# Security Target

**BlackBerry® Enterprise Server Version 5.0.0**

**Document Version 2.0**

**BlackBerry Certifications**

**Research In Motion**

 www.blackberry.com

# Document and Contact Information

| Version | Date | Description |
|---|---|---|
| 2.0 | April 14, 2009 | Document creation. |

| Contact | Corporate Office |
|---|---|
| **BlackBerry Certifications**<br>certifications@rim.com<br>(519) 888-7465 ext. 72921 | **Research In Motion**<br>295 Phillip Street<br>Waterloo, Ontario<br>Canada N2L 3W8<br>www.rim.com<br>www.blackberry.com |

 

# Contents

1 ST Introduction ..... 1
1.1 ST Reference ..... 1
1.2 TOE Reference ..... 1
1.3 Evaluated Configuration ..... 1
1.4 TOE Overview ..... 1
1.5 TOE Description ..... 3
2 Conformance Claim ..... 9
3 Security Problem Definition ..... 10
3.1 Threats ..... 10
3.2 Organisational Security Policies ..... 10
3.3 Assumptions ..... 10
4 Security Objectives ..... 11
4.1 TOE Security Objectives ..... 11
4.2 Environmental Security Objectives ..... 11
4.3 Security Objectives Rationale ..... 11
5 Security Requirements ..... 14
5.1 Conventions ..... 14
5.2 Security Functional Requirements ..... 14
5.3 Security Assurance Requirements ..... 23
5.4 Security Requirements Rationale ..... 24
6 TOE Summary Specification ..... 31
6.1 Security Functions ..... 31
7 Rationale ..... 38
7.1 TOE Security Specification ..... 38
8 Baseline Configuration ..... 42
8.1 Baseline IT Policy Configuration ..... 42
8.2 Baseline Software Configuration ..... 43
9 Glossary ..... 45

 

# List of Tables

Table 1. TOE Components ..... 7
Table 2. Mapping of Security Objectives ..... 12
Table 3. TOE Assurance Components ..... 23
Table 4. Mapping of SFRs to Security Objectives ..... 24
Table 5. SFR Dependencies ..... 25
Table 6. SAR Dependencies ..... 29
Table 7. IT Commands ..... 33
Table 8. IT Policy Rules ..... 33
Table 9. Software Configuration Rules ..... 36
Table 10. Mapping of TOE Security Functions to SFRs ..... 38
Table 11. Baseline IT Policy Configuration ..... 42
Table 12. Baseline Software Configuration ..... 44

 

# List of Figures

Figure 1. BlackBerry Solution Architecture ..... 2
Figure 2. TOE Physical Boundary ..... 6
Figure 3. TOE Physical Boundary ..... 7

 

# 1 ST Introduction

## 1.1 ST Reference

The following information identifies this document:

Title: Security Target: BlackBerry® Enterprise Server Version 5.0.0

Version: 2.0

## 1.2 TOE Reference

The following information identifies the TOE:

Title: BlackBerry® Enterprise Server

Version: 5.0.0

## 1.3 Evaluated Configuration

The evaluated configurations consist of the following:

a. BlackBerry Enterprise Server for IBM Lotus Domino Version 5.0.0 (5.0.0 bundle 223) executing on Microsoft Windows Server™ 2003 Service Pack 2.

b. BlackBerry Enterprise Server for Microsoft Exchange Version 5.0.0 (5.0.0 bundle 223) executing on Microsoft Windows Server 2003 Service Pack 2.

The BlackBerry Enterprise Server version and bundle number is displayed by navigating to the "Add or Remove Programs" interface in Microsoft Windows Server 2003 and clicking the "Click here for support information" link for the BlackBerry Enterprise Server software.

Guidance documents for BlackBerry Enterprise Server for Microsoft Exchange Version 5.0.0 are available at the BlackBerry Technical Solution Center:
http://na.blackberry.com/eng/support/docs/subcategories/?userType=2&category=BlackBerry+Enterprise+Server+for+Microsoft+Exchange

Guidance documents for BlackBerry Enterprise Server for IBM Lotus Domino Version 5.0.0 are available at the BlackBerry Technical Solution Center:
http://na.blackberry.com/eng/support/docs/subcategories/?userType=2&category=BlackBerry+Enterprise+Server+for+IBM+Lotus+Domino

## 1.4 TOE Overview

BlackBerry is the leading wireless solution that allows users to stay connected to a full suite of applications, including email, phone, enterprise applications, Internet, Short Messaging Service (SMS), and organiser information. BlackBerry is a totally integrated package that includes innovative software, advanced BlackBerry wireless devices and wireless network service, providing a seamless solution. The BlackBerry architecture is shown in the following figure.

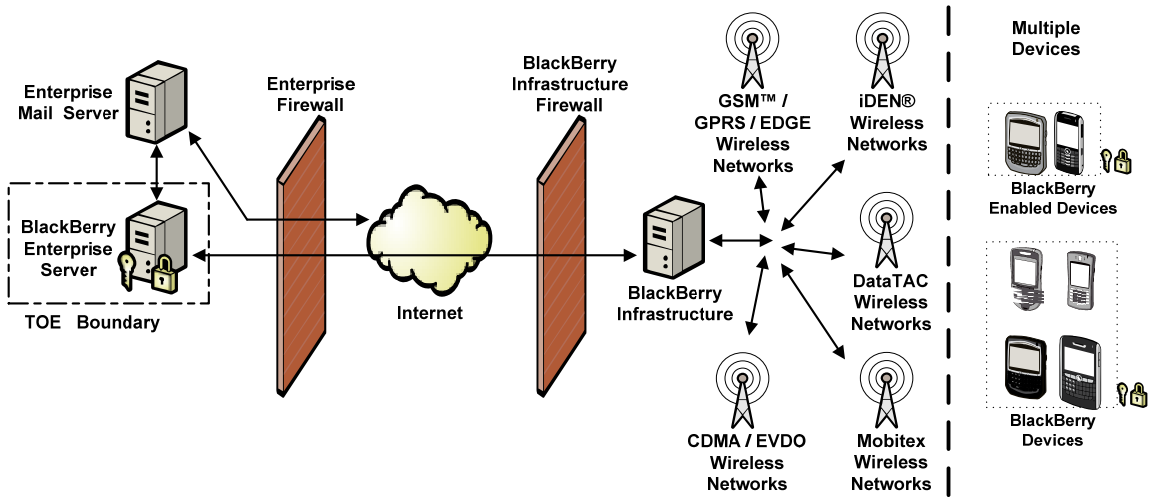


**Figure 1. BlackBerry Solution Architecture**

BlackBerry Enterprise Server software tightly integrates with Microsoft® Exchange, IBM® Lotus® Domino®, and Novell® GroupWise® while working with other existing enterprise systems to enable push-based access of wireless email and data. It allows users to securely send and receive email and information from enterprise data stores and applications. BlackBerry Enterprise Server provides simplified management and centralised control of the wireless environment with industry-standard performance monitoring capabilities, administrative tools, and wirelessly-enabled IT policies. BlackBerry Enterprise Server also enables several other productivity enhancements, including attachment viewing for popular file formats, wireless calendar synchronisation, and remote address lookup, and allows IT departments to benefit from a scalable and flexible solution that meets their evolving wireless requirements.

BlackBerry devices are built on industry-leading wireless technology, allowing users to receive email and information automatically with no need to request for delivery. Additionally, users are notified when new information arrives, making it easier to stay informed.

BlackBerry devices also provide an intuitive user experience. Users simply click on an email address, telephone number, or URL inside a message to automatically begin composing the new email, make the call, or link to the web page. BlackBerry device users can also easily navigate through icons, menus, and options with the roll-and-click trackwheel and quickly compose messages or enter data using the device keyboard.

BlackBerry provides advanced security features to meet the strict confidentiality and security requirements of the public sector. Data remains encrypted at all points between the device and BlackBerry Enterprise Server using FIPS 140-2 validated cryptography, allowing users to feel confident about wirelessly sending and receiving sensitive information.

BlackBerry operates on multiple high speed wireless networks. With wireless service available in North America, South America, Europe, Asia, Australia, and Africa, the BlackBerry solution can support enterprises around the world while providing options for wireless network and service choice.

Visit http://www.blackberry.com for more information on the BlackBerry solution.

## 1.5 TOE Description

### 1.5.1 TOE Features

#### 1.5.1.1.1 Messaging

The BlackBerry solution provides a secure wireless extension of the enterprise messaging environment.

#### 1.5.1.1.2 Email

The TOE integrates seamlessly with existing email accounts. Email is pushed to devices automatically, so users can receive email on their device with the same speed and at least as much reliability as that of their desktop email program.

When users move or delete email messages from their device or their desktop email program, or mark messages read or unread, the changes are reconciled wirelessly between their device and their enterprise email account. Wireless email reconciliation is enabled by default on both the device and the TOE.

#### 1.5.1.2 PIM Data

Users can synchronise personal information management (PIM) items such as calendar entries, tasks, memos, and contacts wirelessly so that the entries on their device and enterprise email account are consistent. If wireless PIM synchronisation is enabled, PIM items are synchronised over the wireless network automatically. With wireless PIM synchronisation and wireless email reconciliation, users do not need to physically connect their device to their desktop to synchronise and reconcile messaging and PIM data.

Users can create or edit meeting requests and accept or decline invitations on their device or their desktop email program. Any changes are synchronised wirelessly between the device and the enterprise email account via the TOE.

When wireless PIM synchronisation is enabled, an initial data synchronisation between the device and the enterprise mail server to fully synchronise both sides is performed in a way that avoids data loss on either side and is optimised for wireless transmission. After the initial synchronisation is complete, incremental changes are synchronised bi-directionally between the device and the enterprise mail server via the TOE.

#### 1.5.1.2.3 Attachments

The TOE enables device users to view supported email attachments on their device in a format that retains the original layout, appearance, and navigation of the attachment. The device attachment viewer is fully integrated with the device mail application and the TOE.

Because the TOE interprets and converts email attachments in binary format, the applications that are associated with the attachment format are not required to be installed on the TOE, and there is no risk of infection on the device by macro viruses that operate within those applications.

The attachment viewer component is installed by default with the TOE software and supports many formats, such as .doc, .dot, .xls, .ppt, .pdf, .txt, .html, .htm, .wpd, and .zip document formats and .jpg, .bmp, .gif, .png, and .tif graphic formats.

#### 1.5.1.2.4 Remote Address Lookup

Remote address lookup enables device users to search for a recipient in their enterprise directory when they compose an email message on their device.

Users can search using letters from the entry's first name, last name, or both. The TOE searches the enterprise directory and returns (up to) the 20 closest matches. If the desired name does not appear in the list, users can request the next 20 search results. When users select a match, they can add the match to their personal address book.

#### 1.5.1.3 BlackBerry Mobile Data Service

The TOE provides the BlackBerry Browser and third-party Java applications with secure access to the Internet and online enterprise data and applications. The TOE can provide a link to standard servers on the enterprise intranet or Internet using standard Internet protocol, such as HTTP, and encrypts content in transit using the same encryption standard used to encrypt email and other BlackBerry data.

#### 1.5.1.4 IT Policy

##### 1.5.1.4.5 Wireless IT Policy

Wireless IT policy enables the TOE administrator to define settings and push them wirelessly to users' devices. A policy consists of rules that define device security, PIM synchronisation settings, and other behaviours for the group of users defined by the TOE administrator. For example, the TOE administrator can define rules and add them to a custom policy designed for sales personnel and then add the personnel to the policy. Because the policies are pushed wirelessly, they are effective immediately.

When the TOE is installed and users are added, the users are first added to the Default policy. Custom policies can also be defined and users added to them. IT policies enable the TOE administrator to define consistent behaviour to simplify managing devices.

##### 1.5.1.4.6 Wireless IT Commands

The TOE administrator can send commands to a device wirelessly and securely. Wireless IT commands include **Erase Data and Disable Handheld** and **Set Password and Lock Handheld**.

#### 1.5.1.5 Security

##### 1.5.1.5.7 BlackBerry Infrastructure

Communication between the TOE and a device is routed by the BlackBerry Infrastructure, the link between the wired and wireless networks in the BlackBerry solution. The communication between the TOE and the BlackBerry Infrastructure utilises the RIM-proprietary Service Routing Protocol (SRP), which allows for a trusted communication channel.

##### 1.5.1.5.8 Secure Communication

The BlackBerry solution enables users to send and receive email and access enterprise data wirelessly, while seamlessly protecting data against attack. Data is encrypted while in transit between the TOE and a BlackBerry device and is never decrypted between these two endpoints.

##### 1.5.1.5.9 Third Party Application Control

The BlackBerry Enterprise Server administrator can control third-party applications on BlackBerry devices in the following ways:

- Allow or disallow third-party applications from being downloaded
- Configure policies that define the type of connections that third-party applications can establish (for example, opening network connections inside the firewall)

- Allow or prevent the installation of specific third-party Java applications on the TOE.
- Limit the permissions of third-party applications, including the resources that the application can access and the types of connections that it can establish.

#### 1.5.1.5.10 Protected storage of external memory on a BlackBerry device

The BlackBerry device is designed to encrypt multimedia data stored on an external memory device according to the External File System Encryption Level IT policy rule or the corresponding BlackBerry device setting.

The BlackBerry device is designed to support:

- File encryption by encrypting specific files on the external memory device using AES-256
- Access control to objects on the external memory device using code signing

The external memory device stores the media card master keys that the BlackBerry device is designed to use to decrypt and encrypt files on the external memory device. The BlackBerry device is designed to use either a device key stored in the NV store in BlackBerry device RAM or a user-provided password to encrypt the master keys.

The BlackBerry device is designed to permit code signing keys in the header information of the encrypted file on the external memory device. The BlackBerry device is designed to check the code signing keys when the BlackBerry device opens the input or output streams of the encrypted file.

The BlackBerry device, any computer platform, and other devices that use the external memory device can modify encrypted files (for example, truncate files) on the external memory device. The BlackBerry device is not designed to perform integrity checks on the encrypted file data.

### 1.5.2 TOE Security Functional Policies

The TOE enforces flow control security functional policies (SFPs) that control information flow to and from the TOE.

#### 1.5.2.1 SRP SFP

The SRP SFP (SRP_SFP) controls the flow of communication between the TOE and a BlackBerry device.

#### 1.5.2.2 Server SFP

The server SFP (Server_SFP) controls the flow of communication between the TOE and the enterprise mail server.

#### 1.5.2.3 IT Command SFP

The IT command SFP (ITCommand_SFP) controls the sending of a wireless IT command to a BlackBerry device.

### 1.5.3 TOE Boundary

#### 1.5.3.1 Physical Boundary

The physical boundary of the TOE is the physical boundary of the general purpose computer executing the BlackBerry Enterprise Server, as shown in the following figure.

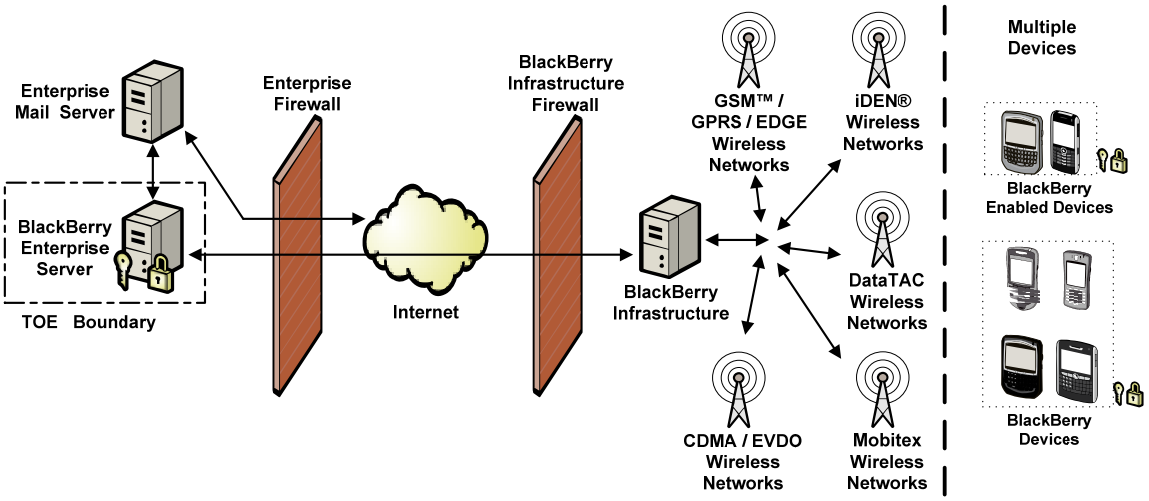


**Figure 2. TOE Physical Boundary**

The following figure further defines the physical boundary of the TOE, and the following table defines the components that comprise the TOE. In particular, the BlackBerry MDS components, which are included with the BlackBerry Enterprise Server product, are excluded from the TOE physical boundary.

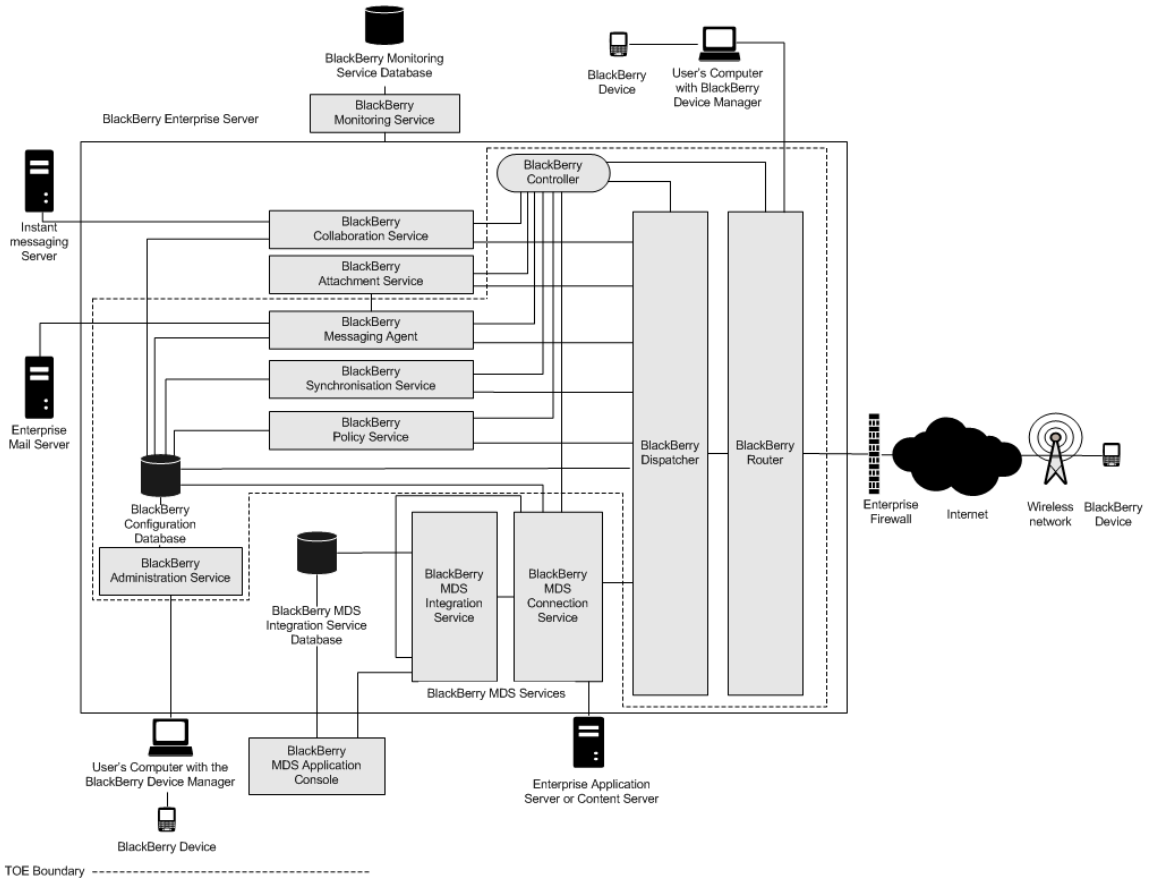


**Figure 3. TOE Physical Boundary**

**Table 1. TOE Components**

| Component | Description |
|---|---|
| BlackBerry Configuration Database | The configuration database is a relational database that contains configuration information that is used by the BlackBerry components that do not connect to the enterprise mail server directly. The configuration database includes the following information:<br>• details about the connection from the BlackBerry Enterprise Server to the wireless network<br>• user list<br>• PIN-to-email address mapping for connection service push functionality<br>• read-only copy of each user security key |
| BlackBerry Controller | The BlackBerry Controller is designed to monitor the BlackBerry components and restart them if they stop responding. |
| BlackBerry Dispatcher | The BlackBerry Dispatcher is designed to compress and encrypt all BlackBerry data. It routes the data through the BlackBerry Router to and from the wireless network. |
| BlackBerry Administration Service | The BlackBerry Administration Service is designed to manage the BlackBerry Domain, which includes BlackBerry Enterprise Server components, user accounts, and features for BlackBerry device administration. |

| Component | Description |
|---|---|
| BlackBerry Messaging Agent | The messaging agent is designed to connect to the messaging and collaboration server to provide message, calendar, address lookup, attachment, and wireless encryption key generation services. The messaging agent also acts as a gateway for the synchronisation service to access PIM data on the messaging server. It synchronises configuration data between the configuration database and user mailboxes. |
| BlackBerry Policy Service | The policy service is designed to perform administration services wirelessly such as sending IT policies and IT commands, and provisioning service books. |
| BlackBerry Router | The BlackBerry Router is designed to connect to the wireless network to route data to and from the BlackBerry device. It is also designed to route data within the corporate network to BlackBerry devices that are connected to the user's computer using the BlackBerry Device Manager. |
| BlackBerry Synchronisation Service | The synchronisation service is designed to synchronise PIM application data between the BlackBerry device and the messaging server wirelessly. |

#### 1.5.3.2 Logical Boundary

The functionality examined in this evaluation is limited to the following core features of the TOE that enable wireless messaging and device management:

- Communication with the enterprise mail server
- Secure communication with BlackBerry devices
- Remote management of BlackBerry devices
- Wireless email messaging and PIM data synchronisation

# 2 Conformance Claim

The target of evaluation (TOE) is Part 2 extended, Part 3 conformant, and EAL 4 augmented to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2. The EAL 4 augmentation is ALC_FLR.1, Basic flaw remediation.

The TOE is not conformant to a protection profile.

# 3 Security Problem Definition

## 3.1 Threats

The following threats are addressed by the TOE:

| | |
|---|---|
| T.RemoteAccess | Unauthorised entities may attempt to remotely access the TOE and execute TOE security functions. |
| T.DataDisclosure | Unauthorised entities may monitor and gain access to user data exchanged between the TOE and the BlackBerry Infrastructure. |
| T.Device | A BlackBerry device under the administrative control of the TOE may violate the enterprise security policy and thereby utilise enterprise resources in an unauthorised manner. |

The following threats are addressed by the environment in which the TOE operates:

| | |
|---|---|
| T.TSFAccess | Personnel authorised to physically access the TOE but unauthorised to access the TOE security functions may attempt to execute TOE security functions. |

## 3.2 Organisational Security Policies

The TOE must comply with the following organisational security policies:

| | |
|---|---|
| P.Admin | The configuration of the TOE security functions and the security functions of the BlackBerry devices under its administrative control must adhere to the enterprise security policy. |
| P.Wireless | The TOE must facilitate a protected wireless extension to the enterprise messaging environment. |

## 3.3 Assumptions

The following assumptions are made about the environment in which the TOE operates:

| | |
|---|---|
| A.PhysicalSecurity | The TOE and enterprise mail server are located in a controlled access facility that prevents unauthorised physical access. |
| A.Network | The TOE is directly connected to the enterprise network, behind the enterprise firewall, and has sufficient privileges to communicate with the enterprise mail server and the BlackBerry Infrastructure. |
| A.Environment | The environment in which the TOE and the enterprise mail server interact protects their communication from unauthorised modification and disclosure. |
| A.ProperAdmin | One or more competent, trusted personnel are assigned and authorised to administer the TOE, and do so using the TOE guidance documentation. |

# 4 Security Objectives

## 4.1 TOE Security Objectives

The following are the TOE security objectives:

| | |
|---|---|
| O.NoRemoteAccess | The TOE must protect itself from unauthorised remote access attempts. |
| O.Admin | The TOE must provide the capability to effectively manage its security functions. |
| O.DeviceAdmin | The TOE must provide the capability to effectively manage the security functions of BlackBerry devices under its administrative control. |
| O.SecureData | The TOE must ensure that all user data exchanged between it and BlackBerry devices is protected from unauthorised disclosure. |
| O.Wireless | For each BlackBerry device under its administrative control, the TOE must facilitate protected bi-directional wireless email messaging and PIM data synchronisation for the enterprise email account associated with the device. |

## 4.2 Environmental Security Objectives

The following security objectives must be met by the environment in which the TOE operates:

| | |
|---|---|
| O.PhysicalSecurity | The TOE and enterprise mail server must be protected from unauthorised physical access. |
| O.Network | The TOE must be able to access the enterprise mail server and the BlackBerry Infrastructure and must be located behind the enterprise firewall. |
| O.Environment | The environment in which the TOE and the enterprise mail server interact must protect their communication from unauthorised modification and disclosure. |
| O.ProperAdmin | The TOE must be administered by trusted, competent personnel in a manner that maintains its security and does not undermine the enterprise security policy or TOE guidance documentation. |
| O.Authentication | The operating system that executes the TOE must require operator authentication prior to granting access to the TOE security functions. |

## 4.3 Security Objectives Rationale

The following table maps the security objectives to the assumptions, threats, and organisational policies identified for the TOE and its environment.

**Table 2. Mapping of Security Objectives**

| | A.PhysicalSecurity | A.Network | A.Environment | A.ProperAdmin | T.RemoteAccess | T.DataDisclosure | T.Device | T.TSFAccess | P.Admin | P.Wireless | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| O.NoRemoteAccess | | | | | X | | | | | | |
| O.Admin | | | | | | | | | X | | |
| O.DeviceAdmin | | | | | | | X | | X | | |
| O.SecureData | | | | | | X | | | | | |
| O.Wireless | | | | | | | | | | X | |
| O.PhysicalSecurity | X | | | | | | | | | | |
| O.Network | | X | | | | | | | | | |
| O.Environment | | | X | | | | | | | | |
| O.ProperAdmin | | | | X | | | | | X | | |
| O.Authentication | | | | | | | | X | | | |

### 4.3.1 A.PhysicalSecurity

The O.PhysicalSecurity objective ensures the TOE and the enterprise mail server are secured from unauthorised physical access.

### 4.3.2 A.Network

The O.Network objective ensures the network connectivity required by the TOE.

### 4.3.3 A.Environment

The O.Environment objective ensures the communication between the TOE and enterprise mail server is protected from unauthorised modification and disclosure.

### 4.3.4 A.ProperAdmin

The O.ProperAdmin objective ensures the TOE administrator is competent and trusted to not violate the security of the TOE or the enterprise security policy and to follow the TOE guidance documentation.

### 4.3.5 T.RemoteAccess

The O.NoRemoteAccess objective ensures that unauthorised entities may not remotely access the TOE and execute TOE security functions even though the TOE has the required network connectivity.

### 4.3.6 T.DataDisclosure

The O.SecureData objective ensures the user data exchanged between the TOE and BlackBerry devices cannot be disclosed to unauthorised entities.

### 4.3.7 T.Device

The O.DeviceAdmin objective ensures the TOE administrator can configure the security functions of the BlackBerry devices under his administrative control.

### 4.3.8 T.TSFAccess

The O.Authentication objective ensures that only authorised personnel can access the TOE security functions.

### 4.3.9 P.Admin

The O.Admin and O.DeviceAdmin objectives ensure the TOE administrator can configure the security functions of the TOE and BlackBerry devices under his administrative control, respectively. The O.ProperAdmin objective ensures that the configuration will not violate the enterprise security policy and will follow the TOE guidance documentation.

### 4.3.10 P.Wireless

The O.Wireless objective ensures the TOE facilitates protected bi-directional wireless email messaging and PIM data synchronisation for enterprise email accounts.

# 5 Security Requirements

This section identifies the security functional and assurance requirements that are applicable to the TOE and the functional requirements that are applicable to the IT environment of the TOE.

## 5.1 Conventions

### 5.1.1 Component Operations

The following typographic conventions are used to identify the permissible operations, as identified in section 6.4.1.3.2 of Part 1, on functional and assurance components:

- Iteration – The iteration operation is identified by enumerating the component. For example, performing the iteration operation on the functional component FMT_MOF.1 would result in the component enumeration FMT_MOF.1 (1) and FMT_MOF.1 (2). Functional elements are also enumerated for clarity, for example, FMT_MOF.1.1 (1) and FMT_MOF.1.1 (2).
- Assignment – The assignment operation is identified with regular text contained in brackets. For example, an assignment operation can be performed on FMT_SMR.1.1 as follows: "The TSF shall maintain the roles [root, guest, and user]."
- Selection – The selection operation is identified with italicised text contained in brackets. For example, a selection operation can be performed on FPT_ITT.1.1 as follows: "The TSF shall protect TSF data from [*disclosure*] when it is transmitted between separate parts of the TOE."
- Refinement – The refinement operation is identified with underscored text. For example, a refinement operation can be performed on FTA_TAB.1.1 as follows: "Before establishing a user session, the TSF shall display an advisory warning message that requires acknowledgement by the user regarding unauthorised use of the TOE."

### 5.1.2 Explicitly Defined Requirements

Explicitly defined functional and assurance requirements are named according to the normal Common Criteria convention with "_EXP" appended. For example, FCS_VAL_EXP.1 is an explicitly defined functional requirement for the FCS, Cryptographic support, functional class.

## 5.2 Security Functional Requirements

The following functional requirements, listed according to their functional class, are applicable to the TOE.

### 5.2.1 Class FCS, Cryptographic Support

#### 5.2.1.1 FCS_VAL_EXP.1, Cryptographic module validation

FCS_VAL_EXP.1.1 The following cryptographic modules of the TSF shall meet the requirements of FIPS 140-2, *Security Requirements for Cryptographic Modules*: [

- BlackBerry Enterprise Server Cryptographic Kernel

].

Dependencies: FCS_CKM.4, FCS_COP.1

#### 5.2.1.2 FCS_CKM.1, Cryptographic key generation (1)

FCS_CKM.1.1 (1) The TSF shall generate cryptographic keys in accordance with a specified key generation algorithm [FIPS 186-2 Appendix 3.1 PRNG] and specified cryptographic key sizes [256 bits (AES)] that meet the following: [FIPS 186-2 Appendix 3.1].

Dependencies: [FCS_CKM.2 or FCS_COP.1], FCS_CKM.4, FMT_MSA.2

#### 5.2.1.3 FCS_CKM.1, Cryptographic key generation (2)

FCS_CKM.1.1 (2) The TSF shall generate cryptographic keys in accordance with a specified key generation algorithm [FIPS 186-2 Change Notice 1 and ANSI X9.62] and specified cryptographic key sizes [571 bits (ECDSA)] that meet the following: [FIPS 186-2 Change Notice 1].

Dependencies: [FCS_CKM.2 or FCS_COP.1], FCS_CKM.4, FMT_MSA.2

#### 5.2.1.4 FCS_CKM.4, Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [zeroization] that meets the following: [FIPS 140-2 zeroization requirements].

Dependencies: [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FMT_MSA.2

#### 5.2.1.5 FCS_COP.1, Cryptographic operation

FCS_COP.1.1 The TSF shall perform [data encryption and decryption, random number generation, message digest generation, message authentication code generation, digital signature generation, and key agreement] in accordance with a specified cryptographic algorithm [

- data encryption and decryption: AES, Triple DES
- random number generation: FIPS 186-2 Appendix 3.1 PRNG
- message digest generation: SHA-1
- message authentication code generation: HMAC
- digital signature generation: ECDSA
- key agreement: ECDH, ECMQV

] and cryptographic key sizes [

- data encryption and decryption: 256 (AES), 192 bits (AES), 128 bits (AES), 112 bits (2-key Triple DES),
- random number generation: not applicable
- message digest generation: not applicable
- message authentication code generation: at least 80 bits
- digital signature generation: 571 bits
- key agreement: 521 bits[1]

] that meet the following: [

[1] The key agreement process results in a 256-bit key for use with AES.

- data encryption and decryption: FIPS 197 (AES), NIST SP 800-38A (CBC mode of operation)
- random number generation: FIPS 186-2
- message digest generation: FIPS 180-2
- message authentication code generation: FIPS 198
- digital signature generation: FIPS 186-2, ANSI X9.62-1998
- key agreement: IEEE P1363 Draft 13

].

Dependencies: [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4, FMT_MSA.2

### 5.2.2 Class FDP, User Data Protection

#### 5.2.2.1 FDP_ETC.2, Export of user data with security attributes (1)

FDP_ETC.2.1 (1) The TSF shall enforce the [SRP_SFP] when exporting user data, controlled under the SFP(s), outside the TOE to the BlackBerry Infrastructure.

FDP_ETC.2.2 (1) The TSF shall export the user data with the user data's associated security attributes.

FDP_ETC.2.3 (1) The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.

FDP_ETC.2.4 (1) The TSF shall enforce the following additional rules when user data is exported from the TOE to the BlackBerry Infrastructure: [none].

Dependencies: [FDP_ACC.1 or FDP_IFC.1]

#### 5.2.2.2 FDP_IFC.1, Subset information flow control (1)

FDP_IFC.1.1 (1) The TSF shall enforce the [SRP_SFP] on [all communication to and from the TOE routed through the BlackBerry Infrastructure (i.e. all communication between the TOE and a BlackBerry device)].

Dependencies: FDP_IFF.1

#### 5.2.2.3 FDP_IFF.1, Simple security attributes (1)

FDP_IFF.1.1 (1) The TSF shall enforce the [SRP_SFP] based on the following types of subject and information security attributes: [for the listed subjects and information:

- TOE (subject):
  - SRP identifier
  - SRP authentication key
  - Master encryption key of source or destination device
- Communication (information):
  - PIN of source or destination device

].

FDP_IFF.1.2 (1) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

- An SRP channel between the TOE and the BlackBerry Infrastructure has been successfully established using the SRP identifier and SRP authentication key.
- The PIN of the corresponding device is included in the information.

].

FDP_IFF.1.3 (1) The TSF shall enforce the following additional rules: [

- The creation of an SRP channel may only be initiated by the TOE.
- During the creation of an SRP channel, the BlackBerry Infrastructure must authenticate to the TSF per FIA_UAU.2 (1) and FIA_UID.2.

].

FDP_IFF.1.4 (1) The TSF shall explicitly authorise an information flow based on the following rules: [none].

FDP_IFF.1.5 (1) The TSF shall explicitly deny an information flow based on the following rules: [

- All information received by the TOE on a TCP/IP port other than 3101 is ignored.
- All attempts by an entity to create an SRP channel with the TOE are ignored.

].

Dependencies: FDP_IFC.1, FMT_MSA.3

#### 5.2.2.4 FDP_ITC.2, Import of user data with security attributes (1)

FDP_ITC.2.1 (1) The TSF shall enforce the [SRP_SFP] when importing user data, controlled under the SFP, from the BlackBerry Infrastructure.

FDP_ITC.2.2 (1) The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3 (1) The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

FDP_ITC.2.4 (1) The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.5 (1) The TSF shall enforce the following additional rules when importing user data controlled under the SFP from the BlackBerry Infrastructure: [none].

Dependencies: [FDP_ACC.1 or FDP_IFC.1], [FTP_ITC.1 or FTP_TRP.1], FPT_TDC.1

#### 5.2.2.5 FDP_ETC.2, Export of user data with security attributes (2)

FDP_ETC.2.1 (2) The TSF shall enforce the [Server_SFP] when exporting user data, controlled under the SFP(s), outside the TSC to the enterprise mail server.

FDP_ETC.2.2 (2) The TSF shall export the user data with the user data's associated security attributes.

FDP_ETC.2.3 (2) The TSF shall ensure that the security attributes, when exported outside the TSC, are unambiguously associated with the exported user data.

FDP_ETC.2.4 (2) The TSF shall enforce the following additional rules when user data is exported from the TSC to the enterprise mail server: [none].

Dependencies: [FDP_ACC.1 or FDP_IFC.1]

#### 5.2.2.6 FDP_IFC.1, Subset information flow control (2)

FDP_IFC.1.1 (2) The TSF shall enforce the [Server_SFP] on [all communication between the TSF and the enterprise mail server].

Dependencies: FDP_IFF.1

#### 5.2.2.7 FDP_IFF.1, Simple security attributes (2)

FDP_IFF.1.1 (2) The TSF shall enforce the [Server_SFP] based on the following types of subject and information security attributes: [for the listed subjects and information:

- Communication (information):
    - Enterprise email account – device PIN mapping

].

FDP_IFF.1.2 (2) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

- Communication between the TOE and the enterprise mail server is always permitted.

].

FDP_IFF.1.3 (2) The TSF shall enforce the following additional rules: [none].

FDP_IFF.1.4 (2) The TSF shall explicitly authorise an information flow based on the following rules: [none].

FDP_IFF.1.5 (2) The TSF shall explicitly deny an information flow based on the following rules: [none].

Dependencies: FDP_IFC.1, FMT_MSA.3

#### 5.2.2.8 FDP_ITC.2, Import of user data with security attributes (2)

FDP_ITC.2.1 (2) The TSF shall enforce the [Server_SFP] when importing user data, controlled under the SFP, from the enterprise mail server.

FDP_ITC.2.2 (2) The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3 (2) The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

FDP_ITC.2.4 (2) The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.5 (2) The TSF shall enforce the following additional rules when importing user data controlled under the SFP from the enterprise mail server: [none].

Dependencies: [FDP_ACC.1 or FDP_IFC.1], [FTP_ITC.1 or FTP_TRP.1], FPT_TDC.1

#### 5.2.2.9 FDP_IFC.1, Subset information flow control (3)

FDP_IFC.1.1 (3) The TSF shall enforce the [ITCommand_SFP] on [sending a wireless IT command to a BlackBerry device].

Dependencies: FDP_IFF.1

#### 5.2.2.10 FDP_IFF.1, Simple security attributes (3)

FDP_IFF.1.1 (3) The TSF shall enforce the [ITCommand_SFP] based on the following types of subject and information security attributes: [for the listed subjects and information:

- TOE (subject):
  - SRP identifier
  - Current time
- IT command (information):
  - IT command type
  - IT command data

].

FDP_IFF.1.2 (3) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

- Sending an IT command to a device (via SRP_SFP) is always permitted.

].

FDP_IFF.1.3 (3) The TSF shall enforce the following additional rules: [none].

FDP_IFF.1.4 (3) The TSF shall explicitly authorise an information flow based on the following rules: [none].

FDP_IFF.1.5 (3) The TSF shall explicitly deny an information flow based on the following rules: [none].

Dependencies: FDP_IFC.1, FMT_MSA.3

### 5.2.3 Class FIA, Identification and Authentication

#### 5.2.3.1 FIA_UAU.2, User authentication before any action (1)

FIA_UAU.2.1 (1) The TSF shall require the BlackBerry Infrastructure to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: FIA_UID.1

#### 5.2.3.2 FIA_UID.2, User identification before any action

FIA_UID.2.1 The TSF shall require the BlackBerry Infrastructure to identify itself before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: None

### 5.2.4 Class FMT, Security Management

#### 5.2.4.1 FMT_MSA.1, Management of security attributes (1)

FMT_MSA.1.1 (1) The TSF shall enforce the [SRP_SFP] to restrict the ability to [*modify*] the security attributes [SRP identifier, SRP authentication key] to [the BlackBerry Enterprise Server administrator].

Dependencies: [FDP_ACC.1 or FDP_IFC.1], FMT_SMF.1, FMT_SMR.1

#### 5.2.4.2 FMT_MSA.1, Management of security attributes (2)

FMT_MSA.1.1 (2) The TSF shall enforce the [Server_SFP] to restrict the ability to [*query*] the security attributes [enterprise email account – device PIN mapping] to [the BlackBerry Enterprise Server administrator].

Dependencies: [FDP_ACC.1 or FDP_IFC.1], FMT_SMF.1, FMT_SMR.1

#### 5.2.4.3 FMT_MSA.1, Management of security attributes (3)

FMT_MSA.1.1 (3) The TSF shall enforce the [ITCommand_SFP] to restrict the ability to [*modify*] the security attributes [IT command type, IT command data] to [the BlackBerry Enterprise Server administrator].

Dependencies: [FDP_ACC.1 or FDP_IFC.1], FMT_SMF.1, FMT_SMR.1

#### 5.2.4.4 FMT_MSA.2, Secure security attributes

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes.

Dependencies: ADV_SPM.1, [FDP_ACC.1 or FDP_IFC.1], FMT_MSA.1, FMT_SMR.1

#### 5.2.4.5 FMT_SMF.1, Specification of management functions

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [

- SRP channel management:
  - Modify the SRP identifier and SRP authentication key
  - Determine the status of the SRP channel
- Management of device functionality[2]:
  - Enable or disable PIN messaging (also known as peer-to-peer messaging)
  - Enable or disable phone capabilities
  - Enable or disable SMS messaging
  - Enable or disable MMS messaging
  - Specify the strength of the elliptic curve cryptography (ECC) public key used by the content protection feature[3]
  - Enable or disable all PIM data synchronisation
  - Enable or disable all Bluetooth® support
  - Enable or disable all WiFi support
  - Enable or disable all GPS support
  - Specify whether the device security locks when placed in the holster
  - Specify the number of days until the device password expires and the user is prompted to provide a new device password

[2] Device functionality is model dependent.
[3] Content protection is a device feature that protects data stored on the device.

- Specify the maximum number of prior passwords against which new passwords can be checked to prevent reuse of the old passwords
- Specify the maximum time, in minutes, allowed before the device security timeout occurs[4]
- Specify the minimum allowable length, in characters, of a password
- Configure the pattern check on a password
- Specify the number of device password attempts (i.e. incorrect device passwords entered) allowed before the device data is erased and the device disabled
- Specify the amount of time, in minutes, before the device security timeout occurs
- Enable or disable a long term security timeout of the device
- Specify the amount of time, in minutes, before the device requires the user to authenticate (even when the device is in use)
- Enable or disable the echoing (i.e. printing to the screen) of characters typed into the device password screen after a given number of failed attempts at unlocking the device
- Enable or disable the ability of the device user to change the specified security timeout
- Enable or disable the ability of the device user to use the browser
- Enable or disable the ability of the device user to use the JavaScript in browser
- Enable or disable protected storage of external memory
- Enable or disable the ability of the device user to use the photo camera
- Enable or disable the ability of the device user to use the video camera
- Enable or disable the ability of the device user to use the voice note recorder

- Management of device:
  - Erase all device information and application data and disable device (see ITCommand_SFP)
  - Set device password and lock device (see ITCommand_SFP)
  - Configure the IT policy group to which a device belongs
  - Configure the software configuration group to which a device belongs
- Management of BlackBerry third-party applications:
  - Enable or disable the ability to download and install third-party applications
  - Enable or disable the ability of third-party applications to initiate connections to entities on the external network
  - Enable or disable the ability of third-party applications to initiate connections to entities on the internal network
  - Enable or disable the ability of third-party applications to access the USB port of the device

[4] The device user can select any timeout value less than this maximum value.

- Limit the permissions of third-party applications to access the TOE resources and user data

].

Dependencies: None

#### 5.2.4.6 FMT_SMR.1, Security roles

FMT_SMR.1.1 The TSF shall maintain the roles [BlackBerry Enterprise Server administrator].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1

### 5.2.5 Class FPT, Protection of the TSF

#### 5.2.5.1 FPT_TDC.1, Inter-TSF basic TSF data consistency (1)

FPT_TDC.1.1 (1) The TSF shall provide the capability to consistently interpret [information whose source or destination is a BlackBerry device] when shared between the TSF and the BlackBerry Infrastructure.

FPT_TDC.1.2 (1) The TSF shall use [the SRP specification] when interpreting the TSF data from the BlackBerry Infrastructure.

Dependencies: None

#### 5.2.5.2 FPT_TDC.1, Inter-TSF basic TSF data consistency (2)

FPT_TDC.1.1 (2) The TSF shall provide the capability to consistently interpret [all information] when shared between the TSF and the enterprise mail server.

FPT_TDC.1.2 (2) The TSF shall use [the listed specification for the identified configuration:

- BlackBerry Enterprise Server for IBM Lotus Domino – Lotus remote procedure call
- BlackBerry Enterprise Server for Microsoft Exchange – Microsoft messaging application programming interface

] when interpreting the TSF data from the enterprise mail server.

Dependencies: None

#### 5.2.5.3 FPT_STM.1, Reliable time stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

Dependencies: None

### 5.2.6 Class FTP, Trusted Path / Channels

#### 5.2.6.1 FTP_ITC.1, Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and the BlackBerry Infrastructure that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit [*the TSF*, *the* BlackBerry Infrastructure] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [sending data to a device].

Dependencies: None

## 5.3 Security Assurance Requirements

The assurance requirements for the TOE are specified by the assurance components in the following table. The components are taken from Part 3 of the Common Criteria and are EAL 4 augmented, with augmented components listed in bold text.

**Table 3. TOE Assurance Components**

| Assurance Class | Assurance Components |
|---|---|
| Security Target evaluation | ASE_CCL.1, Conformance claims |
| | ASE_ECD.1, Extended components definition |
| | ASE_INT.1, ST introduction |
| | ASE_OBJ.2, Security objectives |
| | ASE_REQ.2, Derived security requirements |
| | ASE_SPD.1, Security problem definition |
| | ASE_TSS.1, TOE summary specification |
| Development | ADV_FSP.4, Complete functional specification |
| | ADV_TDS.3, Basic modular design |
| | ADV_ARC.1, Security architecture description |
| | ADV_IMP.1, Implementation representation of the TSF |
| Guidance documents | AGD_OPE.1, Operational user guidance |
| | AGD_PRE.1, Preparative procedures |
| Life cycle support | **ALC_FLR.1, Basic flaw remediation** |
| | ALC_CMC.4, Production support, acceptance procedures and automation |
| | ALC_CMS.4, Problem tracking CM coverage |
| | ALC_DEL.1, Delivery procedures |
| | ALC_DVS.1, Identification of security measures |
| | ALC_LCD.1, Developer defined life-cycle model |
| | ALC_TAT.1, Well-defined development tools |
| Tests | ATE_COV.2, Analysis of coverage |
| | ATE_FUN.1, Functional testing |
| | ATE_IND.2, Independent testing – sample |
| | ATE_DPT.2, Testing: security enforcing modules |
| Vulnerability assessment | AVA_VAN.3, Focused vulnerability analysis |

## 5.4 Security Requirements Rationale

### 5.4.1 Satisfaction of Security Objectives

The following table maps the SFRs to the security objectives for the TOE and its environment.

**Table 4. Mapping of SFRs to Security Objectives**

| | O.NoRemoteAccess | O.Admin | O.DeviceAdmin | O.SecureData | O.Wireless | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| FCS_VAL_EXP.1 | | | | X | | | | | | | |
| FCS_CKM.1 (1) | | | | X | | | | | | | |
| FCS_CKM.1 (2) | | | | X | | | | | | | |
| FCS_CKM.4 | | | | X | | | | | | | |
| FCS_COP.1 | | | | X | | | | | | | |
| FDP_ETC.2 (1) | | | | | X | | | | | | |
| FDP_IFC.1 (1) | X | | | X | X | | | | | | |
| FDP_IFF.1 (1) | X | | | X | X | | | | | | |
| FDP_ITC.2 (1) | | | | | X | | | | | | |
| FDP_ETC.2 (2) | | | | | X | | | | | | |
| FDP_IFC.1 (2) | | | | | X | | | | | | |
| FDP_IFF.1 (2) | | | | | X | | | | | | |
| FDP_ITC.2 (2) | | | | | X | | | | | | |
| FDP_IFC.1 (3) | | | X | | | | | | | | |
| FDP_IFF.1 (3) | | | X | | | | | | | | |
| FIA_UAU.2 (1) | X | | | | | | | | | | |
| FIA_UID.2 | X | | | | | | | | | | |
| FMT_MSA.1 (1) | | X | | | | | | | | | |
| FMT_MSA.1 (2) | | X | | | | | | | | | |
| FMT_MSA.1 (3) | | | X | | | | | | | | |
| FMT_MSA.2 | | | | X | | | | | | | |
| FMT_SMF.1 | | X | X | | | | | | | | |
| FMT_SMR.1 | | X | X | | | | | | | | |
| FPT_TDC.1 (1) | | | | | X | | | | | | |
| FPT_TDC.1 (2) | | | | | X | | | | | | |
| FTP_ITC.1 | | | | | X | | | | | | |
| FPT_STM.1 | | | | | X | | | | | | |

#### 5.4.1.1 O.NoRemoteAccess

FDP_IFC.1 (1) and FDP_IFF.1 (1) ensure that all attempts by an unauthorised entity to remotely access the TSF are explicitly denied. Furthermore, an entity is only authorised to remotely access the TSF once it has successfully authenticated per FIA_UAU.2(1) and FIA_UID.2, under initiation of the TSF.

#### 5.4.1.2 O.Admin

FMT_SMF.1 ensures that the TOE supports administrative functions and FMT_SMR.1 ensures that the TOE supports an administrative role. FMT_MSA.1 (1) ensures that the administrator can manage the SRP channel with the BlackBerry Infrastructure. FMT_MSA.1 (2) ensures that the administrator can manage the mapping between each device and an enterprise email account.

#### 5.4.1.3 O.DeviceAdmin

FDP_IFC.1 (3), FDP_IFF.1 (3), and FMT_MSA.1 (3) ensure that the TOE can issue administrative commands to devices. FMT_SMF.1 ensures that the TOE supports administrative functions and FMT_SMR.1 ensures that the TOE supports an administrative role.

#### 5.4.1.4 O.SecureData

FCS_CKM.1 (1), FCS_CKM.1 (2), FCS_CKM.4, FCS_COP.1 ensure that the TOE implements the cryptographic functionality required to generate and destroy keys and encrypt and decrypt data. FCS_VAL_EXP.1 ensures that the cryptographic operations are implemented correctly. FDP_IFF.1 (1) and FDP_IFC.1 (1) ensure that the TOE encrypts and decrypts data that is sent to and received from a device. FMT_MSA.2 ensures that only secure values can be used for cryptographic operations.

#### 5.4.1.5 O.Wireless

FDP_IFC.1 (1) and FDP_IFF.1 (1) ensure that the TOE can communicate with the BlackBerry Infrastructure, and FDP_ETC.2 (1) and FDP_ITC.2 (1) ensure that the supplied security attributes are correctly associated with the device user. FPT_TDC.1 (1) ensures that the TOE can consistently interpret the data supplied by the BlackBerry Infrastructure. FTP_ITC.1 ensures that the SRP channel between the TOE and the BlackBerry Infrastructure is trusted. FPT_STM.1 ensures that the reliable time stamps provided in each IT command issued to a device.

FDP_IFC.1 (2) and FDP_IFF.1 (2) ensure that the TOE can communicate with the enterprise mail server, and FDP_ETC.2 (2) and FDP_ITC.2 (2) ensure that the supplied security attributes are correctly associated with the device user's enterprise email account. FPT_TDC.1 (2) ensures that the TOE can consistently communicate with the enterprise mail server.

### 5.4.2 Dependencies of Security Functional Requirements

The following table demonstrates that each SFR dependency is either satisfied or has sufficient rationale provided.

**Table 5. SFR Dependencies**

| Requirement | Dependencies | Satisfied By |
|---|---|---|
| FCS_VAL_EXP.1 | FCS_CKM.4 | FCS_CKM.4 |
| | FCS_COP.1 | FCS_COP.1 |
| FCS_CKM.1 (1) | FCS_CKM.2 or FCS_COP.1 | FCS_COP.1 |
| | FCS_CKM.4 | FCS_CKM.4 |

| Requirement | Dependencies | Satisfied By |
|---|---|---|
| | FMT_MSA.2 | FMT_MSA.2 |
| FCS_CKM.1 (2) | FCS_CKM.2 or FCS_COP.1 | FCS_COP.1 |
| | FCS_CKM.4 | FCS_CKM.4 |
| | FMT_MSA.2 | FMT_MSA.2 |
| FCS_CKM.4 | FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 | FCS_CKM.1 |
| | FMT_MSA.2 | FMT_MSA.2 |
| FCS_COP.1 | FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 | FCS_CKM.1 |
| | FCS_CKM.4 | FCS_CKM.4 |
| | FMT_MSA.2 | FMT_MSA.2 |
| FDP_ETC.2 (1) | FDP_ACC.1 or FDP_IFC.1 | FDP_IFC.1 (1) |
| FDP_IFC.1 (1) | FDP_IFF.1 | FDP_IFF.1 (1) |
| FDP_IFF.1 (1) | FDP_IFC.1 | FDP_IFC.1 (1) |
| | FMT_MSA.3 | Not applicable[5] |
| FDP_ITC.2 (1) | FDP_ACC.1 or FDP_IFC.1 | FDP_IFC.1 (1) |
| | FTP_ITC.1 or FTP_TRP.1 | FTP_ITC.1 |
| | FPT_TDC.1 | FPT_TDC.1 (1) |
| FDP_ETC.2 (2) | FDP_ACC.1 or FDP_IFC.1 | FDP_IFC.1 (2) |
| FDP_IFC.1 (2) | FDP_IFF.1 | FDP_IFF.1 (2) |
| FDP_IFF.1 (2) | FDP_IFC.1 | FDP_IFC.1 (2) |
| | FMT_MSA.3 | Not applicable[5] |
| FDP_ITC.2 (2) | FDP_ACC.1 or FDP_IFC.1 | FDP_IFC.1 (2) |
| | FTP_ITC.1 or FTP_TRP.1 | A.Environment[6] |
| | FPT_TDC.1 | FPT_TDC.1 (2) |
| FDP_IFC.1 (3) | FDP_IFF.1 | FDP_IFF.1 (3) |
| FDP_IFF.1 (3) | FDP_IFC.1 | FDP_IFC.1 (3) |
| | FMT_MSA.3 | Not applicable[5] |
| FIA_UAU.2 (1) | FIA_UID.1 | FIA_UID.2 |
| FIA_UID.2 | None | – |
| FMT_MSA.1 (1) | FDP_ACC.1 or FDP_IFC.1 | FDP_IFC.1 (1) |
| | FMT_SMF.1 | FMT_SMF.1 |
| | FMT_SMR.1 | FMT_SMR.1 |
| FMT_MSA.1 (2) | FDP_ACC.1 or FDP_IFC.1 | FDP_IFC.1 (2) |

[5] The dependency on FMT_MSA.3 is not applicable because there are no default values for the identified attributes.
[6] The dependency on FTP_ITC.1 (or FTP_TRP.1) is not satisfied because it is assumed, per A.Environment, that the communication between the TOE and enterprise mail server is protected from unauthorised modification and disclosure.

| Requirement | Dependencies | Satisfied By |
|---|---|---|
| | FMT_SMF.1 | FMT_SMF.1 |
| | FMT_SMR.1 | FMT_SMR.1 |
| FMT_MSA.1 (3) | FDP_ACC.1 or FDP_IFC.1 | FDP_IFC.1 (3) |
| | FMT_SMF.1 | FMT_SMF.1 |
| | FMT_SMR.1 | FMT_SMR.1 |
| FMT_MSA.2 | ADV_SPM.1 | FIPS 140-2 finite state model[7] |
| | FDP_ACC.1 or FDP_IFC.1 | Not applicable[8] |
| | FMT_MSA.1 | Not applicable[8] |
| | FMT_SMR.1 | FMT_SMR.1 |
| FMT_SMF.1 | None | – |
| FMT_SMR.1 | FIA_UID.1 | FIA_UID.2 |
| FPT_TDC.1 (1) | None | – |
| FPT_TDC.1 (2) | None | – |
| FTP_ITC.1 | None | – |
| FPT_STM.1 | None | – |

### 5.4.3 Refinements of Security Functional Requirements on the TOE

#### 5.4.3.1 FDP_ETC.2 (1) Export of User Data with Security Attributes

The SRP_SFP is only applicable for communication between the TOE and the BlackBerry Infrastructure, thus “to the BlackBerry Infrastructure” was added FDP_ETC.2.1 (1) and FDP_ETC.2.4 (1) for clarity. Also in FDP_ETC.2.4 (1) “the following rules” was changed to “the following additional rules” to improve legibility and does not affect the meaning of the functional requirement.

#### 5.4.3.2 FDP_IFF.1 (1) Simple Security Attributes

In FDP_IFF.1.3 (1) “enforce the” was changed to “enforce the following additional rules”. The refinement was made to improve legibility and do not affect the meaning of the functional requirement.

#### 5.4.3.3 FDP_ITC.2 (1) Import of User Data with Security Attributes

The SRP_SFP is only applicable for communication between the TOE and the BlackBerry Infrastructure, thus “outside the TSC” was changed to “to the BlackBerry Infrastructure” in FDP_ITC.2.1 (1) and FDP_ITC.2.5 (1) for clarity. Also in FDP_ITC.2.5 (1) “the following rules” was changed to “the following additional rules” to improve legibility and does not affect the meaning of the functional requirement.

[7] By meeting the requirements of FIPS 140-2, a finite state model of the TSF was prepared and demonstrated that the TSF is always in a known, secure state when accepting and utilising secure cryptographic values.
[8] The TSF automatically generates symmetric keys and performs encryption and decryption as needed and does not provide administration capabilities to the TOE operator. Similarly, administration capabilities are not provided for signature verification or message authentication code generation. Consequently, the dependencies on FDP_ACC.1 (or FDP_IFC.1) and FMT_MSA.1 are not applicable.

#### 5.4.3.4 FDP_ETC.2 (2) Export of User Data with Security Attributes

The Server_SFP is only applicable for communication between the TOE and the enterprise mail server, thus “to the enterprise mail server” was added FDP_ETC.2.1 (2) and FDP_ETC.2.4 (2) for clarity. Also in FDP_ETC.2.4 (2) “the following rules” was changed to “the following additional rules” to improve legibility and does not affect the meaning of the functional requirement.

#### 5.4.3.5 FDP_IFF.1 (2) Simple Security Attributes

In FDP_IFF.1.3 (2) “enforce the” was changed to “enforce the following additional rules”. The refinement was made to improve legibility and do not affect the meaning of the functional requirement.

#### 5.4.3.6 FDP_ITC.2 (2) Import of User Data with Security Attributes

The Server_SFP is only applicable for communication between the TOE and the enterprise mail server, thus “outside the TSC” was changed to “to the enterprise mail server” in FDP_ITC.2.1 (2) and FDP_ITC.2.5 (2) for clarity. Also in FDP_ITC.2.5 (2) “the following rules” was changed to “the following additional rules” to improve legibility and does not affect the meaning of the functional requirement.

#### 5.4.3.7 FDP_IFF.1 (3) Simple Security Attributes

In FDP_IFF.1.3 (3) “enforce the” was changed to “enforce the following additional rules”. The refinement was made to improve legibility and do not affect the meaning of the functional requirement.

#### 5.4.3.8 FIA_UAU.2 (1) User Authentication before Any Action

The TSF only performs authentication for the BlackBerry Infrastructure, thus in FIA_UAU.2.1 (1) “each user” was changed to “the BlackBerry Infrastructure” for clarity.

#### 5.4.3.9 FIA_UID.2 User Authentication before Any Action

The TSF only performs authentication for the BlackBerry Infrastructure, thus in FIA_UID.2.1 “each user” was changed to “the BlackBerry Infrastructure” for clarity.

#### 5.4.3.10 FPT_TDC.1 (1) Inter-TSF Basic TSF Data Consistency

The SRP specification is only used for communication between the TSF and the BlackBerry Infrastructure, thus in FPT_TDC.1.1 (1) and FPT_TDC.1.2 (1) “another trusted IT product” was changed to “the BlackBerry Infrastructure” for clarity.

#### 5.4.3.11 FPT_TDC.1 (2) Inter-TSF Basic TSF Data Consistency

The requirement is placed on communication between the TSF and the enterprise mail server, thus “another trusted IT product” was changed to “the enterprise mail server” in FPT_TDC.1.1 (2) and FPT_TDC.1.2 (2) for clarity.

### 5.4.4 Explicit Security Functional Requirements

#### 5.4.4.1 FCS_VAL_EXP.1 Cryptographic Module Validation

The Common Criteria does not provide an SFR to require that a cryptographic module contained within the TOE boundary meet the requirements of FIPS 140-2. The full statement of FCS_VAL_EXP.1 follows:

FCS_VAL_EXP.1, Cryptographic module validation

FCS_VAL_EXP.1.1 The following cryptographic modules of the TSF shall meet the requirements of FIPS 140-2, *Security Requirements for Cryptographic Modules*: [assignment: *list of cryptographic modules*].

Dependencies: FCS_CKM.4, FCS_COP.1

### 5.4.5 Selection of Security Assurance Requirements

The selection of EAL 4 assurance package is commensurate with the protected environment in which the TOE executes, and the augmentation of ALC_FLR.1 is appropriate to provide assurance to consumers that security flaws are tracked and corrected.

### 5.4.6 Dependencies of Security Assurance Requirements

The following table demonstrates that all SAR dependencies are satisfied.

**Table 6. SAR Dependencies**

| Requirement | Dependencies | Satisfied By |
|---|---|---|
| ASE_CCL.1 | ASE_ECD.1 | ASE_ECD.1 |
| | ASE_INT.1 | ASE_INT.1 |
| | ASE_REQ.1 | ASE_REQ.1 |
| ASE_ECD.1 | None | – |
| ASE_INT.1 | None | – |
| ASE_OBJ.2 | ASE_SPD.1 | ASE_SPD.1 |
| ASE_REQ.2 | ASE_ECD.1 | ASE_ECD.1 |
| | ASE_OBJ.2 | ASE_OBJ.2 |
| ASE_SPD.1 | None | – |
| ASE_TSS.1 | ADV_FSP.1 | ADV_FSP.1 |
| | ASE_ECD.1 | ASE_ECD.1 |
| | ASE_OBJ.2 | ASE_OBJ.2 |
| ADV_FSP.4 | ADV_TDS.1 | ADV_TDS.1 |
| ADV_TDS.3 | ADV_FSP.4 | ADV_FSP.4 |
| ADV_ARC.1 | ADV_FSP.1 | ADV_FSP.1 |
| | ADV_TDS.1 | ADV_TDS.1 |
| ADV_IMP.1 | ADV_TDS.3 | ADV_TDS.3 |
| | ALC_TAT.1 | ALC_TAT.1 |
| AGD_OPE.1 | ADV_FSP.1 | ADV_FSP.1 |
| AGD_PRE.1 | None | – |
| ALC_FLR.1 | None | – |
| ALC_CMC.4 | ALC_CMS.1 | ALC_CMS.1 |
| | ALC_DVS.1 | ALC_DVS.1 |
| | ALC_LCD.1 | ALC_LCD.1 |
| ALC_CMS.4 | None | – |
| ALC_DEL.1 | None | – |
| ALC_DVS.1 | None | – |

| Requirement | Dependencies | Satisfied By |
|---|---|---|
| ALC_LCD.1 | None | – |
| ALC_TAT.1 | ADV_IMP.1 | ADV_IMP.1 |
| ATE_COV.2 | ADV_FSP.2 | ADV_FSP.1 |
| | ATE_FUN.1 | ATE_FUN.1 |
| ATE_FUN.1 | ATE_COV.1 | ATE_COV.1 |
| ATE_IND.2 | ADV_FSP.2 | ADV_FSP.2 |
| | AGD_OPE.1 | AGD_OPE.1 |
| | AGD_PRE.1 | AGD_PRE.1 |
| | ATE_FUN.1 | ATE_FUN.1 |
| | ATE_COV.1 | ATE_COV.1 |
| ATE_DPT.2 | ADV_TDS.3 | ADV_TDS.3 |
| | ADV_ARC.1 | ADV_ARC.1 |
| | ATE_FUN.1 | ATE_FUN.1 |
| AVA_VAN.3 | ADV_FSP.2 | ADV_FSP.2 |
| | ADV_TDS.3 | ADV_TDS.3 |
| | ADV_IMP.1 | ADV_IMP.1 |
| | ADV_ARC.1 | ADV_ARC.1 |
| | AGD_OPE.1 | AGD_OPE.1 |
| | AGD_PRE.1 | AGD_PRE.1 |

### 5.4.7 Refinements of Security Assurance Requirements on the TOE

Refinement operations are not performed on any of the SARs on the TOE.

# 6 TOE Summary Specification

## 6.1 Security Functions

The TOE implements the following security functions:

### 6.1.1 F. Profile BlackBerry Device User Profile

The TOE maintains a profile of each BlackBerry device under its administrative control that contains the following information:

- the enterprise email account that corresponds to the device
- the master encryption key (i.e. AES-256 key) of the device
- the IT policy group to which the device belongs
- the software configuration group to which the device belongs

### 6.1.2 F.SRP Service Routing Protocol

The TOE implements the RIM-proprietary SRP, which allows for a distinct and trusted communication channel with the BlackBerry Infrastructure. The TOE is assigned a unique SRP identifier and SRP authentication key during the TOE manufacturing process. There are no default values for the SRP identifier and SRP authentication key in order to prevent unauthorised communication with the BlackBerry Infrastructure.

The SRP channel is a persistent TCP/IP connection over TCP port 3101 that may only be established when initiated by the TOE. The TOE explicitly denies attempts by any entity, including the BlackBerry Infrastructure, to establish an SRP channel.

Establishment of the SRP channel involves a two-way challenge and response protocol, thus an SRP channel can only be established if the BlackBerry Infrastructure successfully responds to the challenge issued by the TOE and vice versa. The SRP identifier and authentication key are utilised during the challenge and response protocol, and the strength of the protocol is based on the cryptographic strength of HMAC SHA-1.

To send data to a device the TOE sends the data and the PIN of the destination device to the BlackBerry Infrastructure over the SRP channel. The BlackBerry Infrastructure, in turn, routes the data to the destination device over the wireless network.

The SRP channel is also used by the TOE to receive data from a device. The data sent from the device travels over the wireless network to the BlackBerry Infrastructure, and the BlackBerry Infrastructure sends the data and the PIN of the source device to the TOE.

### 6.1.3 F.Transport Secure Data Transport

Data transmitted between the TOE and a device, as described in F.SRP, is encrypted using AES-256. The data is split into 2 KB datagrams and each datagram is encrypted with a unique session key created using the FIPS 186-2 PRNG. The session key is encrypted with the master encryption key, and the encrypted datagram and encrypted session key are transmitted. Once the TOE receives an encrypted datagram, the encrypted session key is decrypted using the master encryption key and the session key is used to decrypt the encrypted datagram.

### 6.1.4 F.Kernel BlackBerry Enterprise Server Cryptographic Kernel

The BlackBerry Enterprise Server Cryptographic Kernel is the cryptographic module responsible for supporting secure data transport from the TOE. It implements, among others, the following cryptographic algorithms:

- AES-256 (CBC mode of operation)
- SHA-1, -256, and -512
- HMAC SHA-1, -256, and -512
- FIPS 186-2 Appendix 3.1 PRNG
- ECDSA
- EC Diffie-Hellman
- EC MQV

Version 1.0.2.10 of the BlackBerry Enterprise Server Cryptographic Kernel is included in BlackBerry Enterprise Server Version 5.0.0 (5.0.0 bundle 223) software and has been awarded FIPS 140-2 validation certificate no.591.

### 6.1.5 F.Email Wireless Email Messaging

The TOE supports wireless email messaging to and from BlackBerry devices. To support email messaging to a device, the TOE monitors the Inbox of the corresponding email account on the enterprise mail server and when a new message arrives sends it to the device (via F.TRANSPORT and F.SRP). To support email messaging from a device, the TOE receives messages from the device (via F.TRANSPORT and F.SRP) and places them in the Outbox of the corresponding email account on the enterprise mail server for delivery. There is no default mapping of an enterprise email account to a device PIN to prevent unauthorised access to the email account.

### 6.1.6 F.PIM Personal Information Management Synchronisation

The TOE supports bi-directional, wireless synchronisation of PIM data between the enterprise mail server and BlackBerry devices. To ensure the PIM data remains current on a device, the TOE monitors the corresponding email account and, whenever the PIM data is modified, sends the updated data to the device (via F.TRANSPORT and F.SRP). To ensure the PIM data remains current on the enterprise mail server, the TOE updates the PIM data of the corresponding email account whenever it receives updated PIM data from a device (via F.TRANSPORT and F.SRP).

### 6.1.7 F.Administration Administration

The TOE provides management capabilities that allow the BlackBerry Enterprise Server administrator to perform the following administrative functions:

- Modify the SRP identifier and authentication key
- Monitor the status of the SRP channel
- View the enterprise email account – device PIN mapping for each device under its administrative control
- Issue IT commands to BlackBerry devices, as specified in F.ITCommand
- Issue IT policy configurations to BlackBerry devices, as specified in F.ITPolicy
- Issue software configurations to BlackBerry devices, as specified in F.SWConfiguration

### 6.1.8 F.ITCommand Wireless IT Commands

The TOE provides management capabilities that allow the BlackBerry Enterprise Server administrator to issue wireless IT commands to the BlackBerry devices under its administrative control. The SRP identifier and current time of the TOE are included with each IT command

issued to a device. The IT commands in the following table may be issued by the BlackBerry Enterprise Server administrator.

**Table 7. IT Commands**

| IT Command | Includes IT Command Data? | Description |
|---|---|---|
| Erase Data and Disable Handheld | No | Erases all information and application data on the device. The device is returned to its factory default settings and is no longer integrated with the email account of the device user. |
| Set Password and Lock Handheld[9] | Yes | Sets the device password to the password specified in the IT command data and locks the device. |
| Set IT Policy | Yes | Specifies the IT policy configuration to be enforced by the device. The IT policy configuration is specified in the IT command data. See F.ITPolicy for more information. |

### 6.1.9 F.ITPolicy Wireless IT Policy

The TOE provides management capabilities that allow the BlackBerry Enterprise Server administrator to configure IT policy rules to be enforced by the BlackBerry devices under its administrative control. In addition to the SRP identifier and current time of the TOE, the following information is included when an IT policy configuration is sent to a device:

- ECDSA public key
- ECDSA signature of the IT policy and ECDSA public key

The BlackBerry Enterprise Server administrator is able to specify an IT policy configuration that consists of the IT policy rules described in the following table, which is a subset of the entire set of IT policy rules supported by the TOE. Refer to *Baseline Configuration* on page 42 for configuration information on the listed IT policy rules.

**Table 8. IT Policy Rules**

| IT Policy Rule | Description |
|---|---|
| Allow Browser | Controls whether the user can use the default browser included on the device. |
| Allow External Connections | Controls whether third-party applications on the device can initiate external connections (e.g., to WAP or other public gateway). |
| Allow Internal Connections | Controls whether third-party applications on the device can initiate internal connections (e.g., to the Mobile Data Service). |
| Allow Peer-to-Peer Messages | Specifies whether device users can send PIN messages. This rule does not prevent device users from receiving PIN messages. |
| Allow Phone | Specifies whether device users can access phone capabilities. This rule does not prevent device users from making emergency phone calls. |
| Allow SMS | Specifies whether device users can send and receive SMS messages. |
| Allow Third Party Apps to Use Serial Port | Specifies whether third-party applications can use the USB port on the device. |

[9] Note that if the **Set Password and Lock Handheld** IT command is executed it overrides the **Password Policy Group** rules presented in Table 11.

| IT Policy Rule | Description |
|---|---|
| Content Protection Strength | Forces the use of the content protection feature and specifies the strength of the ECDH key pair used to generate an AES-256 key while the device is locked.<br>Null – Content protection is not forcibly enabled<br>0 – Strong - 160 bits<br>1 – Stronger - 283 bits<br>2 – Strongest - 571 bits |
| Disable 3DES Transport Crypto | Forces the device to encrypt and decrypt packets to and from the BlackBerry Enterprise Server that sent the IT policy using AES instead of Triple DES. |
| Disable All Wireless Sync | Disables wireless synchronisation of PIM data. |
| Disable Bluetooth | Disables all Bluetooth support. |
| Disable External Memory | Specifies whether to prevent the expandable memory (microSD) feature from working on supported BlackBerry devices. |
| Disable GPS | Specifies whether the GPS functionality on the BlackBerry device is turned on. |
| Disable JavaScript in Browser | Specifies whether to prevent JavaScript execution in the BlackBerry Browser. |
| Disable MMS | Specifies whether to prevent the BlackBerry device user from using Multimedia Messaging Service (MMS) functionality on the BlackBerry device. |
| Disable Photo Camera | Specifies whether the ability to take still pictures with the camera is turned off on the BlackBerry device. |
| Disable USB Mass Storage | Specifies whether to prevent the USB Mass Storage feature from working on supported BlackBerry devices. |
| Disable Video Camera | Specifies whether the ability to record video with the camera is turned off on the BlackBerry device. Set this rule to True to turn off the video recorder feature. |
| Disable Voice Note Recording | Specifies whether the voice note recording feature on the BlackBerry device is turned on. |
| Disable WLAN | Disables use of WLAN on the device. |
| Disallow Third Party Application Downloads | Specifies whether third-party applications may be downloaded and installed on the device. |
| Enable Long Term Timeout | Controls whether the device locks after a predefined period of time, regardless of user activity. |
| External File System Encryption Level | Specifies the level of encryption that the BlackBerry device uses to encrypt files that it stores on an external file system, such as an external memory device.<br>0 – Not Required<br>1 - Encrypt to User Password (excluding multimedia directories)<br>2 - Encrypt to User Password (including multimedia directories)<br>3 - Encrypt to Device Key (excluding multimedia directories)<br>4 - Encrypt to Device Key (including multimedia directories)<br>5 - Encrypt to User Password and Device Key (excluding multimedia directories)<br>6 - Encrypt to User Password and Device Key (including multimedia directories) |
| Force Lock When Holstered | Specifies whether the device is locked when placed in the holster. |

| IT Policy Rule | Description |
|---|---|
| Maximum Password Age | Specifies the number of days until a device password expires and the user is prompted to provide a new password.<br>0 – The password never expires.<br>1-65535 – The password expires after the specified number of days. |
| Maximum Password History | Specifies the maximum number of previous device passwords against which new passwords can be checked to prevent reuse of the old passwords.<br>0 – The password is not checked against previous passwords.<br>1-15 – The password is checked against the specified number of previous passwords. |
| Maximum Security Timeout | Specifies the maximum time, in minutes, allowed before a device security timeout occurs. The device user can select any timeout value less than the maximum value. |
| Minimum Password Length | Specifies the minimum allowable length, in characters, of the device password. |
| Password Pattern Checks | Creates a pattern check on the device password.<br>0 – No restrictions.<br>1 – The password must contain at least one alpha and one numeric character.<br>2 – The password must contain at least one alpha, one numeric, and one special character.<br>3 – The password must contain at least one uppercase alpha, one lowercase alpha, one numeric, and one special character. |
| Password Required | Specifies whether the use of a device password is required. |
| Periodic Challenge Time | Specifies the interval, in minutes, after which the user is prompted to enter a password, regardless of user activity. |
| Set Maximum Password Attempts | Specifies the number of unsuccessful authentication attempts (i.e. the number of incorrect passwords entered) allowed on the device before the device data is erased and the device disabled. |
| Set Password Timeout | Specifies the amount of time, in minutes, before the security timeout occurs on the device. |
| S/MIME Allowed Content Ciphers | Specifies the content ciphers that the BlackBerry device can use to encrypt S/MIME messages.<br>0 - AES (256-bit)<br>1 - AES (192-bit)<br>2 - AES (128-bit)<br>3 - CAST (128 bit)<br>4 - RC2 (128 bit)<br>5 - Triple DES (112 bit)<br>6 - RC2 (64 bit)<br>7 - RC2 (40 bit) |
| Suppress Password Echo | Disables the echoing (printing to the screen) of characters typed into the device password screen[10]. |
| User Can Change Timeout | Specifies whether the device user can change the specified security timeout. |

[10] BlackBerry devices that use SureType® technology, such as the BlackBerry 7130e, briefly display feedback to the user before masking password characters with an asterisk

### 6.1.10 F.Environment Enterprise Email Environment

The TOE supports integration into the IBM Lotus Domino and Microsoft Exchange enterprise email environments.

### 6.1.11 F.SWConfiguration Software Configuration

The TOE provides the ability to control access of third-party applications to TOE resources and user data subject to the restrictions specified by the BlackBerry Enterprise Server administrator. The user can make application access control configuration more restrictive by changing application permissions on the TOE.

The TOE is able to enforce a software configuration that consists of the software configuration policy rules specified in the following table, which is a subset of the entire set of the software configuration policy rules supported by the TOE.

BlackBerry Enterprise Server administrator can use a default application control policy that blocks all third-party applications. To permit specific third-party applications to run on BlackBerry devices, the administrator can register those applications in the shared folder and apply a new application control policy that permits only those applications. When users try to download third party applications to their BlackBerry devices, the devices add only the allowed applications. To prevent users from deleting permitted third-party applications from their BlackBerry devices, administrator must set the application control policy to permit the application as required, instead of optional.

**Table 9. Software Configuration Rules**

| Software Configuration Rule | Description |
|---|---|
| Disposition | Specify whether the application is optional, required, or not allowed on the BlackBerry device. You can use this software configuration rule to require that the BlackBerry device download a specific application or prevent the BlackBerry device from downloading an unspecified or untrusted application.<br>To delete all existing third-party applications from the BlackBerry device and prevent the BlackBerry device from adding any new third-party applications, administrator sets **Disposition** to **Disallowed**. To permit the third-party application, one of the following actions can be performed:<br>• To permit the user to add the third-party application to the BlackBerry device, and to permit the user to delete the application from the BlackBerry device, administrator sets **Disposition** to **Optional**.<br>• To push the application to the BlackBerry device over the wireless network automatically, and to prevent the user from deleting the application from the BlackBerry device, administrator sets **Disposition** to **Required**. |
| Interprocess Communication | Specify whether or not the application can perform interprocess communication operations. You can use this software configuration rule to prevent two or more applications from sharing data and to prevent one application from using the connection permissions of another application. |
| Internal Network Connections | Specify whether or not the application can make internal corporate network connections. You can use this software configuration rule to allow or prevent the application from sending or receiving data on the BlackBerry device using an internal protocol (for example, using the connection service) or to require that the user respond to a prompt on the BlackBerry device to allow internal connections through the BlackBerry device firewall. |
| External Network Connections | Specify whether or not the application can make external network connections. You can use this software configuration rule to allow or prevent the application from sending or receiving data on the BlackBerry device using an external protocol (for example, using a WAP gateway, public BlackBerry MDS Services, or TCP), or to require that the user respond to a prompt on their BlackBerry device to allow external connections through the BlackBerry device firewall. |

| Software Configuration Rule | Description |
|---|---|
| Local Connections | Specify whether or not the application can make local network connections (for example, connections to the BlackBerry device using a USB or serial port). |
| Phone Access | Specify whether or not the application can make phone calls and access phone logs on the BlackBerry device. You can use this software configuration rule to allow or prevent the application from making calls on the BlackBerry device or to require that the user respond to a prompt on the BlackBerry device to allow the application to make a phone call. |
| Message Access | Specify whether or not the application can send and receive messages on the BlackBerry device using the email API. |
| PIM Data Access | Specify whether or not the application can access the BlackBerry device PIM APIs, which control access to the user's personal information on the BlackBerry device, including the address book.<br>**Note**: Allowing the application to access PIM data APIs and use internal and external network connection protocols creates an opportunity for an application to send all of the user's personal data from their BlackBerry device. |
| Event Injection | Specify whether or not the application can inject synthetic input events, such as pressing keys and performing trackwheel actions, on the BlackBerry device. |
| Bluetooth Serial Profile | Specify whether or not the application can access the Bluetooth® Serial Port Profile (SPP) API.<br>**Note**: If you set the Disable Serial Port Profile IT policy rule to True, the Bluetooth enabled BlackBerry device cannot use the Bluetooth SPP to establish a serial connection to a Bluetooth enabled device. |
| BlackBerry Device Keystore | Specify whether or not the application can access the BlackBerry device key store APIs.<br>If you set the Minimal Signing Key Store Security Level and the Minimal Encryption Key Store Security Level IT policy rules to high, the BlackBerry device prompts the user for the BlackBerry device key store password each time an application tries to access the user's private key on the BlackBerry device, and the BlackBerry device does not use this software configuration rule. |
| BlackBerry Device Keystore Medium Security | Specify whether or not the application can access key store items at the medium security level (the default level), which requires that the BlackBerry device prompt the user for the BlackBerry device key store password when an application tries to access the user's private key for the first time or when the private key password timeout expires.<br>If you set the Minimal Signing Key Store Security Level and the Minimal Encryption Key Store Security Level IT policy rules to high, the BlackBerry device prompts the user for the BlackBerry device key store password each time an application tries to access their private key, and this software configuration rule is not recognized. |
| Device GPS | Specify whether or not the application can access the BlackBerry device Global Positioning System (GPS) APIs. You can use this software configuration rule to allow or prevent the application from accessing the GPS APIs on the BlackBerry device or to require that the user respond to a prompt on the BlackBerry device to allow access to the GPS APIs. |
| User Authenticator API | Specify whether or not the BlackBerry device allows an application to access the user authenticator framework API. The user authenticator framework allows the registration of drivers (currently smart card drivers only) that provide two-factor authentication to unlock the BlackBerry device. This software configuration rule applies to the BlackBerry Device Software and third-party Java applications. |

# 7 Rationale

## 7.1 TOE Security Specification

### 7.1.1 TOE Security Functions

The following table maps the TOE security functions to the SFRs.

**Table 10. Mapping of TOE Security Functions to SFRs**

| | F.Profile | F.SRP | F.Transport | F.Kernel | F.Email | F.PIM | F.Administration | F.ITCommand | F.ITPolicy | F.Environment | F.SWConfiguration |
|---|---|---|---|---|---|---|---|---|---|---|---|
| FCS_VAL_EXP.1 | | | | X | | | | | | | |
| FCS_CKM.1 (1) | | | | X | | | | | | | |
| FCS_CKM.1 (2) | | | | X | | | | | | | |
| FCS_CKM.4 | | | | X | | | | | | | |
| FCS_COP.1 | | | | X | | | | | | | |
| FDP_ETC.2 (1) | | X | | | | | | | | | |
| FDP_IFC.1 (1) | | X | X | | | | | | | | |
| FDP_IFF.1 (1) | X | X | X | X | | | | | | | |
| FDP_ITC.2 (1) | | X | | | | | | | | | |
| FDP_ETC.2 (2) | X | | | | X | X | | | | | |
| FDP_IFC.1 (2) | X | | | | X | X | | | | | |
| FDP_IFF.1 (2) | X | | | | X | X | | | | | |
| FDP_ITC.2 (2) | X | | | | X | X | | | | | |
| FDP_IFC.1 (3) | | | | | | | | X | X | | X |
| FDP_IFF.1 (3) | | | | | | | | X | X | | X |
| FIA_UAU.2 (1) | | X | | | | | | | | | |
| FIA_UID.2 | | X | | | | | | | | | |
| FMT_MSA.1 (1) | | | | | | | X | | | | |
| FMT_MSA.1 (2) | | | | | | | X | | | | |
| FMT_MSA.1 (3) | | | | | | | X | | | | |
| FMT_MSA.2 | | | | X | | | | | | | |
| FMT_SMF.1 | | | | | | | X | X | X | | |
| FMT_SMR.1 | | | | | | | X | | | | |
| FPT_TDC.1 (1) | | X | | | | | | | | | |
| FPT_TDC.1 (2) | | | | | | | | | | X | |
| FTP_ITC.1 | | X | X | X | | | | | | | |

| | F.Profile | F.SRP | F.Transport | F.Kernel | F.Email | F.PIM | F.Administration | F.ITCommand | F.ITPolicy | F.Environment | F.SWConfiguration |
|---|---|---|---|---|---|---|---|---|---|---|---|
| FPT_STM.1 | | | | | | | | X | | | |

#### 7.1.1.1 FCS_VAL_EXP.1, Cryptographic module validation

The cryptographic module embedded in the TOE meets the requirements of FIPS 140-2 (F.Kernel).

#### 7.1.1.2 FCS_CKM.1, Cryptographic key generation (1)

The cryptographic module embedded in the TOE is validated to FIPS 140-2 and generates AES keys using the FIPS 186-2 PRNG (F.Kernel).

#### 7.1.1.3 FCS_CKM.1, Cryptographic key generation (2)

The cryptographic module embedded in the TOE is validated to FIPS 140-2 and generates ECDSA keys using the FIPS 186-2 Change Notice 1 and ANSI X9.62 (F.Kernel).

#### 7.1.1.4 FCS_CKM.4, Cryptographic key destruction

The cryptographic module embedded in the TOE is validated to FIPS 140-2 and destroys keys according to the FIPS 140-2 key zeroization requirements (F.Kernel).

#### 7.1.1.5 FCS_COP.1, Cryptographic operation

The cryptographic module embedded in the TOE is validated to FIPS 140-2 and performs AES data encryption and decryption; FIPS 186-2 Appendix 3.1 random number generation, and message authentication code generation (F.Kernel). The TOE provides S/MIME messaging functionality .

#### 7.1.1.6 FDP_ETC.2, Export of user data with security attributes (1)

When sending data to a device, the SRP ensures that user data sent from the TOE to the BlackBerry Infrastructure is associated with the PIN of the destination device (F.SRP).

#### 7.1.1.7 FDP_IFC.1, Subset information flow control (1)

All communication between the TOE and a device is mediated by the BlackBerry Infrastructure, and the communication between the TOE and the BlackBerry Infrastructure follows the SRP (F.SRP). All data transferred between the TOE and a device is protected (F.Transport).

#### 7.1.1.8 FDP_IFF.1, Simple security attributes (1)

All communication between the TOE and a device is mediated by the BlackBerry Infrastructure, and the communication between the TOE and the BlackBerry Infrastructure follows the SRP (F.SRP). Only the TOE may initiate a communication channel with the BlackBerry Infrastructure, and all attempts by an entity to establish a communication channel with the TOE are explicitly denied (F.SRP). All data transferred between the TOE and a device is protected through the use

of encryption (F.Transport, F.Kernel). The TOE ensures that data encrypted for the device uses the appropriate encryption key (F.Profile).

#### 7.1.1.9 FDP_ITC.2, Import of user data with security attributes (1)

When receiving data from a device, the SRP ensures that user data sent to the TOE from the BlackBerry Infrastructure is associated with the PIN of the source device (F.SRP).

#### 7.1.1.10 FDP_ETC.2, Export of user data with security attributes (2)

The TOE maintains a profile for each device under its administrative control that maps the device user's enterprise email account to the PIN of his device (F.Profile). The protocol utilised to communicate with the enterprise mail server ensures that user data sent from the TOE is associated with the enterprise email account – device PIN mapping (F.Email, F.PIM).

#### 7.1.1.11 FDP_IFC.1, Subset information flow control (2)

The TOE maintains a profile for each device under its administrative control that maps the device user's enterprise email account to the PIN of his device (F.Profile). The TOE supports wireless email messaging and PIM data synchronisation (F.Email, F.PIM).

#### 7.1.1.12 FDP_IFF.1, Simple security attributes (2)

The TOE maintains a profile for each device under its administrative control that maps the device user's enterprise email account to the PIN of his device (F.Profile). The TOE supports wireless email message and PIM data synchronisation (F.Email, F.PIM).

#### 7.1.1.13 FDP_ITC.2, Import of user data with security attributes (2)

The TOE maintains a profile for each device under its administrative control that maps the device user's enterprise email account to the PIN of his device (F.Profile). The protocol utilised to communicate with the enterprise mail server ensures that user data sent to the TOE is associated with the enterprise email account – device PIN mapping (F.Email, F.PIM).

#### 7.1.1.14 FDP_IFC.1, Subset information flow control (3)

The TOE provides the BlackBerry Enterprise Server administrator with the capability to issue IT commands to and set the IT policy configuration and software configuration of devices under its administrative control (F.ITCommand, F.ITPolicy).

#### 7.1.1.15 FDP_IFF.1, Simple security attributes (3)

The TOE provides the BlackBerry Enterprise Server administrator with the capability to issue IT commands to and set the IT policy configuration and software configuration of devices under its administrative control (F.ITCommand, F.ITPolicy).

#### 7.1.1.16 FIA_UAU.2, User authentication before any action (1)

The BlackBerry Infrastructure must authenticate to the TOE before an SRP channel can be established (F.SRP).

#### 7.1.1.17 FIA_UID.2, User identification before any action

The BlackBerry Infrastructure must authenticate to the TOE before an SRP channel can be established (F.SRP).

#### 7.1.1.18 FMT_MSA.1, Management of security attributes (1)

The TOE provides the BlackBerry Enterprise Server administrator with the capability to modify the SRP identifier and authentication key (F.Administration).

#### 7.1.1.19 FMT_MSA.1, Management of security attributes (2)

The TOE provides the BlackBerry Enterprise Server administrator with the capability to view the enterprise email account – device PIN mapping for all devices under administrative control of the TOE (F.Administration).

#### 7.1.1.20 FMT_MSA.1, Management of security attributes (3)

The TOE provides the BlackBerry Enterprise Server administrator with the capability to specify which IT commands, and the corresponding IT command data, are sent to devices (F.Administration).

#### 7.1.1.21 FMT_MSA.2, Secure security attributes

The BlackBerry Enterprise Server Cryptographic Kernel ensures that only secure cryptographic values are accepted and utilised, per the requirements of FIPS 140-2 (F.Kernel).

#### 7.1.1.22 FMT_SMF.1, Specification of management functions

The TOE provides SRP channel management functions (F.Administration), IT policy management functions (F.ITPolicy), and IT command management functions (F.ITCommand).

#### 7.1.1.23 FMT_SMR.1, Security roles

The TOE supports the BlackBerry Enterprise Server administrator role (F.Administration).

#### 7.1.1.24 FPT_TDC.1, Inter-TSF basic TSF data consistency (1)

The TOE communicates with the BlackBerry Infrastructure using the SRP (F.SRP).

#### 7.1.1.25 FPT_TDC.1, Inter-TSF basic TSF data consistency (2)

The TOE supports the IBM Lotus Domino and Microsoft Exchange enterprise email environments (F.Environment).

#### 7.1.1.26 FTP_ITC.1, Inter-TSF trusted channel

The TOE communicates with the BlackBerry Infrastructure using an SRP channel which provides assurance of its endpoints (F.SRP). Communication between the TOE and the BlackBerry Infrastructure is protected through the use of encryption (F.Transport, F.Kernel).

#### 7.1.1.27 FPT_STM.1, Reliable time stamps

The TOE provides reliable date and time information included with each IT Command issued to a device. (F.ITCommand).

# 8 Baseline Configuration

## 8.1 Baseline IT Policy Configuration

The baseline IT policy configuration is the evaluated configuration of the TOE that provides the most flexibility to tailor the listed IT policy rules to comply with an enterprise security policy. The deployed configuration of the TOE shall be at least as restrictive as the baseline configuration. The following table identifies the valid range of values, default value, and baseline value for each IT policy rule specified in F.ITPolicy. With the exception of the values marked with an asterisk ("*"), modifying the baseline values will result in a more restrictive configuration, and thus may be configured to comply with an enterprise security policy while maintaining an evaluated configuration. Refer to the BlackBerry Enterprise Server Policy Reference Guide and appropriate System Administration Guide for instructions on configuring IT policy rules.

**Table 11. Baseline IT Policy Configuration**

| IT Policy Rule | Value | | |
|---|---|---|---|
| | Range | Default | Baseline |
| Global Policy Group | | | |
| Allow Browser | {Yes, No} | Yes | Yes |
| Allow Phone | {Yes, No} | Yes | Yes |
| Common Policy Group | | | |
| Disable MMS | {Yes, No} | No | No |
| Disable Voice Note Recording | {Yes, No} | No | No |
| Security Policy Group | | | |
| Allow External Connections | {Yes, No} | Yes | Yes |
| Allow Internal Connections | {Yes, No} | Yes | Yes |
| Allow Third Party Apps to Use Serial Port | {Yes, No} | Yes | Yes |
| Content Protection Strength | 0-2 | Null | Null |
| Disable 3DES Transport Crypto | {Yes, No} | No | Yes* |
| Disable GPS | {Yes, No} | No | No |
| Disable External Memory | {Yes, No} | No | No |
| Disable USB Mass Storage | {Yes, No} | No | No |
| Disallow Third Party Application Downloads | {Yes, No} | No | No |
| External File System Encryption Level | 0-6 | 0 | 0 |
| Force Lock When Holstered | {Yes, No} | No | No |
| Device-Only Policy Group | | | |
| Allow Peer-to-Peer Messages | {Yes, No} | Yes | Yes |
| Allow SMS | {Yes, No} | Yes | Yes |
| Enable Long Term Timeout | {Yes, No} | Null | Null |
| Maximum Password Age | 0-65535 | 0 | 0 |
| Maximum Security Timeout | 10-480 | Null | 60 |

| IT Policy Rule | Value | | |
|---|---|---|---|
| | Range | Default | Baseline |
| Minimum Password Length | 4-14 | 4 | 4 |
| Password Pattern Checks[11] | 0-3 | 0 | 1 |
| Password Required | {Yes, No} | No | Yes* |
| User Can Change Timeout | {Yes, No} | Yes | Yes |
| PIM Synch Policy Group | | | |
| Disable All Wireless Sync | {Yes, No} | No | No |
| Bluetooth Policy Group | | | |
| Disable Bluetooth | {Yes, No} | No | No |
| S/MIME Application Policy Group | | | |
| S/MIME Allowed Content Ciphers | 0-7 | ALL | {0, 1, 2, 5}[12] |
| Browser Policy Group | | | |
| Disable Java Script in Browser | {Yes, No} | No | No |
| WLAN Policy Group | | | |
| Disable WLAN | {Yes, No} | No | No |
| Camera Policy Group | | | |
| Disable Photo Camera | {Yes, No} | No | No |
| Disable Video Camera | {Yes, No} | No | No |
| Password Policy Group | | | |
| Maximum Password History | 0-15 | 0 | 0 |
| Periodic Challenge Time | 1-1440 | Null | Null |
| Set Maximum Password Attempts | 3-10 | 10 | 10 |
| Set Password Timeout | 1-60 | 30 | 30 |
| Suppress Password Echo | {Yes, No} | Yes | Yes |

## 8.2 Baseline Software Configuration

The baseline software configuration is the evaluated configuration of the TOE that provides the most flexibility to tailor the listed software configuration rules to comply with an enterprise security policy. The deployed configuration of the TOE shall be at least as restrictive as the baseline configuration. The following table identifies the valid range of values, default value, and baseline value for each software configuration rule specified in F.SWConfiguration. Modifying the baseline values will result in a more restrictive configuration, and thus may be configured to comply with an enterprise security policy while maintaining an evaluated configuration. The software configuration rules defined in the table below can be applied to listed and unlisted applications.

[11] The allowed range of values for the Password Pattern Checks IT policy rule is 1-3. A value of 0 is not allowed in the evaluated configuration.
[12] The allowed range of values for the S/MIME Allowed Content Ciphers IT policy rule is 0-2, 5. The values of 3, 4, 6 and 7 are not allowed in the evaluated configuration.

**Table 12. Baseline Software Configuration**

| Software Configuration Rule | Value | | |
|---|---|---|---|
| | Range | Default | Baseline |
| Software Configuration | | | |
| Disposition | {Optional, Required, Not Permitted} | Optional | Optional |
| Application Control Policy | | | |
| Interprocess Communication | {Allowed, Not Permitted} | Allowed | Allowed |
| Internal Network Connections | {Prompt User, Allowed, Not Permitted} | Prompt User | Prompt User |
| External Network Connections | {Prompt User, Allowed, Not Permitted} | Prompt User | Prompt User |
| Local Connections | {Allowed, Not Permitted} | Allowed | Allowed |
| Phone Access | {Prompt User, Allowed, Not Permitted} | Prompt User | Prompt User |
| Message Access | {Allowed, Not Permitted} | Allowed | Allowed |
| PIM Data Access | {Allowed, Not Permitted} | Allowed | Allowed |
| Event Injection | {Allowed, Not Permitted} | Not Permitted | Not Permitted |
| Bluetooth Serial Profile | {Allowed, Not Permitted} | Allowed | Allowed |
| BlackBerry Device Keystore | {Allowed, Not Permitted} | Allowed | Allowed |
| BlackBerry Device Keystore Medium Security | {Allowed, Not Permitted} | Allowed | Allowed |
| Device GPS | {Prompt User, Allowed, Not Permitted} | Prompt User | Prompt User |
| User Authenticator API | {Allowed, Not Permitted} | Allowed | Allowed |

# 9 Glossary

| | |
|---|---|
| AES | Advanced Encryption Standard |
| ANSI | American National Standards Institute |
| CBC | Cipher block chaining |
| CDMA | Code division multiple access |
| EAL | Evaluation assurance level |
| ECC | Elliptic curve cryptography |
| ECDH | Elliptic curve Diffie-Hellman |
| ECDSA | Elliptic curve digital signature algorithm |
| ECMQV | Elliptic curve Menezes-Qu-Vanstone |
| EVDO | Evolution data optimised |
| FIPS | Federal Information Processing Standard |
| GPRS | GSM general packet radio service |
| GSM | Global system for mobile communication |
| HMAC | Keyed-hashed message authentication code |
| IT | Information technology |
| MMS | Multimedia Messaging Service |
| PIM | Personal information management |
| PIN | Personal identification number |
| PRNG | Pseudo-random number generator |
| RIM | Research In Motion |
| RNG | Random number generator |
| SAR | Security assurance requirement |
| SFP | Security function policy |
| SFR | Security functional requirement |
| SHA | Secure Hash Algorithm |
| S/MIME | Secure/Multi-purpose Internet Mail Extensions |
| SMS | Short Messaging Service |
| SRP | Service routing protocol |
| TCP | Transmission control protocol |
| TCP/IP | Transmission control protocol/Internet protocol |
| TOE | Target of evaluation |
| Triple DES | Triple Data Encryption Standard |
| TSC | TSF scope of control |
| TSF | TOE security function |
| TSP | TOE security policy |
| URL | Uniform resource locator |

OF CONTRACT, NEGLIGENCE, TORT, STRICT LIABILITY OR ANY OTHER LEGAL THEORY AND SHALL SURVIVE A FUNDAMENTAL BREACH OR BREACHES OR THE FAILURE OF THE ESSENTIAL PURPOSE OF THIS AGREEMENT OR OF ANY REMEDY CONTAINED HEREIN; AND (B) TO RIM AND ITS AFFILIATED COMPANIES, THEIR SUCCESSORS, ASSIGNS, AGENTS, SUPPLIERS (INCLUDING AIRTIME SERVICE PROVIDERS), AUTHORIZED RIM DISTRIBUTORS (ALSO INCLUDING AIRTIME SERVICE PROVIDERS) AND THEIR RESPECTIVE DIRECTORS, EMPLOYEES, AND INDEPENDENT CONTRACTORS.

IN ADDITION TO THE LIMITATIONS AND EXCLUSIONS SET OUT ABOVE, IN NO EVENT SHALL ANY DIRECTOR, EMPLOYEE, AGENT, DISTRIBUTOR, SUPPLIER, INDEPENDENT CONTRACTOR OF RIM OR ANY AFFILIATES OF RIM HAVE ANY LIABILITY ARISING FROM OR RELATED TO THE DOCUMENTATION.

Prior to subscribing for, installing, or using any Third Party Products and Services, it is your responsibility to ensure that your airtime service provider has agreed to support all of their features. Installation or use of Third Party Products and Services with RIM's products and services may require one or more patent, trademark, copyright, or other licenses in order to avoid infringement or violation of third party rights. You are solely responsible for determining whether to use Third Party Products and Services and if any third party licenses are required to do so. If required you are responsible for acquiring them. You should not install or use Third Party Products and Services until all necessary licenses have been acquired. Any Third Party Products and Services that are provided with RIM's products and services are provided as a convenience to you and are provided “AS IS” with no express or implied conditions, endorsements, guarantees, representations, or warranties of any kind by RIM and RIM assumes no liability whatsoever, in relation thereto. Your use of Third Party Products and Services shall be governed by and subject to you agreeing to the terms of separate licenses and other agreements applicable thereto with third parties, except to the extent expressly covered by a license or other agreement with RIM.

The terms of use of any RIM product or service are set out in a separate license or other agreement with RIM applicable thereto. NOTHING IN THIS DOCUMENTATION IS INTENDED TO SUPERSEDE ANY EXPRESS WRITTEN AGREEMENTS OR WARRANTIES PROVIDED BY RIM FOR PORTIONS OF ANY RIM PRODUCT OR SERVICE OTHER THAN THIS DOCUMENTATION.

Research In Motion Limited
295 Phillip Street
Waterloo, ON N2L 3W8
Canada

Research In Motion UK Limited
200 Bath Road
Slough, Berkshire SL1 3XE
United Kingdom

Published in Canada