



## BLACKBERRY ENTERPRISE SERVER

VERSIONS 5.0.0, 5.0.1, 5.0.2, 5.0.3

### Product Description

The BlackBerry Enterprise Server is a software application that resides on a general purpose computer within an enterprise. The BlackBerry Enterprise Server provides a secure wireless extension of the enterprise message environment as well as centralised management and control of enterprise BlackBerry devices by means of the BlackBerry Infrastructure. BlackBerry Enterprise Server core functionality includes:

- Communication with the enterprise mail server
- Secure communication with BlackBerry devices
- Remote management of BlackBerry devices
- Wireless email messaging
- Wireless personal information management (PIM) items synchronization

### Evaluation Scope

The scope of the DSD Cryptographic Evaluation included the following functionality:

- Secure communication with the enterprise mail server
- Secure communication with BlackBerry devices

### 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 correct implementation of encryption for data in transit. It was noted that data transmitted between a BlackBerry device and a BES is encrypted using AES.

As the BlackBerry message solution has been evaluated to EAL4+ with a DSD cryptographic evaluation, it can be used to downgrade the requirements for data in transit.

As such, the product can be used in accordance with the Australian Government Information Security Manual (ISM) for the transit of information of classifications:

- PROTECTED
- RESTRICTED
- IN-CONFIDENCE
- UNCLASSIFIED

Since filtering of messages was not in the scope of evaluation, the BlackBerry solution can only be connected to networks of classifications:

- PROTECTED
- RESTRICTED
- IN-CONFIDENCE
- UNCLASSIFIED

## Additional Resources

Agencies wishing to deploy the BlackBerry solution should refer to the ISM controls on Email Applications – Protective Marking Policy.

DSD provides a hardening guide for the BlackBerry solution. DSD recommends that agencies consider the implementation of as many recommendations as possible to increase the security of their deployed solution.

The hardening guide is considered a compliance document for PROTECTED and RESTRICTED level networks ONLY, however it may assist agencies connecting it to lower classification networks in complying with existing policies in the ISM.

The hardening guide is available from the DSD web site.

## 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](mailto: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>.