.

Security function	TOE security feature
	Mobile VPN. Incorporating secure key exchange (IKEv2), an IPSec VPN tunnel can be established between the TOE and the MDM Gateway Server, supported by an SSL/TLS tunnel between the TOE and LOB or infrastructure server. This 'double envelope' approach provides protection for information communicated between the TOE and the trusted enterprise.
	Storage Card Encryption. Windows Mobile 6.1 supports 128-bit AES encryption of data stored locally on removable storage cards.
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.** Windows Mobile can be configured to only permit applications signed with a trusted certificate to be installed and access privileged resources.
	Controlled application execution. Code execution control allows the device to be locked so that only applications signed with a trusted certificate or approved by the Mobile User can execute on the device.
Secure enterprise access. The TOE provides the capability to securely connect the TOE to trusted Enterprise assets and facilitate data transfer.	**Secure channel.** Windows Mobile establishes a secure channel for communicating with another trusted IT product.
	Synchronization of Mailbox Items. Mobile Users (employing a secure channel) can synchronize their emails, tasks, calendar and contacts with their enterprise mailbox.
	Line of Business server access. Mobile Users can employ the Mobile VPN capability to access Line of Business (LOB) servers within the Enterprise.
Device configuration control. The TOE provides the capability to protect against modification by un-trusted systems.	**Password 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 as authorized by the Enterprise Administrator.
Device access control. The TOE has inbuilt security mechanisms that can be enabled to provide controlled access to the	**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.

Security function	TOE security feature
Mobile Device.	**Local device wipe.** Windows Mobile can be configured to perform a local device wipe after a specified number of incorrect login attempts.
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.

2.4.2 Non-evaluated Functionality

24 Potential users of the TOE are advised that some functions and services have not been evaluated as part of the evaluation. Potential users of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration; Australian Government users should refer to Australian Government Information and Communications Technology Security Manual (ACSI 33) [2] for policy relating to using an evaluated product in an un-evaluated configuration. New Zealand Government users should refer to the New Zealand Information and Communications Technology Security series, (NZSIT 400) [3].

25 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.

26 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

27 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(s) meet the minimum Australian Government policy requirements. New Zealand Government users should refer to NZSIT 400 [3].

28 The evaluated configuration is provided in the Installation and Administrator Guide [4]. The key 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 maximum unsuccessful authentication attempts;

e) SMIME settings, 3DES/SHA1;

f) Applications must be signed to be installed or to run;

g) SI/SL/OMA-CP disabled; and

h) Device password required for Desktop ActiveSync.

2.5.2 Delivery procedures

29 The end customer does not purchase the TOE directly from the developer. Windows Mobile 6.1 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.

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

2.5.2.1 OEM

31 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.

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

a) Submit their developed OEM image to an National Standards Testing Laboratory for independent verification and validation; or

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

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

34 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

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

36 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.

37 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.

38 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

39 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.

40 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.

41 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

42 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

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

a) Windows Mobile 6.1 Installation and Administration Guide 1.0, June 2008 [4]; and

b) Windows Mobile 6.1 User Guide Supplement 1.0, June 2008 [5].

44 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.

45 To gain access to the relevant evaluation guidance the Enterprise Administrator can request access to the Windows Mobile 6 LTK Beta program (covering version 6.1), 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 and secure channel via SSL for all access to Microsoft Connect.

46 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.

47 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 the individual in the Windows Mobile LTK Preview program.

48 To register on Connect, the followings steps should 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.

49 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

50 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.
A.IT_ENTERPRISE	The MDM Gateway Server, MDM Device Management Server, MDM Enrolment Server, Enterprise Exchange Server, Certificate Authority and Active Directory Server are located within the enterprise boundary and are protected from unauthorized logical/physical access.
A.IT_MOBILE	The Trusted Provisioning Server is located within the Mobile Operator's network boundary and is protected from unauthorized 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_NET	The IT environment will provide the server-side of a secure channel between the Trusted Provisioning Server and the Mobile Device.
A.COMMS_ENT	The IT environment will provide the server-side of a secure channel between the Enterprise Exchange Server, MDM Gateway Server, MDM Device Management Server, MDM Enrolment Server, Line of Business 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

51 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

52 The criteria against which the Target of Evaluation (TOE) has been evaluated are contained in the Common Criteria for Information Technology Security Evaluation [6], [7], [8]. The methodology used is described in the Common Methodology for Information Technology Security Evaluation (CEM) [9]. The evaluation was also carried out in accordance with the operational procedures of the Australasian Information Security Evaluation Program (AISEP) [10], [11], [12], [13]. In addition, the conditions outlined in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security [14] were also upheld.

3.3 Functional Testing

53 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

54 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.

55 Of the vulnerabilities identified, 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 recover user data from the internal RAM of the TOE device before the RAM resets to the original factory state. If an attacker obtained the physical TOE device, they could freeze the RAM or use specialised equipment and increase the potential of recovering user data from the RAM. This residual vulnerability is highly dependent on the type of hardware of the mobile device used.

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

56 This chapter contains information about the result of the certification, an overview of the assurance provided by the level chosen, and recommendations made by the certifiers.

4.2 Certification Result

57 After due consideration of the conduct of the evaluation as witnessed by the certifiers, and of the Evaluation Technical Report [15], the Australasian Certification Authority (ACA) certifies the evaluation of Windows Mobile 6.1 performed by the Australasian Information Security Evaluation Facility, stratsec.

58 stratsec has found that Windows Mobile 6.1 upholds the claims made in the Security Target [1] and has met the requirements of the Common Criteria (CC) evaluation assurance level EAL 2 augmented with ALC_FLR.1.

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

4.3 Assurance Level Information

60 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.

61 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).

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

4.4 Recommendations

63 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 refer to NZSIT 400 [3].

64 In addition to ensuring that the assumptions concerning the operational environment are fulfilled and the guidance document is followed [4], [5], the ACA also recommends the following for users and administrators.

a) 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.

b) 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.

c) 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.

d) The administrator should advise users against using the device as a primary data store. This is because device wipe makes the data on a storage card unreadable even if it is removed from the TOE before the wipe is executed, as the keys stored on the device are destroyed.

Annex A - References and Abbreviations

A.1 References

[1] Windows Mobile 6.1 Security Target EAL2 augmented with ALC_FLR.1 1.0, July 2008

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

[3] New Zealand Government Information Technology Security Manual (NZSIT 400), February 2008, Government Communications Security Bureau (available at http://www.gcsb.govt.nz/newsroom/nzsits.html).

[4] Windows Mobile 6.1 Installation and Administration Guide 1.0, June 2008.

[5] Windows Mobile 6.1 User Guide Supplement 1.0, June 2008.

[6] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model (CC), Version 2.3, August 2005, CCMB-2005-08-001.

[7] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements (CC), Version 2.3, August 2005, CCMB-2005-08-002.

[8] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements (CC), Version 2.3, August 2005, CCMB-2005-08-003.

[9] Common Methodology for Information Technology Security Evaluation (CEM), Version 2.3, August 2005, CCMB-2005-08-004.

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

[11] AISEP Publication No. 2 – Certifier Guidance, AP 2. Version 3.1, 29 September 2006, Defence Signals Directorate.

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

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

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

[15] Evaluation Technical Report for Windows Mobile 6.1 v1.0, 25 July 2008.

A.2 Abbreviations and Acronyms

ACSI	Australian Government Information and Communications Technology Security Manual
AES	Advanced Encryption Standard
AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Program
CC	Common Criteria
CRC	Cyclic Redundancy Check
CEM	Common Evaluation Methodology
DSD	Defence Signals Directorate
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GCSB	Government Communications Security Bureau
GWES	Graphics, Windowing and Events Subsystems
LOB	Line of Business
NZSIT	New Zealand Government Information Technology Security Manual
OEM	Original Equipment Manufacturer
PP	Protection Profile
RAM	Random Access Memory
SCMDM	System Center Mobile Device Manager
SFP	Security Function Policy
SFR	Security Functional Requirements
SSL	Secure Sockets Layer
ST	Security Target
TOE	Target of Evaluation
TLS	Transport Layer Security
TSF	TOE Security Functions
TSP	TOE Security Policy