Australian Government
Department of Defence
Intelligence, Security and International Policy

DSD'S CONSUMER GUIDE

WINDOWS MOBILE 5.0 WITH MESSAGING AND SECURITY FEATURE PACK

Product Description

Windows Mobile 5.0 with Messaging and Security Feature Pack (MSFP) is a compact operating system for use on Pocket PCs and Smartphones that allows users to extend their corporate Windows desktop to mobile devices in a secure manner.

Window's Mobile 5.0 with MSFP is an enterprise mobile messaging solution that has a number of features, including:

- applications and services the Windows Mobile operating system can use to securely synchronise and access email, contacts and calendar whilst away from the office workstation;
- the capability for establishing corporate mobile device security policies and standards;
- security functionality designed to protect data while in transit between the mobile device and corporate network;
- the ability to wipe the data, either remotely or locally, in response to the possible compromise of a mobile device; and
- self protection mechanisms to prevent unauthorised code from being executed on the mobile device.

Scope of Evaluation

The scope of the Common Criteria (CC) certification included the following security functionality:

- Device data protection
  - □ SSL/TLS channel encryption
  - □ Certified cryptographic module
- Device application control
  - □ Controlled application installation
  - □ Controlled application execution
- Secure enterprise access
  - □ Secure channel
  - □ Synchronisation of Mailbox items
- Device configuration control
  - □ Exchange ActiveSync Mailbox Policy
  - □ Trusted provisioning

- □ Local configuration control
- Device access control
  - □ Device authentication and lock
  - □ Local device wipe
- Device security management
  - □ Security roles
  - □ Security policies
  - □ Remote wipe

The functions and services that have not been evaluated include:

- Microsoft Windows Mobile applications;
- OEM applications;
- applications provided by independent software vendors;
- drivers;
- the boot loader;
- OEM configuration files; and
- hardware.

Mobile devices with any of the following Adaptation Kit Updates (AKUs) are capable of executing the evaluated handheld software versions.

- 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

Common Criteria Certification Summary

The product has met the requirements of the Common Criteria Evaluation Assurance Level (EAL) 2 augmented with basic flaw remediation (ALC_FLR.1).

DSD's Cryptographic Evaluation

Since the product employs cryptography, DSD is in the process of performing a cryptographic evaluation on the product in addition to the Common Criteria certification.

DSD's Recommendations

As the DSD cryptographic evaluation is yet to be completed, Windows Mobile 5.0 with MSFP can only be used to downgrade the requirements for data in transit from RESTRICTED and IN-CONFIDENCE to UNCLASSIFIED. Furthermore, since filtering functionality was not in the scope of the evaluation, Windows Mobile 5.0 with MSFP solutions can only be connected to RESTRICTED, IN-CONFIDENCE or UNCLASSIFIED agency networks.

Agencies should be aware that user data is not encrypted on Windows Mobile 5.0 with MSFP devices. As a result, devices will take on the classification of the agency network they are connected to.

Agencies should develop Standard Operating Procedures (SOPs) for the protection of classified mobile devices to mitigate threats of lost or stolen active, or recently active, devices.

As the Windows Mobile 5.0 with MSFP devices provide no security for voice calls agencies MUST NOT use devices for classified phone calls.

Agencies wishing to use Windows Mobile 5.0 with MSFP devices should also refer to ACSI 33 policy on:

- Electronic Mail Security,
- Electronic Mail - Protective Marking Policy,
- Portable Electronic Devices, and
- Convergence.

Agencies should also be aware of AGIMO guidance on protective marking. These are the Implementation Guide for Email Protective Markings for Australian Government Agencies and Email Protective Marking Standard for the Australian Government. These can be found at the following locations respectively:

- http://www.agimo.gov.au/__data/assets/pdf_file/0003/46461/Protective_Markings.pdf
- http://www.agimo.gov.au/__data/assets/pdf_file/0010/46459/Email_Protective.pdf

Point of Contact

For further information regarding the certification, cryptographic evaluation or compliance with ACSI 33, please contact DSD on (02) 6265 0197 or email assist@dsd.gov.au.

ACSI 33

The advice given in this document is in accordance with ACSI 33 release date September 2007. Australian Government agencies are reminded to check the latest release of ACSI 33 at www.dsd.gov.au/library/infosec/acsi33.html.

Date of this Consumer Guide

This Consumer Guide was issued by DSD on 03 March 2008.