PROTECT

BLACKBERRY WIRELESS HANDHELD SOFTWARE

VERSIONS 4.1.0, 4.2.0, 4.2.1, 4.2.2, 4.3.0, 4.5.0, 4.6.0, 4.6.1 & 4.7.0

Product Description

The BlackBerry Wireless Handheld allows users to stay connected to a suite of applications including email, phone, enterprise applications, Internet, Short Messaging Service (SMS), and organiser information. The BlackBerry Wireless Handheld integrates with the BlackBerry Enterprise Server which provides centralised management and control of the BlackBerry Wireless Handheld. The BlackBerry Wireless Handheld provides advanced security features to meet confidentiality and security requirements.

Scope of Common Criteria Certification

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

- Secure communication with the BlackBerry Enterprise Server
- Secure communication with other BlackBerry devices
- Remote management of the device
- Content protection
- Third-party application control
- Wireless communication
- Wireless PIM data synchronisation

DSD has performed cryptographic evaluations on the following handsets with the stated software versions:

- BlackBerry 8700 with versions 4.1.0 and 4.5.0
- BlackBerry 8800 with versions 4.2.1 and 4.5.0
- BlackBerry 9000 with version 4.6.0

Other handsets and software versions covered by the Common Criteria evaluation but have not undergone DSD cryptographic evaluation are as follows.

BlackBerry 7130e (4.1.0)	BlackBerry 8100 (4.2.0, 4.5.0)
BlackBerry 8110 (4.3.0)	BlackBerry 8120 (4.3.0)
BlackBerry 8220 (4.6.0)	BlackBerry 8300 (4.2.2, 4.5.0)
BlackBerry 8350i (4.6.1)	BlackBerry 8707 (4.1.0, 4.2.2)
BlackBerry 8830 (4.2.2)	BlackBerry 8900 (4.6.1)
BlackBerry 9500 (4.7.0)	BlackBerry 9530 (4.7.0)

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 performed a cryptographic evaluation on the aforementioned handsets in addition to the Common Criteria certification.

DSD was able to confirm the implementation of encryption for data in transit and data at rest. It was noted that data transmitted between a BlackBerry device and a BES or another BlackBerry device is encrypted using AES or Triple DES. Additionally, the content protection feature was found to encrypt the following stored user data using AES:

- Email - subject, email addresses, message body and attachments
- Calendar - subject, location, organiser, attendees and notes included in the appointment or meeting request
- MemoPad - title and information in the note body
- Tasks - subject and information in the task body
- Contacts - all information except for title and category
- Auto Text - all entries that the original text is replaced with
- BlackBerry Browser - content that is pushed to the TOE, web sites that are saved on the TOE
- Browser cache

PROTECT

DSD's Recommendations

As the BlackBerry handheld devices have been evaluated to EAL2 with a DSD cryptographic evaluation, the DSD evaluated devices are suitable to be used to downgrade the requirements for data at rest. As such, the product can be used in accordance with the Information and Communications Technology Security Manual (ISM) for the storage of information of classifications:

- PROTECTED
- RESTRICTED
- IN-CONFIDENCE
- UNCLASSIFIED

Agencies should be aware that the reduction of handling and storage requirements for BlackBerry handheld devices to UNCLASSIFIED is only in force when information is at rest. This applies only when devices are turned off or unauthenticated to. Conversely, when a device is turned on and authenticated to it takes the classification on the agency network it is connected to. Agencies should develop Standard Operating Procedures (SOPs) for the protection of classified mobile devices to mitigate against threats of lost or stolen active devices.

As the BlackBerry handheld devices provide no security for voice calls agencies MUST NOT use BlackBerry handheld devices for classified phone calls. In addition, agencies MUST NOT use the peer-to-peer messaging or APB capability of the BlackBerry handheld devices to send any classified information.

Additional Resources

Agencies wishing to use BlackBerry handheld devices should refer to the ISM policy on Portable Electronic Devices and Convergence.

Point of contact

For further information regarding the certification of these products, or compliance with the ISM, please contact DSD on (02) 6265 0197 or email assist@dsd.gov.au.

PROTECT

Information Security Manual

The advice given in this document is in accordance with ISM release date September 2009.

Australian Government agencies are reminded to check the latest release of the ISM at http://www.dsd.gov.au/library/infosec/ism.html.

Date of this Consumer Guide

This Consumer Guide was issued by DSD on 20 May 2010.