



WINDOWS MOBILE 6.1 EAL2+

Product Description

Windows Mobile 6.1 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.

Windows Mobile 6.1 is an enterprise mobile messaging solution that has a number of features, these include:

- applications and services the Windows Mobile operating system can use to synchronise and access email, contacts and calendar whilst away from the 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 and at rest on the device and optional external storage cards;
- the ability to wipe saved 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.

Windows Mobile 6.1 extends and strengthens the core security features of the Windows Mobile 6 operating system by encrypting locally stored data and enabling management of mobile devices with System Center Mobile Device Manager (SCMDM). SCMDM provides a 'double-enveloped' (IPSec and SSL) secure mobile VPN capability between the mobile device and the trusted enterprise and improves mobile device management and configuration control.

Scope of Evaluation

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

- Device data protection
- Device application control
- Secure enterprise access
- Device configuration control
- Device access control
- Device security management

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 Adaption Kit Updates (AKUs) are capable of executing the evaluated handheld software versions.

- Build 19212 AKU 1.0.3
- Build 19214 AKU 1.0.4
- Build 19581 AKU 1.1.1

Common Criteria Certification Summary

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

DSD's Cryptographic Evaluation

DSD is required to perform a cryptographic evaluation on the product in addition to the Common Criteria certification. The DSD Cryptographic Evaluation has commenced on a small selection of handsets.

DSD's Recommendations

As the DSD cryptographic evaluation has yet to be completed, Windows Mobile 6.1 EAL2+ can only be used as follows:

Data in Transit

To downgrade the requirements for data in transit from RESTRICTED and IN-CONFIDENCE to UNCLASSIFIED. Windows Mobile 6.1 devices may only be connected to RESTRICTED, IN-CONFIDENCE or UNCLASSIFIED agency networks.

Data at Rest

Windows Mobile 6.1 devices encrypt user data, both locally and on optional external storage cards, using a DSD approved cryptographic algorithm. As a result, handling requirements for devices is approved as follows:

RESTRICTED: A device connected to a RESTRICTED agency network must be handled as RESTRICTED. The handling requirements are not reduced.

IN CONFIDENCE: A device connected to an IN CONFIDENCE agency network may be handled as UNCLASSIFIED.

UNCLASSIFIED: A device connected to an UNCLASSIFIED agency network may be handled as UNCLASSIFIED.

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 6.1 devices provide no security for voice calls agencies **MUST NOT** use devices for classified phone calls.

Agencies wishing to use Windows Mobile 6.1 devices should also refer to ISM policy on:

- Using electronic mail, and
- Portable electronic devices and laptops.

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 location:

- <http://www.finance.gov.au/publications/protective-markings-and-blackberry-devices-guidance/index.html>

Point of Contact

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

Information Security Manual

The advice given in this document is in accordance with ISM release date September 2008. Australian Government agencies are reminded to check the latest release of the ISM at www.dsd.gov.au/library/infosec/ism.html to investigate if any changes have taken place.

Date of this Consumer Guide

This consumer guide was issued by DSD on 23 September 2009 and supersedes any previously issued consumer guide.