PROTECT

BLACKBERRY WIRELESS HANDHELD SOFTWARE VERSION 6

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 organizer information. The BlackBerry Wireless Handheld integrates with the BlackBerry Enterprise Server which provides centralized management and control of the BlackBerry Wireless Handheld. The BlackBerry Wireless Handheld provides advanced security features to meet confidentiality and security requirements.

Evaluation Scope

The scope of the DSD Cryptographic Evaluation included the following 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

Common Criteria Certification Summary

The product has met the requirements of the Common Criteria Evaluation Assurance Level (EAL) 4 augmented with basic flaw remediation (ALC_FLR.1).

DSD's Findings and Recommendations

DSD performed a cryptographic evaluation on the product.

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, organizer, 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, websites that are saved to the TOE
- Browser Cache

As the BlackBerry Wireless Handheld has been evaluated to EAL4+ with a DSD cryptographic evaluation, it can be used to downgrade the requirements for data at rest.

As such, the product can be used in accordance with the Australian Government Information 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 Wireless Handheld 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 of the agency network it is connected to. Agencies should develop Standard Operation Procedures (SOPs) for the protection of classified mobile devices to mitigate threats of lost or stolen active devices.

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

PROTECT

Additional Resources

Agencies wishing to use the BlackBerry Wireless Handheld should refer to the ISM controls on Working Off-Site – Mobile Devices.

Point of contact

For further information regarding certification, cryptographic evaluation or compliance with the ISM please contact DSD on 1300 CYBER1 (1300 292 371) or email assist@dsd.gov.au.

Information Security Manual

The advice given in this document is in accordance with ISM release date November 2010. Australian Government agencies are reminded to check the latest release of the ISM at http://www.dsd.gov.au/infosec/ism/index.html.