



## WINDOWS MOBILE 6

### Product Description

Windows Mobile 6 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 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 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 and at rest on the external storage cards;
- 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
  - S/MIME support
  - Removable storage card 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 17228 AKU 0.1.0 | • Build 17944 AKU 0.3.1 |
| • Build 17233 AKU 0.1.1 | • Build 17945 AKU 0.3.2 |
| • Build 17234 AKU 0.1.2 | • Build 17947 AKU 0.3.3 |
| • Build 17235 AKU 0.1.3 | • Build 17950 AKU 0.3.5 |
| • Build 17236 AKU 0.1.4 | • Build 18120 AKU 0.4.0 |
| • Build 17740 AKU 0.2.0 | • Build 18125 AKU 0.4.2 |
| • Build 17741 AKU 0.2.1 | • Build 18127 AKU 0.4.3 |
| • Build 17742 AKU 0.2.2 | • Build 18128 AKU 0.4.5 |
| • Build 17745 AKU 0.2.3 | • Build 18129 AKU 0.4.6 |
| • Build 17746 AKU 0.2.4 | • Build 18165 AKU 0.5.0 |
| • Build 17747 AKU 0.2.5 | • Build 18317 AKU 0.6.0 |
| • Build 17748 AKU 0.2.6 | • Build 18322 AKU 0.6.1 |
| • Build 17751 AKU 0.2.7 | • Build 18324 AKU 0.6.2 |
| • Build 17754 AKU 0.2.8 | • Build 18325 AKU 0.6.3 |
| • Build 17755 AKU 0.2.9 | • Build 18541 AKU 0.7.0 |
| • Build 17936 AKU 0.3.0 |                         |

## 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 6 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 6 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 6 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 6 devices provide no security for voice calls agencies MUST NOT use devices for classified phone calls.

Agencies wishing to use Windows Mobile 6 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/0003/46461/Protective_Markings.pdf)
- [http://www.agimo.gov.au/\\_\\_data/assets/pdf\\_file/0010/46459/Email\\_Protective.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](mailto: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](http://www.dsd.gov.au/library/infosec/acsi33.html).

## **Date of this Consumer Guide**

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