

# BlackBerry Device Service 6.0 and BlackBerry PlayBook Tablet 2.0

Security Technical Overview

Version: 6.0







# Contents

1	Document revision history.....	7
2	Tablet security features .....	8
3	Architecture: BlackBerry Device Service.....	10
4	How a tablet connects to the BlackBerry Device Service.....	13
	Securing the communication between a tablet and your organization's network.....	14
	How a tablet can connect to the BlackBerry Infrastructure.....	14
	Data flow: Opening a TLS connection between the BlackBerry Infrastructure and a tablet .....	14
	Encrypting data that the BlackBerry Device Service and a tablet send to each other over the BlackBerry Infrastructure.....	15
	Device transport keys .....	15
	Message keys .....	16
	Protecting a connection between a tablet and a work Wi-Fi network .....	17
	How a tablet and BlackBerry Device Service protect sensitive Wi-Fi information.....	17
	Layer 2 security methods that a tablet supports .....	18
	EAP authentication methods that a tablet supports.....	19
	Using a VPN with a tablet .....	20
	Certificates on the BlackBerry Device Service and tablet.....	21
	Using SCEP to enroll certificates to a tablet.....	21
	Managing certificates that a tablet enrolls using SCEP.....	22
5	Activating a tablet.....	23
	Data flow: Activating user accounts using BlackBerry Web Desktop Manager.....	23
6	How a BlackBerry Device Service and the BlackBerry Infrastructure authenticate with each other.....	25
	What happens when a BlackBerry Device Service and the BlackBerry Infrastructure open an initial connection .....	25
	Data flow: Authenticating the BlackBerry Device Service with the BlackBerry Infrastructure.....	25
	How the BlackBerry Device Service protects a TCP/IP connection to the BlackBerry Infrastructure.....	26
7	Using IT policies to manage BlackBerry Device Service security.....	27
	Preconfigured IT policy.....	27
	Resolving IT policy conflicts.....	27
8	Securing tablets in your organization's environment for work use.....	29
	How a tablet distinguishes between work data, BlackBerry Bridge data, and personal data.....	29
	How a tablet protects work data.....	30
	What happens when a user updates or creates files on a tablet.....	31
	How a tablet controls whether an application is a work application, BlackBerry Bridge application, or personal application.....	32
	Determining which applications are work applications, BlackBerry Bridge applications, or personal applications.....	33
	Comparison of work applications, BlackBerry Bridge applications, and personal applications.....	34

	Access rights for work data, BlackBerry Bridge data, and personal data that the BlackBerry Tablet OS grants to applications.....	35
	Managing applications.....	36
	Signing third-party applications .....	37
	When a tablet prevents a user from accessing work data or work applications .....	37
	Using the browser to connect a tablet to web servers that support NTLM.....	37
<b>9</b>	<b>The BlackBerry Tablet OS.....</b>	<b>38</b>
	The tablet file system.....	38
	How the BlackBerry Tablet OS uses sandboxing to protect application data.....	39
	How the BlackBerry Tablet OS manages the resources on a tablet.....	39
	How the tablet manages permissions for applications.....	39
	How a tablet verifies the software that it runs.....	40
	How a tablet verifies the boot ROM code.....	40
	How a tablet verifies the Tablet OS and its filesystem.....	40
	How a tablet verifies applications and software upgrades.....	40
	How a tablet is designed to prevent the exploitation of memory corruption.....	41
	How a tablet minimizes the number of processes running as root.....	42
<b>10</b>	<b>Protecting the data that the BlackBerry Device Service stores in your organization's environment.....</b>	<b>43</b>
	Data that the BlackBerry Configuration Database stores .....	43
	Best practice: Protecting the data that the BlackBerry Configuration Database stores.....	43
<b>11</b>	<b>Configuring single sign-on authentication for the BlackBerry Administration Service and BlackBerry Web Desktop Manager.....</b>	<b>46</b>
	Architecture: BlackBerry Administration Service single sign-on.....	46
	How BlackBerry Administration Service single sign-on uses Kerberos to help protect your organization's resources.....	47
	How the BlackBerry Administration Service completes Kerberos authentication.....	47
	Data flow: Accessing the BlackBerry Administration Service console and BlackBerry Web Desktop Manager when you configure BlackBerry Administration Service single sign-on.....	48
<b>12</b>	<b>How a tablet is designed to prevent BlackBerry Runtime for Android apps from accessing work data or work applications.....</b>	<b>50</b>
	Protecting a tablet from malicious applications that are written for Android.....	50
<b>13</b>	<b>Protecting user information.....</b>	<b>51</b>
	Using the tablet password.....	51
	Deleting all data from a tablet.....	51
	Deleting all data from the work perimeter on a tablet.....	54
	Using IT policy rules to specify when all data must be deleted from a tablet.....	55
	Using IT policy rules to specify when all data on the work perimeter of a tablet must be deleted.....	55
<b>14</b>	<b>Cryptographic algorithms, codes, protocols, and APIs that a tablet supports .....</b>	<b>56</b>
	Symmetric encryption algorithms.....	56
	Asymmetric encryption algorithms.....	57
	Hash algorithms.....	57

	Message authentication codes.....	57
	Signature scheme algorithms.....	58
	Key agreement schemes.....	58
	Cryptographic protocols.....	58
	Cipher suites that a tablet supports for opening TLS connections.....	59
	Cryptographic APIs.....	60
	VPN cryptographic support.....	60
	Wi-Fi cryptographic support.....	60
15	<a href="#">Related resources</a> .....	61
16	<a href="#">Glossary</a> .....	62
17	<a href="#">Legal notice</a> .....	66

# Document revision history

1

Date	Description
21 February 2012	Initial version

# Tablet security features

## 2

Feature	Description
Protection of data between the BlackBerry Device Service and a BlackBerry PlayBook tablet	The BlackBerry Device Service is designed to protect data that is in transit between the BlackBerry Device Service and a tablet. The BlackBerry Device Service and a tablet can communicate using both transport layer encryption (using AES-256) and TLS.
Protection of work data on a tablet	<ul style="list-style-type: none"> <li>• The tablet is designed to isolate the work file system, the personal file system, and the BlackBerry Bridge file system.</li> <li>• The tablet is designed to isolate the work applications, the personal applications, and the BlackBerry Bridge applications.</li> <li>• The tablet helps protect work data using XTS-AES-256 encryption.</li> </ul>
Control of tablet access to your organization's network	The BlackBerry Device Service is designed to allow you to send work Wi-Fi and work VPN profiles to a tablet so that the tablet can connect to your organization's network.
Control of the behavior of a tablet	<p>To control the behavior of a tablet, you can send IT administration commands and IT policies to a tablet so that you can perform the following actions:</p> <ul style="list-style-type: none"> <li>• You can send IT administration commands to lock the tablet, permanently delete work data, permanently delete user information and application data, and return the device settings to the default values.</li> <li>• You can send an IT policy to a tablet to change security settings. You can use the IT policy to enforce the tablet password</li> </ul>
Protection of BlackBerry PlayBook tablet user information	The tablet is designed to allow a user to delete all user information and application data from the tablet memory.
Protection of BlackBerry Tablet OS	<ul style="list-style-type: none"> <li>• When the BlackBerry Tablet OS starts, it completes integrity tests to detect damage to the kernel.</li> </ul>

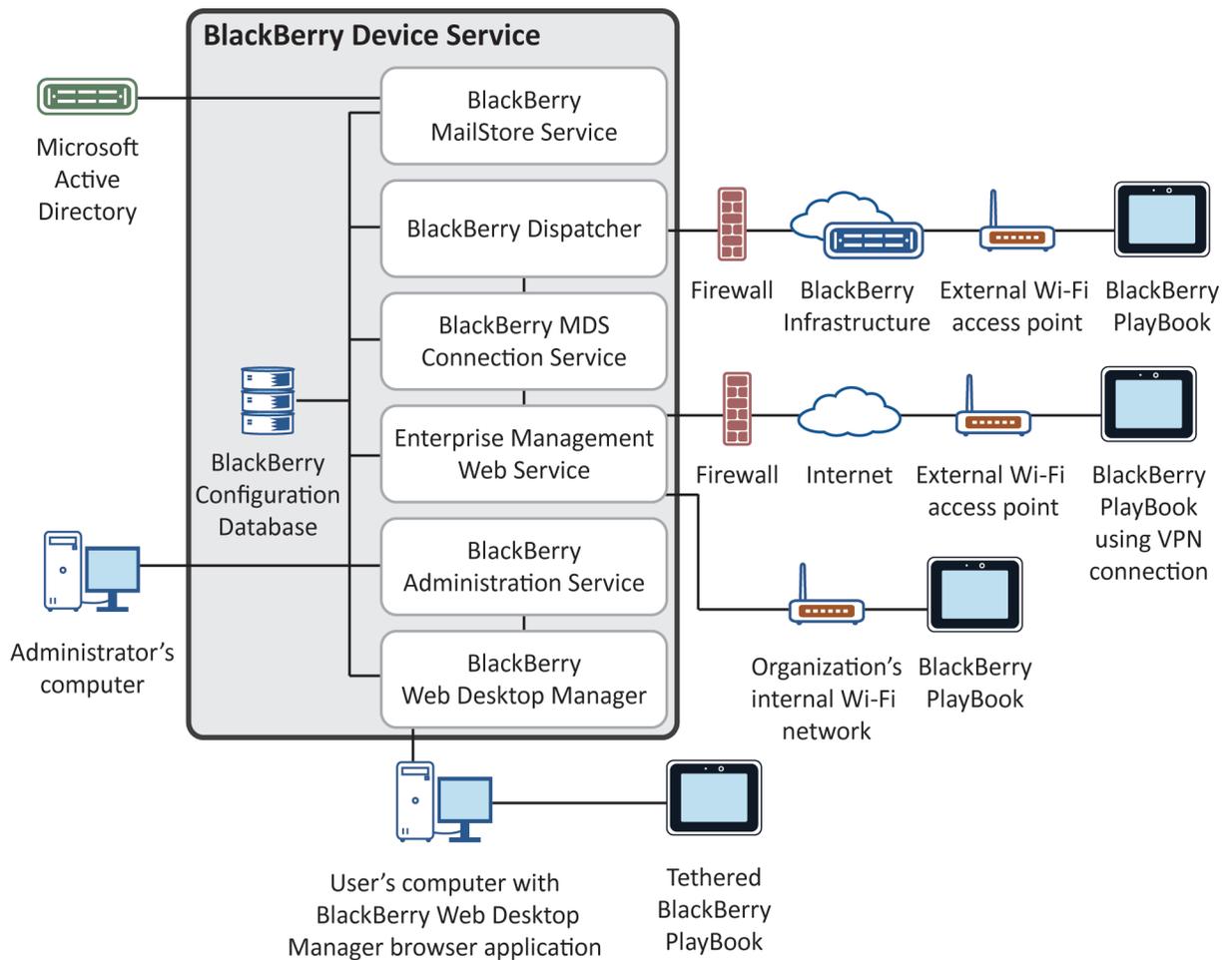
Feature	Description
	<ul style="list-style-type: none"><li>• The BlackBerry Tablet OS can restart a process that stops responding without negatively affecting other processes.</li><li>• The BlackBerry Tablet OS validates requests that applications make for resources on the tablet.</li></ul>
Protection of application data using sandboxing	<p>The BlackBerry Tablet OS uses sandboxing to separate and restrict the capabilities and permissions of applications that run on the tablet. Each application process runs in its own sandbox.</p> <p>The BlackBerry Tablet OS is designed to evaluate the requests that an application's processes make for memory outside of its sandbox.</p>
Protection of resources	<p>The BlackBerry Tablet OS uses adaptive partitioning to allocate resources that are not used by applications during typical operating conditions and to make sure that resources are available to applications during times of peak operating conditions.</p>
Management of permissions to access capabilities	<p>The BlackBerry Tablet OS evaluates every request that an application makes to access a capability on the tablet.</p>
Verification of the boot ROM code	<p>The tablet verifies that the boot ROM code is permitted to run on the tablet.</p>

# Architecture: BlackBerry Device Service

3

The BlackBerry Device Service consists of various components that are designed to help you perform the following actions:

- Install and manage your organization's applications on BlackBerry PlayBook tablets.
- Protect your organization's data and applications on tablets



Component	Description
BlackBerry Administration Service	You can use the BlackBerry Administration Service to manage the BlackBerry Device Service and the user accounts and tablets that are associated with it. You can manage user accounts and assign groups, administrative roles, software configurations, email profiles, and IT policies to user accounts. The BlackBerry Administration Service connects to the BlackBerry Configuration Database.
BlackBerry Configuration Database	The BlackBerry Configuration Database is a relational database that contains user account information and configuration information (such as connection details) that the BlackBerry Device Service components use.
BlackBerry Mail Store Service	The BlackBerry Mail Store Service connects to the Microsoft Active Directory in your organization's environment and retrieves user information that the BlackBerry Administration Service requires to activate user accounts. You can add a user account to the BlackBerry Device Service only if the user account exists in your organization's Microsoft Active Directory.
Enterprise Management Web Service	The Enterprise Management Web Service is a set of web services that communicates commands, configuration information, IT policies, VPN profiles, Wi-Fi profiles, and email profiles between the BlackBerry Administration Service and the Enterprise Management Agent on the tablets.
BlackBerry MDS Connection Service	The BlackBerry MDS Connection Service provides a secure connection between the Enterprise Management Agent on the tablets and the Enterprise Management Web Service in the BlackBerry Device Service. The connection is used when the tablet is not connected to your organization's Wi-Fi network or VPN.
BlackBerry Dispatcher	The BlackBerry Dispatcher maintains a connection with the BlackBerry Infrastructure over the Internet. The BlackBerry Dispatcher is responsible for compressing and encrypting and for decrypting and decompressing data that travels over the Internet to and from the tablets.
BlackBerry Web Desktop Manager	The BlackBerry Web Desktop Manager is a web application that permits users to activate and manage tablets.
Microsoft Active Directory	The BlackBerry Mail Store Service obtains user account information from the Microsoft Active Directory that is required to create user accounts in the BlackBerry Device Service.
organization's Wi-Fi network	After a tablet is activated on the BlackBerry Device Service, communication between the BlackBerry Device Service and the tablet can occur over your organization's Wi-Fi network when the tablet is within a wireless coverage area and enabled for access as may be required by your organization's network security policies.
external Wi-Fi access point	Depending on your organization's network configuration, communication can occur between the BlackBerry Device Service and tablets that are located

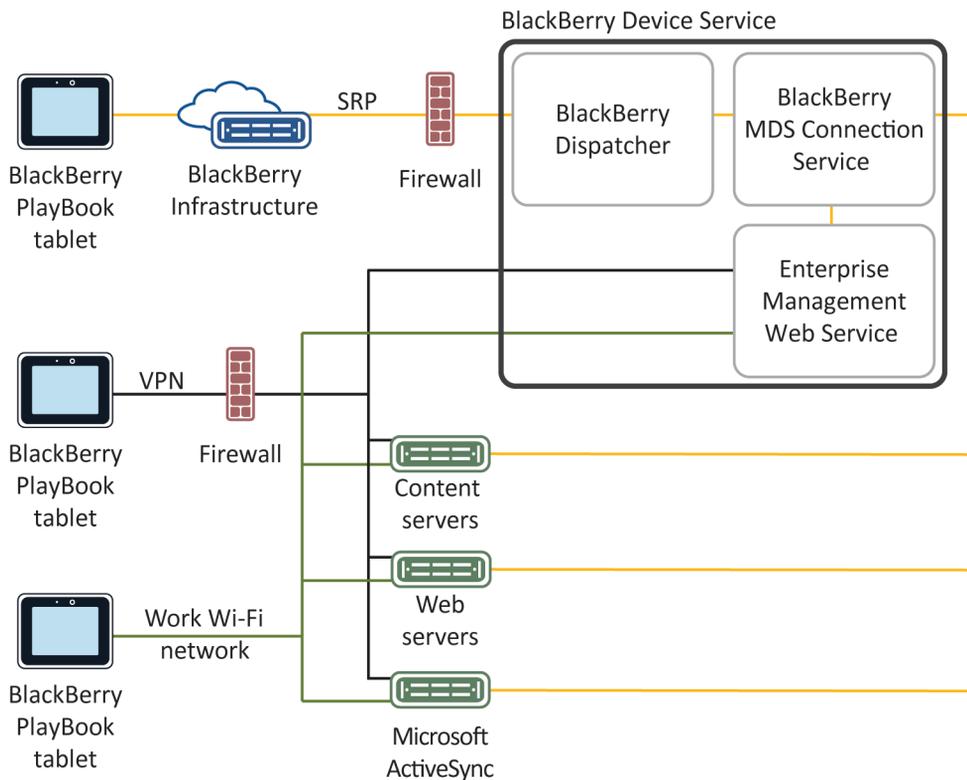
Component	Description
firewall	outside the firewall and connected to the Internet over an external Wi-Fi connection.  The BlackBerry Device Service requires an outbound-initiated, bidirectional connection through port 3101 on the firewall and over the Internet to the BlackBerry Infrastructure to transport data to and from the tablets.
Internet	The Internet transports data between the BlackBerry Infrastructure and the BlackBerry Device Service. Depending on your organization's network configuration, the tablets may also communicate with the BlackBerry Device Service using a VPN connection over the Internet.

# How a tablet connects to the BlackBerry Device Service

## 4

The BlackBerry PlayBook tablet can connect to the BlackBerry Device Service and access your organization's network using a number of communication methods. By default, the tablet attempts to connect to your organization's network using the following communication methods, in order:

1. Work VPN profiles that you configure
2. Work Wi-Fi profiles that you configure
3. BlackBerry Infrastructure
4. Personal VPN profiles and personal Wi-Fi profiles that a user configures on the tablet



By default, the Enterprise Management Agent on the tablet can use all of these communication methods to connect to the BlackBerry Device Service and obtain the latest updates that you made to IT policies, profiles, software configurations, or IT administration commands.

Work applications on the tablet can also use any of these communication methods to access the resources in your organization's environment (for example, Microsoft ActiveSync servers, web servers, and content servers).

## Securing the communication between a tablet and your organization's network

The BlackBerry PlayBook tablet permits work applications and personal applications to use any of the Wi-Fi profiles or VPN profiles that are stored on the tablet to connect to your organization's network. If you configure work Wi-Fi profiles or work VPN profiles using the BlackBerry Device Service, you permit personal applications on the tablet to access your organization's network.

If the security requirements of your organization do not permit personal applications to access your organization's network, you can restrict the communication methods that a tablet can use to connect to your organization's network through the BlackBerry Device Service by limiting enterprise connectivity options to the BlackBerry MDS Connection Service and the BlackBerry Infrastructure.

Personal applications cannot use the BlackBerry MDS Connection Service and the BlackBerry Infrastructure to connect to your organization's network.

## How a tablet can connect to the BlackBerry Infrastructure

The BlackBerry PlayBook tablet and BlackBerry Infrastructure send all data to each other over a TLS connection. The TLS connection is designed to encrypt the data that the tablet and BlackBerry Infrastructure send between each other.

A TLS connection between a tablet and the BlackBerry Infrastructure is designed so that a potentially malicious user cannot use the TLS connection to send data to or receive data from the tablet.

If a potentially malicious user tries to impersonate the BlackBerry Infrastructure, the tablet is designed to prevent the connection. The tablet verifies whether the public key of the TLS certificate of the BlackBerry Infrastructure matches the private key of the root certificate that is preloaded on the tablet during the manufacturing process. If a user accepts a certificate that is not valid, the connection cannot open unless the tablet can also authenticate with a valid BlackBerry Device Service.

## Data flow: Opening a TLS connection between the BlackBerry Infrastructure and a tablet

1. A BlackBerry PlayBook tablet sends a request to the BlackBerry Infrastructure to open a TLS connection.
2. The BlackBerry Infrastructure sends its TLS certificate to the tablet.
3. The tablet uses a root certificate that is preloaded on the tablet to verify the TLS certificate. If the user deleted the root certificate, the tablet prompts the user to trust the TLS certificate.
4. The tablet opens the TLS connection.

## Encrypting data that the BlackBerry Device Service and a tablet send to each other over the BlackBerry Infrastructure

To encrypt data that is in transit between the BlackBerry Device Service and a BlackBerry PlayBook tablet in your organization, the BlackBerry Device Service and tablet use BlackBerry transport layer encryption. BlackBerry transport layer encryption is designed to encrypt data in transit over the BlackBerry Infrastructure.

Before the BlackBerry Device Service and a tablet send data to each other, they compress the data, encrypt the data using message keys, and encrypt the message keys using the device transport key. When the BlackBerry Device Service and tablet receive data from each other, they decrypt the message keys using the device transport key, decrypt the data, and then decompress the data.

The BlackBerry Device Service and tablet use AES-256 in CBC mode as the symmetric algorithm for BlackBerry transport layer encryption.

### Device transport keys

The device transport key encrypts the message keys that help protect the data that is sent between a BlackBerry Device Service and BlackBerry PlayBook tablet. The BlackBerry Device Service and tablet generate the device transport key when a user activates the tablet.

The BlackBerry Device Service and tablet do not send the device transport key over the wireless network when they generate the device transport key or when they exchange messages.

Only the BlackBerry Device Service and tablet are designed to know the value of the device transport key. The BlackBerry Device Service and tablet reject a data packet if they do not recognize the format of a data packet or do not recognize the device transport key that protects the data packet.

A tablet stores the device transport keys in a key store database in flash memory. The key store database is designed to prevent a potentially malicious user from copying the device transport keys to a computer by trying to back up the device transport keys. A potentially malicious user cannot extract key data from flash memory.

The BlackBerry Device Service stores device transport keys in the BlackBerry Configuration Database. To avoid compromising the device transport keys that are stored in the BlackBerry Configuration Database, you must protect the BlackBerry Configuration Database.

### Generating the device transport key for a tablet

When you install the BlackBerry Device Service, the setup application creates an enterprise management root certificate and an authentication certificate for the BlackBerry Device Service. When a user activates a BlackBerry PlayBook tablet, the tablet sends a certificate signing request to the BlackBerry Device Service. The BlackBerry Device Service uses the certificate signing request to create a client certificate, signs the client certificate with the enterprise management root certificate, and sends the client certificate and the authentication certificate for the BlackBerry Device Service to the tablet. To help protect the connection between the tablet and the BlackBerry Device Service during the certificate exchange, the tablet and the BlackBerry Device Service create a short-lived symmetric key using the activation password and EC-SPEKE.

To generate the device transport key, the tablet and the BlackBerry Device Service use the key pairs that are associated with the client certificate, the authentication certificate for the BlackBerry Device Service, and ECMQV. The elliptic curve used in ECMQV is the NIST-recommended 521-bit curve.

## Message keys

A BlackBerry Device Service and BlackBerry PlayBook tablet generate one or more message keys that are designed to protect the integrity of the data (for example, short keys or large messages) that the BlackBerry Device Service and tablet send between each other using the BlackBerry Infrastructure. If a message exceeds 2 KB and consists of several data packets, the BlackBerry Device Service and tablet generate a unique message key for each data packet.

Each message key consists of random data that is designed to make it difficult for a third party to decrypt, re-create, or duplicate the message key.

The BlackBerry Device Service and tablet do not store the message keys in persistent storage. They free the memory that is associated with the message keys after the BlackBerry Device Service or tablet uses the message keys to decrypt the message.

The tablet uses the pseudorandom bits retrieved from the random source on the tablet to generate a message key.

### Data flow: Generating a message key on a tablet

A BlackBerry PlayBook tablet uses the DRBG function to generate a message key.

To generate a message key, the device performs the following actions:

1. Retrieves random data from multiple sources to generate the seed using a technique that the device derives from the initialization function of the ARC4 encryption algorithm
2. Uses the random data to reorder the contents of a 256-byte state array
3. Adds the 256-byte state array into the ARC4 encryption algorithm to further randomize the 256-byte state array
4. Draws 521 bytes from the ARC4 state array

The tablet draws an additional 9 bytes for the 256-byte state array, for a total of 521 bytes ( $512 + 9 = 521$ ) to make sure that the pointers before and after the call are not in the same place, and in case the first few bytes of the ARC4 state array are not random

5. Uses SHA-512 to hash the 521-byte value to 64 bytes
6. Uses the 64-byte value to seed the DRBG function

The tablet stores a copy of the seed in a file. When the tablet restarts, it reads the seed from the file and uses the XOR function to compare the stored seed with the new seed.

7. Uses the DRBG function to generate 256 pseudorandom bits for use with AES encryption
8. Uses the pseudorandom bits to create the message key

For more information about the DRBG function, see *NIST Special Publication 800-90*.

### Data flow: Generating a message key on a BlackBerry Device Service

A BlackBerry Device Service is designed to use the DSA PRNG function to generate a message key.

To generate a message key, the BlackBerry Device Service performs the following actions:

1. Retrieves random data from multiple sources for the seed, using a technique that the BlackBerry Device Service derives from the initialization function of the ARC4 encryption algorithm
2. Uses the random data to reorder the contents of a 256-byte state array  
The BlackBerry Device Service requests 512 bits of randomness from the Microsoft Cryptographic API to increase the randomness of the data.
3. Adds the 256-byte state array into the ARC4 algorithm to further randomize the 256-byte state array
4. Draws 521 bytes from the 256-byte state array  
The BlackBerry Device Service draws an additional 9 bytes for the 256-byte state array, for a total of 521 bits ( $512 + 9 = 521$ ) to make sure that the pointers before and after the generation process are not in the same place, and in case the first few bytes of the 256-byte state array are not random.
5. Uses SHA-512 to hash the 521-byte value to 64 bytes
6. Uses the 64-byte value to seed the DSA PRNG function  
The BlackBerry Device Service stores a copy of the seed in a file. When the BlackBerry Device Service restarts, it reads the seed from the file and uses the XOR function to compare the stored seed with the new seed.
7. Uses the DSA PRNG function to generate 256 pseudorandom bits for use with AES encryption
8. Uses the pseudorandom bits with AES encryption to generate the message key

For more information about the DSA PRNG function, see *Federal Information Processing Standard - FIPS PUB 186-2*.

## Protecting a connection between a tablet and a work Wi-Fi network

A BlackBerry PlayBook tablet is designed to connect to work Wi-Fi networks that use the IEEE® 802.11® standard. The IEEE 802.11i standard uses the IEEE 802.1X standard for authentication and key management to protect work Wi-Fi networks. The IEEE 802.11i standard specifies that organizations must use the PSK protocol or the IEEE 802.1X standard as the access control method for Wi-Fi networks.

For more information about protecting a work Wi-Fi network, see the documentation from your organization's Wi-Fi solution provider.

## How a tablet and BlackBerry Device Service protect sensitive Wi-Fi information

To permit a BlackBerry PlayBook tablet to access a Wi-Fi network, you must send sensitive Wi-Fi information such as encryption keys and passwords to the tablet using Wi-Fi profiles and VPN profiles. After the tablet receives the sensitive Wi-Fi information, the tablet encrypts the encryption keys and passwords and stores them in flash memory.

The BlackBerry Device Service encrypts the sensitive Wi-Fi information that it sends to the tablet and stores the sensitive Wi-Fi information in the BlackBerry Configuration Database. You can help protect the sensitive Wi-Fi information in the BlackBerry Configuration Database using access controls and configuration settings.

## Layer 2 security methods that a tablet supports

You can configure a BlackBerry PlayBook tablet to use security methods for layer 2 (also known as the IEEE 802.11 link layer) so that the wireless access point can authenticate the tablet and the tablet and the wireless access point can encrypt data that they send to each other. The tablet supports the following layer 2 security methods:

- WEP encryption (64-bit and 128-bit)
- IEEE 802.1X standard and EAP authentication using EAP-FAST, EAP-TLS, EAP-TTLS, and PEAP
- TKIP and AES-CCMP encryption for WPA™-Personal, WPA2-Personal, WPA-Enterprise, and WPA2-Enterprise

To support layer 2 security methods, the tablet has a built-in IEEE 802.1X supplicant.

If a work Wi-Fi network uses EAP authentication, you can permit and deny tablet access to the work Wi-Fi network by updating your organization's central authentication server. You are not required to update the configuration of each access point.

For more information about IEEE 802.11 and IEEE 802.1X, see [www.ieee.org/portal/site](http://www.ieee.org/portal/site). For more information about EAP authentication, see RFC 3748.

### IEEE 802.1X standard

The IEEE 802.1X standard defines a generic authentication framework that a Wi-Fi enabled BlackBerry PlayBook tablet and a work Wi-Fi network can use for authentication. The EAP framework is specified in RFC 3748.

The tablet supports EAP authentication methods that meet the requirements of RFC 4017 to authenticate the tablet to the work Wi-Fi network. Some EAP authentication methods (for example, EAP-TLS, EAP-TTLS, EAP-FAST, or PEAP) use credentials to provide mutual authentication between the tablet and the work Wi-Fi network.

The tablet is compatible with the WPA-Enterprise and WPA2-Enterprise specifications.

### Data flow: Authenticating a tablet with a work Wi-Fi network using the IEEE 802.1X standard

If you configured a wireless access point to use the IEEE 802.1X standard, the access point permits communication using EAP authentication only. This data flow assumes that you configured a BlackBerry PlayBook tablet to use an EAP authentication method to communicate with the access point.

1. The tablet associates itself with the access point that you configured to use the IEEE 802.1X standard. The tablet sends its credentials (typically a user name and password) to the access point.
2. The access point sends the credentials to the authentication server.
3. The authentication server performs the following actions:
  - a Authenticates the tablet on behalf of the access point
  - b Instructs the access point to permit access to the work Wi-Fi network
  - c Sends Wi-Fi credentials to the tablet to permit it to authenticate with the access point
4. The access point and tablet use EAPoL-Key messages to generate encryption keys (for example, WEP, TKIP, or AES-CCMP, depending on the EAP authentication method that the tablet uses).

When the tablet sends EAPoL messages, the tablet uses the encryption and integrity requirements that the EAP authentication method specifies. When the tablet sends EAPoL-Key messages, the tablet uses the ARC4 algorithm or AES algorithm to provide integrity and encryption.

After the access point and tablet generate the encryption key, the tablet can access the work Wi-Fi network.

## EAP authentication methods that a tablet supports

### PEAP authentication

PEAP authentication permits a BlackBerry PlayBook tablet to authenticate with an authentication server and access a work Wi-Fi network. PEAP authentication uses TLS to create an encrypted tunnel between the tablet and the authentication server. It uses the TLS tunnel to send the authentication credentials of the tablet to the authentication server.

The tablet supports PEAPv0 and PEAPv1 for PEAP authentication. The tablet also supports EAP-MS-CHAPv2 and EAP-GTC as second-phase protocols during PEAP authentication so that the tablet can exchange credentials with the work Wi-Fi network.

To configure PEAP authentication, you must install a root certificate on the tablet that corresponds to the authentication server certificate and install client certificates, if required. You can send root certificates to every tablet and you can use SCEP to enroll client certificates on tablets.

For more information, see the *BlackBerry Device Service Administration Guide*.

### EAP-TLS authentication

EAP-TLS authentication uses a PKI to permit a BlackBerry PlayBook tablet to authenticate with an authentication server and access a work Wi-Fi network. EAP-TLS authentication uses TLS to create an encrypted tunnel between the tablet and the authentication server. EAP-TLS authentication uses the TLS encrypted tunnel and a client certificate to send the credentials of the tablet to the authentication server.

The tablet supports EAP-TLS authentication when the authentication server and the client use certificates that meet specific requirements. To configure EAP-TLS authentication, you must install a client certificate and a root certificate on the tablet that corresponds to the certificate of the authentication server. You can use SCEP to enroll certificates on a tablet. For more information, see the *BlackBerry Device Service Administration Guide*.

For more information about EAP-TLS authentication, see RFC 2716.

### EAP-TTLS authentication

EAP-TTLS authentication extends EAP-TLS authentication to permit a BlackBerry PlayBook tablet and an authentication server to mutually authenticate. When the authentication server uses its certificate to authenticate with the tablet and open a protected connection to the tablet, the authentication server uses an authentication protocol over the protected connection to authenticate with the tablet.

The tablet supports EAP-MS-CHAPv2 and MS-CHAPv2 as second-phase protocols during EAP-TTLS authentication so that the tablet can exchange credentials with the work Wi-Fi network.

To configure EAP-TTLS authentication, you must install the root certificate on the tablet that corresponds to the certificate of the authentication server. For more information, see the *BlackBerry Device Service Administration Guide*.

## EAP-FAST authentication

EAP-FAST authentication uses PAC to open a TLS connection to a BlackBerry PlayBook tablet and verify the supplicant credentials of the tablet over the TLS connection.

The tablet supports EAP-MS-CHAPv2 and EAP-GTC as second-phase protocols during EAP-FAST authentication so that the tablet can exchange authentication credentials with a work Wi-Fi network. The tablet supports the use of automatic PAC provisioning with EAP-FAST authentication only.

For more information about EAP-FAST authentication, see RFC 4851.

## EAP authentication methods that a tablet supports the use of CCKM with

A BlackBerry PlayBook tablet supports the use of CCKM with all supported EAP authentication methods to improve roaming between wireless access points. The tablet does not support the use of CCKM with the Cisco CKIP encryption algorithm or the AES-CCMP encryption algorithm.

## Using certificates with PEAP authentication, EAP-TLS authentication, or EAP-TTLS authentication

If your organization uses PEAP authentication, EAP-TLS authentication, or EAP-TTLS authentication to protect the wireless access points for a work Wi-Fi network, a BlackBerry PlayBook tablet must authenticate mutually with an access point using an authentication server. To generate the certificates that the tablet and authentication server use to authenticate with each other, you require a certification authority.

For PEAP authentication, EAP-TLS authentication, or EAP-TTLS authentication to be successful, the tablet must trust the certificate of the authentication server. The tablet does not trust the certificate of the authentication server automatically. Before you can configure the tablet to trust the certificate of the authentication server, the following conditions must exist:

- A certification authority that the tablet and authentication server mutually trust must generate the certificate of the authentication server and a certificate for the tablet.
- The tablet must store the root certificates in the certificate chain for the certificate of the authentication server.

Each tablet stores a list of root certificates that are issued by certification authorities that it explicitly trusts.

You can send root certificates to every tablet and you can use SCEP to enroll client certificates on tablets. For more information, see the *BlackBerry Device Service Administration Guide*.

## Using a VPN with a tablet

If your organization's environment includes VPNs, such as IPsec VPNs or SSL VPNs, you can configure a BlackBerry PlayBook tablet to authenticate with the VPN so that it can access your organization's network. A VPN provides an encrypted tunnel between a tablet and your organization's network.

A VPN solution consists of a VPN client on the tablet and a VPN concentrator. The tablet can use the VPN client to authenticate with a VPN concentrator, which acts as the gateway to your organization's network. Each tablet includes a built-in VPN client that supports several VPN concentrators. The VPN client on the tablet is designed to use strong encryption to authenticate itself with the VPN concentrator. It creates an encrypted tunnel between the tablet and VPN concentrator that the tablet and your organization's network can use to communicate.

For more information about configuring VPN profiles, see the *BlackBerry Device Service Administration Guide*.

## Certificates on the BlackBerry Device Service and tablet

When you install the BlackBerry Device Service, the BlackBerry Device Service setup application creates an enterprise management root certificate. The BlackBerry Device Service uses the enterprise management root certificate for the following purposes:

- To sign an authentication certificate for the Enterprise Management Web Service component
- To sign client certificates for BlackBerry PlayBook tablets
- To set up a TLS connection between the BlackBerry Device Service and a tablet so that the BlackBerry Device Service can activate the tablet and send management commands to it

The BlackBerry Device Service setup application creates the authentication certificate during the installation process.

When a user activates a tablet, the tablet generates a key pair and sends the public key to the BlackBerry Device Service in a certificate signing request. The BlackBerry Device Service creates a client certificate and sends the enterprise management root certificate, authentication certificate, and client certificate to the tablet. The BlackBerry Device Service and tablet automatically renew the client certificate when it expires after one year.

The tablet uses the enterprise management root certificate to verify the authentication certificate for the Enterprise Management Web Service. The BlackBerry Device Service and the tablet use the client certificate to authenticate the user, perimeter, and tablet.

## Using SCEP to enroll certificates to a tablet

You might need to distribute client certificates to BlackBerry PlayBook tablets so that they can connect to a work Wi-Fi network or work VPN network. Client certificates are required if the tablet must present certificates to connect to a network or server in your organization's environment (for example, if the work Wi-Fi network uses EAP-TLS authentication).

You can use SCEP to enroll certificates to a tablet during the activation process and when certificates need to be renewed. SCEP is an IETF protocol that is designed to simplify the process of enrolling certificates to a large number of users. A tablet can use SCEP to connect to the certification authority in your organization and obtain any required client certificates. When the certification authority sends client certificates to the tablet, it includes the complete certificate chain, including intermediate and root certificates.

Certificate enrollment using SCEP starts after the tablet receives the certification authority profile that you configured using the BlackBerry Device Service. The tablet can download certification authority profiles during the activation process, when you change a certification authority profile, or when you assign another certification authority profile to a user account.

After the certificate enrollment completes, the client certificate and its certificate chain and private key are stored in the work key store on the tablet.

The tablet can connect to any SCEP compliant certification authority, such as Microsoft certification authority, using SCEP. You must configure the certification authorities to support global challenge passwords.

For more information about SCEP, visit [www.ietf.org](http://www.ietf.org).

## Managing certificates that a tablet enrolls using SCEP

After a BlackBerry PlayBook tablet enrolls a certificate, the SCEP component monitors the expiry date and revocation status of any certificate that was obtained using SCEP. When the expiry date of a certificate approaches, the SCEP component starts the certificate enrollment process for a new certificate. You can use the Automatic Renewal IT policy rule to configure how many days before the certificate expires that automatic renewal occurs.

The certificate enrollment process can also start again if you change the following IT policy rules and resend the IT policy:

- Certification Authority Identifier
- Certificate Thumbprint
- ECC Strength
- Key Algorithm
- RSA Strength

A certificate enrollment process does not delete the existing certificate from the tablet or notify the certification authority that the certificate is no longer in use. If a certification authority profile is removed from the BlackBerry Device Service, the corresponding certificate is not removed from the tablet.

# Activating a tablet

## 5

## Data flow: Activating user accounts using BlackBerry Web Desktop Manager

When you activate user accounts, you associate the work perimeter on BlackBerry PlayBook tablets with user accounts in the BlackBerry Device Service and establish a secure communication channel between the tablets and the BlackBerry Device Service so that BlackBerry PlayBook tablet users can access your organization's resources.

1. An administrator adds a user account to the BlackBerry Administration Service from the account information in the organization's Microsoft Active Directory.
2. A user performs the following actions:
  - a Connects a tablet to a computer using a USB cable.
  - b Browses to BlackBerry Web Desktop Manager using Windows Internet Explorer and logs in.
3. If necessary, the browser downloads and installs the BlackBerry Device Communication Components. The BlackBerry Device Communication Components are Microsoft ActiveX controls that permit the BlackBerry Administration Service to communicate with a tethered tablet.
4. The BlackBerry Device Communication Components send the tablet PIN to the BlackBerry Administration Service over an HTTPS connection to start the activation process.
5. The BlackBerry Administration Service receives the tablet PIN and performs the following actions:
  - a Stores the tablet PIN in the BlackBerry Configuration Database.
  - b Generates an activation password. The administrator and user cannot view the activation password.
  - c Sends the activation password, user ID, and the server name and port of the Enterprise Management Web Service to the Enterprise Management Agent.
6. The Enterprise Management Agent creates the work perimeter.
7. The Enterprise Management Agent and Enterprise Management Web Service generate a shared symmetric key using the activation password and EC-SPEKE. The shared symmetric key is designed to help protect the CSR and response.
8. The Enterprise Management Agent performs the following actions:
  - a Generates a key pair for the certificate.
  - b Creates a PKCS#10 CSR that includes the public key of the key pair.
  - c Sends the CSR to the Enterprise Management Web Service.
9. The Enterprise Management Web Service performs the following actions:

- a Retrieves the user ID, work perimeter ID, tablet PIN, and your organization's name from the BlackBerry Configuration Database.
  - b Packages a client certificate using the information it retrieved and the CSR that the Enterprise Management Agent sent.
  - c Signs the client certificate using the enterprise management root certificate.
  - d Sends the client certificate, enterprise management root certificate, and the Enterprise Management Web Service URL to the Enterprise Management Agent.
10. The Enterprise Management Agent stores the client certificate, enterprise management root certificate, and the authentication certificate for the Enterprise Management Web Service in its key store.
  11. The Enterprise Management Agent and Enterprise Management Web Service generate the device transport key using ECMQV and the long-term public keys in the client certificate and the authentication certificate for the Enterprise Management Web Service.
  12. The Enterprise Management Agent stores the device transport key in its key store.
  13. The Enterprise Management Web Service performs the following actions:
    - a Stores the device transport key in the BlackBerry Configuration Database.
    - b Sends the IT policy, SRP information, profiles, and software configurations to the tablet over TLS.
  14. The Enterprise Management Agent sends an acknowledgment that it received the IT policy and other data to the Enterprise Management Web Service over TLS. The activation process is complete.

The elliptic curve protocols used during activation use the NIST-recommended 521-bit curve.

# How a BlackBerry Device Service and the BlackBerry Infrastructure authenticate with each other

6

The BlackBerry Infrastructure and BlackBerry Device Service must authenticate with each other before they can transfer data. The BlackBerry Device Service uses SRP to authenticate with and connect to the BlackBerry Infrastructure.

SRP is a point-to-point protocol that runs over TCP/IP. The BlackBerry Device Service uses SRP to contact the BlackBerry Infrastructure and open a connection. When the BlackBerry Device Service and BlackBerry Infrastructure open a connection, they can perform the following actions:

1. Authenticate with each other
2. Exchange configuration information
3. Send and receive data

The BlackBerry Device Service and BlackBerry Infrastructure use the SRP authentication key when they authenticate with each other. The SRP authentication key is a 20-byte encryption key that the BlackBerry Device Service and BlackBerry Infrastructure share.

## What happens when a BlackBerry Device Service and the BlackBerry Infrastructure open an initial connection

After a BlackBerry Device Service and the BlackBerry Infrastructure open an initial connection over the Internet, the BlackBerry Device Service is designed to send a basic information packet to the BlackBerry Infrastructure immediately. A basic information packet includes the BlackBerry Device Service version information, SRP identifiers, and other information that is required to open an SRP connection. Both the BlackBerry Device Service and BlackBerry Infrastructure can recognize the basic information packet. The BlackBerry Device Service and BlackBerry Infrastructure can use the basic information packet to configure the parameters of the SRP implementation.

## Data flow: Authenticating the BlackBerry Device Service with the BlackBerry Infrastructure

1. The BlackBerry Device Service sends a data packet that contains its unique SRP identifier to the BlackBerry Infrastructure to claim the SRP identifier.
2. The BlackBerry Infrastructure sends a random challenge string to the BlackBerry Device Service.
3. The BlackBerry Device Service sends a challenge string to the BlackBerry Infrastructure.

4. The BlackBerry Infrastructure hashes the challenge string it received from the BlackBerry Device Service with the SRP authentication key using HMAC with the SHA-1 algorithm. The BlackBerry Infrastructure sends the resulting 20-byte value to the BlackBerry Device Service as a challenge response.
5. The BlackBerry Device Service hashes the challenge string it received from the BlackBerry Infrastructure with the SRP authentication key, and sends the result as a challenge response to the BlackBerry Infrastructure.
6. The BlackBerry Infrastructure performs one of the following actions:
  - Accepts the challenge response and sends a confirmation to the BlackBerry Device Service to complete the authentication process and configure an authenticated SRP connection
  - Rejects the challenge response

If the BlackBerry Infrastructure rejects the challenge response, the authentication process is not successful. The BlackBerry Infrastructure and BlackBerry Device Service close the SRP connection.

If a BlackBerry Device Service uses the same SRP authentication key and SRP identifier to connect to (and then disconnect from) the BlackBerry Infrastructure five times in one minute, the BlackBerry Infrastructure deactivates the SRP identifier to help prevent a potentially malicious user from using the SRP identifier to create conditions for a DoS attack.

## How the BlackBerry Device Service protects a TCP/IP connection to the BlackBerry Infrastructure

After a BlackBerry Device Service and the BlackBerry Infrastructure open an SRP connection, the BlackBerry Device Service uses a persistent TCP/IP connection to send data to the BlackBerry Infrastructure.

The TCP/IP connection between the BlackBerry Device Service and BlackBerry Infrastructure is designed to be highly secure because the BlackBerry Device Service and BlackBerry PlayBook tablet encrypt the data that they send to each other. No intermediate point decrypts and encrypts the data again.

No data traffic of any kind can occur between the BlackBerry Device Service and the tablet unless the BlackBerry Device Service can decrypt the data using a valid device transport key. Only the BlackBerry Device Service and tablet have the correct device transport key.

You must configure your organization's firewall or proxy server to permit the BlackBerry Device Service to start and maintain an outgoing connection to the BlackBerry Infrastructure over TCP port 3101.

# Using IT policies to manage BlackBerry Device Service security

## 7

You can use IT policies to control and manage BlackBerry devices in your organization's environment. An IT policy consists of multiple IT policy rules that manage the security and behavior of the BlackBerry Enterprise Solution. For example, you can use IT policy rules to manage the following security features and behaviors of the device:

- Encryption
- Use of a password or pass phrase
- Connections that use Bluetooth wireless technology

The Default IT policy includes IT policy rules that are configured to indicate the default behavior of the device.

After a device user activates a device, the BlackBerry Device Service automatically sends to the device the IT policy that you assigned to the user account or group. By default, if you do not assign an IT policy to the user account or group, the BlackBerry Device Service sends the Default IT policy. If you delete an IT policy that you assigned to the user account or group, the BlackBerry Device Service automatically re-assigns the Default IT policy to the user account and resends the Default IT policy to the device.

For more information, see the *BlackBerry Device Service Policy Reference Guide*.

## Preconfigured IT policy

The BlackBerry Device Service includes the following preconfigured IT policy. You can change the preconfigured IT policy to meet the requirements of your organization or copy this IT policy to create new IT policies.

Preconfigured IT policy	Description
Default	This policy includes all the standard IT policy rules that are set on the BlackBerry Device Service.

## Resolving IT policy conflicts

If you add a user account to multiple groups, multiple IT policies can be added to the user account. You can control how the BlackBerry Device Service applies the correct IT policies and IT policy rules to the user account.

The BlackBerry Device Service applies the IT policy that you assign directly to the user account first.

If you do not assign an IT policy directly to the user account, the BlackBerry Device Service applies the IT policies that you assign to the group using one of the following methods:

Method	Description
Apply one IT policy to the user account	You can configure the BlackBerry Device Service to apply only one IT policy to a user account. If you select this method to resolve IT policy conflicts, the BlackBerry Device Service applies the IT policy with the highest ranking in the BlackBerry Administration Service.
Apply multiple IT policies to a user account	You can configure the BlackBerry Device Service to apply multiple IT policies to a user account. If you select this method to resolve IT policy conflicts, the BlackBerry Device Service combines the IT policies into one IT policy and applies it to the user account.  A conflict occurs when you change an IT policy rule from the default value to different values in different IT policies. If there is a conflict between IT policy rules in different IT policies, the BlackBerry Device Service uses the IT policy rule from the IT policy with the highest ranking in the BlackBerry Administration Service.

# Securing tablets in your organization's environment for work use

## 8

The BlackBerry Device Service permits you to manage the work file system on BlackBerry PlayBook tablets that run BlackBerry Tablet OS 2.0 or later. Security features on tablets can control how the tablet helps protect your organization's data and applications.

The BlackBerry Device Service security features allow you to:

- Control the connections that tablets make to your organization's environment, including connections to your work Wi-Fi networks and Microsoft ActiveSync
- Install and manage your organization's applications on tablets
- Protect your organization's data and applications on tablets

## How a tablet distinguishes between work data, BlackBerry Bridge data, and personal data

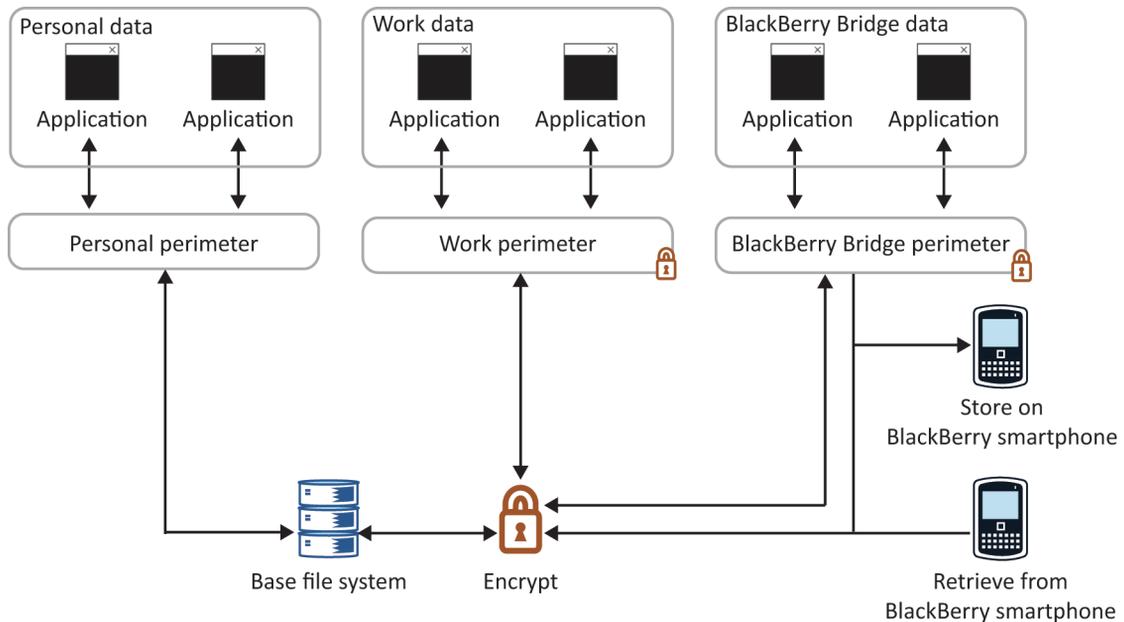
Work data consists of IT policies, profiles, and software configurations that the BlackBerry Device Service and a BlackBerry PlayBook tablet send to each other, data (such as email messages, calendar entries, and attachments) that the tablet receives from your organization's network using the connection with the BlackBerry Device Service, and any data that is associated with BlackBerry Bridge applications (for example, metadata).

To help protect work data, the tablet automatically creates a work perimeter in the BlackBerry Tablet OS during the activation process that isolates work data and work applications from personal data and personal applications and, if the tablet is connected to a BlackBerry smartphone using the BlackBerry Bridge app, from BlackBerry Bridge data and BlackBerry Bridge applications. The tablet encrypts the work file system using XTS-AES-256 encryption.

To help protect BlackBerry Bridge data when a tablet is connected to a smartphone, the tablet automatically creates a BlackBerry Bridge perimeter in the BlackBerry Tablet OS that isolates BlackBerry Bridge data and BlackBerry Bridge applications from personal data and personal applications and, if the tablet is activated on the BlackBerry Device Service, from work data and work applications. The tablet encrypts the BlackBerry Bridge file system using XTS-AES-256 encryption.

If a tablet is both activated on a BlackBerry Device Service in your organization's network and connected to a smartphone that is activated on a BlackBerry Enterprise Server in your organization's network, the BlackBerry Bridge applications have read-write access to shared documents in the work perimeter and work applications have read-write access to shared documents on the media card that is inserted in the smartphone.

The tablet does not encrypt the personal perimeter.



## How a tablet protects work data

The BlackBerry PlayBook tablet is designed to encrypt data stored on the work file system using XTS-AES-256.

The tablet uses a randomly generated 512-bit file encryption key to encrypt the contents of a file. The file encryption process creates a security record for the encrypted file that consists of a 512-bit random salt, the file encryption key, and several attributes of the file. The tablet encrypts the file security record using the domain key, which is a 512-bit randomly generated key.

The tablet uses the domain key to encrypt all file security records in the work file system. The domain key is stored in a security record that is similar to the file security record. The domain security record is encrypted using the work perimeter key. The work perimeter key is stored in RAM and is not written to persistent storage on the tablet.

The tablet system key and the domain key are stored in NVRAM on the tablet and are encrypted with a key that is stored in the replay protected memory block in flash memory. The replay protected memory block is encrypted with a key that is embedded in the processor when the processor is manufactured.

The tablet does not encrypt the user's personal data.

### Data flow: Generating a work perimeter key when the “Two-factor Encryption Key Generation” IT policy rule is set to Enable

If you set the "Two-factor Encryption Key Generation" IT policy rule to Enable, the BlackBerry PlayBook tablet bases the encryption key on both the protected secret and the password for the work perimeter. For more information about IT policies, see the *BlackBerry Device Service Policy Reference Guide*.

1. The user types the password for the work perimeter to unlock the work perimeter.

## 2. The tablet performs the following actions:

- a Uses the password, a 128-bit random salt, and 20,000 iterations of the SHA-512 hash function to derive an intermediate key.
- b Uses SHA-512 to hash the intermediate key and the tablet system key to produce the work perimeter key.  
The tablet system key is created during the manufacturing process and is the SHA-512 hash of a hardware ID and a 512-bit random key.
- c Overwrites and then frees the memory that stored the password, the intermediate key, and the work perimeter key when it is finished using them.

## Data flow: Generating a work perimeter key when the “Two-factor Encryption Key Generation” IT policy rule is set to Disable

If you set the "Two-factor Encryption Key Generation" IT policy rule to Disable, the BlackBerry PlayBook tablet bases the encryption key on the protected secret only. For more information about IT policies, see the *BlackBerry Device Service Policy Reference Guide*.

To generate a work perimeter key, the tablet performs the following actions:

1. Retrieves the domain key from the NV store on the tablet.
2. Uses the domain key, a 128-bit random salt, and 20,000 iterations of the SHA-512 hash function to derive an intermediate key.
3. Uses SHA-512 to hash the intermediate key and the tablet system key to produce the work perimeter key.  
The tablet system key is created during the manufacturing process and is the SHA-512 hash of a hardware ID and a 512-bit random key.
4. Overwrites and then frees the memory that stored the domain key, the intermediate key, and the work perimeter key when it is finished using them.

## What happens when a user updates or creates files on a tablet

The BlackBerry PlayBook tablet helps protect data when a user performs the following actions:

Action	Description
Open a file to view or update it	When the user opens a file that belongs to one perimeter (either the work perimeter, BlackBerry Bridge perimeter, or personal perimeter), the tablet starts the application in the perimeter mode that the file belongs to. For example, if the user opens a work email message, the tablet starts the email application in work mode.
Copy and paste data to a file	The tablet does not permit the user to move data from either the work perimeter or the BlackBerry Bridge perimeter to the personal perimeter. For example, the user cannot cut, copy, or paste data from a work file to a personal file.

Action	Description
	<p>The tablet does permit a user to move data from the personal perimeter to the work perimeter or the BlackBerry Bridge perimeter. For example, the user can cut, copy, or paste personal data into a work file. The user can also attach a personal file to a work email message or work calendar entry.</p> <p>If a tablet is both activated on a BlackBerry Device Service in your organization's network and connected to a BlackBerry smartphone that is activated on a BlackBerry Enterprise Server in your organization's network, the BlackBerry Bridge applications have read-write access to shared documents in the work perimeter and work applications have read-write access to shared documents on the media card that is inserted in the BlackBerry smartphone.</p>

## How a tablet controls whether an application is a work application, BlackBerry Bridge application, or personal application

Applications on a BlackBerry PlayBook tablet can run in work mode, personal mode and, if the tablet is connected to a BlackBerry smartphone using the BlackBerry Bridge app, BlackBerry Bridge mode. By default, all applications on the tablet run in personal mode.

After a user connects a tablet to a smartphone that is activated on a BlackBerry Enterprise Server, an application can run in BlackBerry Bridge mode.

When you use the BlackBerry Device Service to install and manage applications on tablets, the applications are considered work applications. The tablet automatically installs required applications in the work perimeter after the tablet downloads them. A user can download and install optional applications from the Work tab in the BlackBerry App World storefront; these applications are installed in the work perimeter on tablets. Work applications can only access work data and interact with other work applications that are also located in the work perimeter.

If a tablet is both activated on a BlackBerry Device Service in your organization's network and connected to a smartphone that is activated on a BlackBerry Enterprise Server in your organization's network, the BlackBerry Bridge applications have read-write access to shared documents in the work perimeter and work applications have read-write access to shared documents on the media card that is inserted in the smartphone. The work applications have read-only access to the personal applications and personal data that are located in the personal perimeter.

Some applications, such as Documents To Go, can run in work mode, BlackBerry Bridge mode, or personal mode. If the user opens an attachment in a work email message or work calendar entry, Documents To Go runs in work mode. If the user opens an attachment in a BlackBerry Bridge email message or BlackBerry Bridge calendar entry, Documents To Go runs in BlackBerry Bridge mode. If the user opens an attachment in a personal email message or personal calendar entry, Documents To Go runs in personal mode.

## Determining which applications are work applications, BlackBerry Bridge applications, or personal applications

The following table lists the applications that the BlackBerry PlayBook tablet permits to run in work mode, BlackBerry Bridge mode, or personal mode.

Application	Work mode	BlackBerry Bridge mode	Personal mode
Applications that a user downloads and installs on the tablet			√
Applications that a user downloads from the Work tab in the BlackBerry App World storefront (the applications that you specified as optional)	√		
Applications that are sent to the tablet using software configurations in the BlackBerry Device Service	√		
Bridge Browser		√	
Browser	√	√	√
Calendar application	√		√
Calendar application in the BlackBerry Bridge folder		√	
Contacts application	√		√
Contacts application in the BlackBerry Bridge folder		√	
Document viewers (for example, Documents To Go and Adobe Reader)	√	√	√
File Manager application	√	√	√
MemoPad application in the BlackBerry Bridge folder		√	
Messages application	√		√

Application	Work mode	BlackBerry Bridge mode	Personal mode
Messages application in the BlackBerry Bridge folder		√	
Music application	√	√	√
Pictures application	√	√	√
Print To Go application	√		√
Tasks application in the BlackBerry Bridge folder		√	
Videos application	√	√	√
Work Browser	√		

## Comparison of work applications, BlackBerry Bridge applications, and personal applications

Work applications	BlackBerry Bridge applications	Personal applications
Work applications can access work data.	BlackBerry Bridge applications can access BlackBerry Bridge data; they can view but not change personal data.	Personal applications cannot access work data or BlackBerry Bridge data but they can access personal data.
Work applications can view but not change personal data.		
Work applications can access shared documents on the media card that is inserted in the BlackBerry smartphone if the BlackBerry PlayBook tablet is both activated on a BlackBerry Device Service in your organization's network and connected to a smartphone that is activated on a BlackBerry Enterprise Server in your organization's network.	BlackBerry Bridge applications can access shared documents in the work perimeter if the tablet is both activated on a BlackBerry Device Service in your organization's network and connected to a smartphone that is activated on a BlackBerry Enterprise Server in your organization's network.	
Work applications can attach personal files to work email messages or work calendar entries (for example, a tablet user can attach a picture that the user took using the tablet camera to a work email message).	BlackBerry Bridge applications can attach personal files to BlackBerry Bridge email messages or BlackBerry Bridge calendar entries.	Personal applications cannot attach work files or BlackBerry Bridge files to personal email messages or personal calendar entries.

Work applications	BlackBerry Bridge applications	Personal applications
A user can access work applications when you activate a tablet on the BlackBerry Device Service.	A user can access BlackBerry Bridge applications only when the tablet is connected to a BlackBerry smartphone and the smartphone allows it (for example, if a user opens a .pdf file attachment in a BlackBerry Bridge email message, the Adobe Reader application can open the file).	A user can access personal applications regardless of whether you are using the BlackBerry Device Service to manage work applications on the tablet or whether the tablet is connected to the smartphone.
The tablet upgrades work applications when the BlackBerry Tablet OS is upgraded.	The tablet upgrades BlackBerry Bridge applications when the BlackBerry Tablet OS is upgraded.	The tablet upgrades preinstalled personal applications when the BlackBerry Tablet OS is upgraded. The user can upgrade the personal applications that the user installs at any time.

## Access rights for work data, BlackBerry Bridge data, and personal data that the BlackBerry Tablet OS grants to applications

The following table displays the access rights that applications have to work data, BlackBerry Bridge data, or personal data.

If a BlackBerry PlayBook tablet is both activated on a BlackBerry Device Service in your organization's network and connected to a BlackBerry smartphone that is activated on a BlackBerry Enterprise Server in your organization's network, the BlackBerry Bridge applications have read-write access to shared documents in the work perimeter and work applications have read-write access to shared documents on the media card that is inserted in the BlackBerry smartphone. The work applications have read-only access to the personal applications and personal data that are located in the personal perimeter.

Access right	Work application A	Work application B	BlackBerry Bridge application C	BlackBerry Bridge application D	Personal application E	Personal application F
Access a work file that a work application saves	Read-write access	Read-write access	No access	No access	No access	No access
Access a BlackBerry Bridge file that a BlackBerry	No access	No access	Read-write access	Read-write access	No access	No access

Access right	Work application A	Work application B	BlackBerry Bridge application C	BlackBerry Bridge application D	Personal application E	Personal application F
Bridge application saves						
Access a personal file that a personal application saves	Read-only	Read-only	Read-only	Read-only	Read-write access	Read-write access
Access the private data of Work application A	Read-write access	No access	No access	No access	No access	No access
Access the private data of Personal application E	No access	No access	No access	No access	Read-write access	No access

## Managing applications

You can use the BlackBerry Device Service to install and manage third-party applications on BlackBerry PlayBook tablets. You can specify the versions of the applications that you want to install, update, or remove, and you can specify which applications are required or optional on tablets. If you specify that an application is optional, the BlackBerry Device Service makes the application available to the user for installation on the Work tab in the BlackBerry App World storefront. If you specify that an application is required, the application is automatically installed on the tablet and the user cannot remove it.

When you use the BlackBerry Device Service to manage applications, the applications are considered work applications and are installed in the work perimeter on tablets. The applications can only access work data and interact with other work applications that are also located in the work perimeter. The applications have read-only access to personal data and cannot interact with personal applications that are located in the personal perimeter. You cannot manage or remove the personal applications that BlackBerry PlayBook users installed on their tablets.

Application developers can use various development tools to create, test, and package applications so that you can install them on the tablets in your organization's environment. For more information about the development tools, visit [www.blackberry.com/developers](http://www.blackberry.com/developers).

**Note:** The work perimeters on tablets do not support Android Runtime applications.

## Signing third-party applications

Before you can make a third-party application that is developed by your organization available to BlackBerry PlayBook tablets on the BlackBerry App World storefront Work tab, Research In Motion requires that the RIM signing authority system must digitally sign the application.

The RIM signing authority system uses public key cryptography to authorize and authenticate the application code.

The developer must visit <https://www.blackberry.com/SignedKeys> to register the application with the RIM signing authority system so that the application can use the signing tool that is included with the BlackBerry Tablet OS SDK. The signing tool permits an application to request, receive, and verify a digital signature from RIM. When a user starts the application, the BlackBerry Tablet OS verifies that the RIM signing authority signed the application files and that the application files did not change since that application was installed.

For more information about code signing applications, see <http://www.blackberry.com/developers>.

## When a tablet prevents a user from accessing work data or work applications

You can use the BlackBerry Device Service to allow a user to access work data and work applications. The BlackBerry PlayBook tablet does not permit the user to access work data or work applications when you or the user deletes all tablet data.

If you configure the Password Required for Work Perimeter IT policy rule to enforce the use of a password for the work perimeter and the user types the password for the work perimeter incorrectly more than the Maximum Password Attempts IT policy rule permits, the tablet closes all work applications and deletes the work perimeter.

Personal data and personal applications are not affected by the actions that the tablet performs to prevent the user from accessing work data and work applications.

## Using the browser to connect a tablet to web servers that support NTLM

NTLM is a suite of security protocols that Microsoft designed to provide authentication, integrity, and confidentiality for web connections.

If a BlackBerry PlayBook tablet user uses the browser to connect to web servers that support NTLM using a work Wi-Fi network or a work VPN network, the BlackBerry PlayBook tablet supports NTLMv1 authentication. The tablet also supports the message-signing capabilities of both NTLMv1 standard session security and NTLM Extended Session Security (also known as NTLM2). The web servers can be located either inside or outside of your organization's environment.

# The BlackBerry Tablet OS

## 9

The BlackBerry Tablet OS is the microkernel operating system of the BlackBerry PlayBook tablet. Microkernel operating systems implement the minimum amount of software in the kernel and run other processes in the user space that is outside of the kernel.

Microkernel operating systems are designed to contain less code in the kernel than other operating systems. The reduced amount of code helps the kernel to avoid the vulnerabilities that are associated with complex code and to make verification easier. Verification is the process of evaluating a system for programming errors. Many of the processes that run in the kernel in a conventional operating system run in the user space of the BlackBerry Tablet OS.

The BlackBerry Tablet OS is designed to be tamper resistant. The kernel performs an integrity test when the BlackBerry Tablet OS starts and if the integrity test detects damage to the kernel, the tablet does not start.

The BlackBerry Tablet OS is designed to be resilient. The kernel is designed to isolate a process in its user space if it stops responding and to restart the process without negatively affecting other processes. In addition, the kernel uses adaptive partitioning to allocate resources to specific processes during overload conditions.

The BlackBerry Tablet OS is designed to be highly secure. The kernel validates requests for resources and an authorization manager controls how applications access the capabilities of the tablet.

## The tablet file system

The BlackBerry PlayBook tablet file system runs outside of the kernel and is designed to keep work data highly secure and separate from personal data. The BlackBerry Tablet OS divides the file system into the following areas:

1. Base file system
2. Personal file system
3. Work file system
4. BlackBerry Bridge file system, if the tablet is connected to a BlackBerry smartphone using the BlackBerry Bridge app

The base file system is read-only and contains system files. Because the base file system is read-only, the BlackBerry Tablet OS can check the integrity of the base file system and mitigate the damage that a potentially malicious user who changes the file system can cause.

The personal file system contains the applications that run in personal mode and personal application data. Applications that a BlackBerry PlayBook tablet user installs on the tablet are located in the personal file system.

The work file system contains the applications that run in work mode and work application data. The tablet encrypts the work file system. The key that the tablet uses to decrypt the work file system is derived from keys that are stored in the replay protected memory block in flash memory. The replay protected memory block is encrypted with a key that is embedded in the processor when the processor is manufactured.

The BlackBerry Bridge file system contains the applications that run in BlackBerry Bridge mode and BlackBerry Bridge application data. The tablet encrypts the BlackBerry Bridge file system. The key that the tablet uses to decrypt the BlackBerry Bridge file system is stored on the BlackBerry smartphone that is connected to the tablet to prevent access to BlackBerry Bridge data when the tablet and the smartphone are not connected.

## How the BlackBerry Tablet OS uses sandboxing to protect application data

The BlackBerry Tablet OS uses a security mechanism called sandboxing to separate and restrict the capabilities and permissions of applications that run on the BlackBerry PlayBook tablet. Each application process runs in its own sandbox, which is a virtual container that consists of the memory and the part of the file system that the application process has access to at a specific time.

Each sandbox is associated with both the application and the perimeter that it is used in. For example, an application can have one sandbox in the personal perimeter and another sandbox in the work perimeter; each sandbox is isolated from the other sandbox.

The BlackBerry Tablet OS evaluates the requests that an application's process makes for memory outside of its sandbox. If a process tries to access memory outside of its sandbox without approval from the BlackBerry Tablet OS, the BlackBerry Tablet OS is designed to end the process, reclaim all of the memory that the process is using, and restart the process without negatively affecting other processes.

When the BlackBerry Tablet OS is installed, it assigns a unique group ID to each application. Two applications cannot share the same group ID, and the BlackBerry Tablet OS does not reuse group IDs after applications are removed. An application's group ID remains the same when the application is upgraded.

By default, each application stores its data in its own sandbox. The BlackBerry Tablet OS prevents applications from accessing file system locations that are not associated with the application's group ID.

An application can also store and access data in a shared directory, which is a sandbox that is available to any application that has access to it. When an application that wants to store or access files in the shared directory starts for the first time, the application prompts the user to allow access.

## How the BlackBerry Tablet OS manages the resources on a tablet

The BlackBerry Tablet OS is designed to manage the BlackBerry PlayBook tablet resources so that an application cannot take resources from another application. The BlackBerry Tablet OS uses adaptive partitioning to reallocate unused resources to applications during typical operating conditions and enhance the availability of the resources to specific applications during peak operating conditions.

## How the tablet manages permissions for applications

The authorization manager is the part of the BlackBerry Tablet OS that evaluates requests from applications to access the capabilities of the BlackBerry PlayBook tablet. Capabilities include taking a photograph and recording audio. The BlackBerry Tablet OS invokes the authorization manager when an application starts to set the permissions for the capabilities that the application uses. When an application starts, it might prompt the BlackBerry PlayBook tablet user to

allow access to a capability. The authorization manager can store a permission that the user grants access to and apply the permission the next time that the application starts.

## How a tablet verifies the software that it runs

### How a tablet verifies the boot ROM code

The BlackBerry PlayBook tablet uses an authentication method that is designed to verify that the boot ROM code is permitted to run on the tablet. The manufacturing process installs the boot ROM code in the processor on the tablet and the RIM signing authority system uses an RSA public key to sign the boot ROM code. The tablet stores information that it can use to verify the digital signature of the boot ROM code.

When a BlackBerry PlayBook tablet user turns on a tablet, the processor runs internal ROM code that reads the boot ROM from memory and verifies the digital signature of the boot ROM code using the RSA public key. If the verification process completes, the boot ROM is permitted to run on the tablet. If the verification process cannot complete, the tablet stops running.

### How a tablet verifies the Tablet OS and its filesystem

If the boot ROM code is permitted to run on the BlackBerry PlayBook tablet, the boot ROM code verifies the BlackBerry Tablet OS. The BlackBerry Tablet OS is digitally signed using EC 521 with a series of private keys. The boot ROM code uses the corresponding public keys to verify that the digital signature is correct. If it is correct, the boot ROM code runs the BlackBerry Tablet OS.

Before the BlackBerry Tablet OS mounts the read-only base filesystem, it runs a validation program that generates a SHA-256 hash of the base filesystem content, including all metadata. The program compares the SHA-256 hash to a SHA-256 hash that is stored outside the base filesystem. This stored hash is digitally signed using EC 521 with a series of private keys. If the hashes match, the validation program uses the corresponding public keys to verify the signature and the integrity of the stored hash.

### How a tablet verifies applications and software upgrades

Once the base filesystem is validated, the BlackBerry Tablet OS verifies existing applications by reading an application's XML file and verifying the assets of the application against the cryptographically signed hashes contained in the XML manifest.

Each software upgrade and application for the tablet is packaged in the BlackBerry Archive (BAR) format. This format includes SHA-2 hashes of each archived file, and it includes an ECC signature that covers the list of hashes. When a user installs a software upgrade or application, the installation program verifies that the hashes and the digital signature are correct.

The digital signatures for a BAR file also indicate to the user the author of the software upgrade or application. The user can then decide whether to install the software based on its author.

Because the tablet can verify the integrity of a BAR file, the tablet can download BAR files over an HTTP connection, which makes the download process faster than over a more secure connection.

## How a tablet is designed to prevent the exploitation of memory corruption

The BlackBerry PlayBook tablet is designed to prevent exploitation of memory corruption in a number of different ways, including the six security mechanisms listed below.

Security mechanism	Description
Non-executable stack and heap	The stack and heap areas of memory are marked as non-executable. This means that a process cannot execute machine code in these areas of the memory, which makes it more difficult for an attacker to exploit potential buffer overflows.
Stack cookies	Stack cookies are a form of buffer overflow protection that helps prevent attackers from executing arbitrary code.
Robust heap implementations	The heap implementation includes a defence mechanism against the deliberate corruption of the heap area of memory. The mechanism is designed to detect or mitigate the overwriting of in-band heap data structures so that a program can fail in a secure manner. The mechanism helps prevent attackers from executing arbitrary code via heap corruption.
Address space layout randomization (ASLR)	By default, the memory positions of all areas of a program are randomly arranged in a process's address space. This mechanism makes it more difficult for an attacker to perform an attack that involves predicting target addresses to execute arbitrary code.
Compiler-level source fortification	The compiler GCC uses the FORTIFY_SOURCE option to replace insecure code constructs where possible. For example, it might replace an unbounded memory copy with its bounded equivalent.
Guard pages	If a process attempts to access a memory page, the guard page raises a one-time exception and causes the process to fail. These guard pages are placed strategically between memory used for different purposes, such as the standard program heap and the object heap. This mechanism helps prevent an attacker from causing a heap buffer overflow and changing the behavior of a process or executing arbitrary code with the permissions of the compromised process.

## How a tablet minimizes the number of processes running as root

The BlackBerry PlayBook tablet is designed to minimize the number of processes running as root. Only the most essential first-party processes and no third-party processes can run as root. A subset of root capabilities is available to first-party processes that do not need full root capabilities.

# Protecting the data that the BlackBerry Device Service stores in your organization's environment

10

## Data that the BlackBerry Configuration Database stores

The BlackBerry Configuration Database stores the following information:

- Name of the BlackBerry Device Service
- Unique SRP authentication keys and unique SRP IDs, or UIDs, that the BlackBerry Device Service uses in the SRP authentication process to open a connection to the BlackBerry Infrastructure
- IT policy private keys of the IT policy key pairs that the BlackBerry Device Service generates for each BlackBerry PlayBook tablet
- PIN of each tablet
- Read-only copies of each device transport key
- Copy of your organization's user directory

## Best practice: Protecting the data that the BlackBerry Configuration Database stores

Best practice	Description
Audit connections to the Microsoft SQL Server.	<p>Consider the following guidelines:</p> <ul style="list-style-type: none"> <li>• At a minimum, write failed connection attempts to the Microsoft SQL Server log file and review the log file regularly.</li> <li>• When possible, save log files to a different hard disk drive than the one that the data files are stored on.</li> </ul>
Delete unsecured, old setup files.	<p>Consider deleting Microsoft SQL Server setup files that might contain plaintext, credentials encrypted with weak public keys, or sensitive information that the Microsoft SQL Server logged to a Microsoft SQL Server version-dependent location during the Microsoft SQL Server installation process.</p> <p>Microsoft distributes the Killpwd tool, which is designed to locate and delete passwords from unsecured, old setup files in your organization's</p>

Best practice	Description
Limit the permission level of the Microsoft SQL Server.	<p>environment. For more information, visit <a href="http://support.microsoft.com">support.microsoft.com</a> to read article KB263968.</p> <p>Consider associating each Microsoft SQL Server service with a Windows account that the service derives its security context from.</p> <p>Microsoft SQL Server permits the sa account and, in some cases, other user accounts to access operating system calls based on the security context of the account that runs the Microsoft SQL Server service. If you do not limit the permission level of the Microsoft SQL Server, a potentially malicious user might use these operating system calls to attack any other resource that the account has access to.</p>
Make the Microsoft SQL Server port numbers that are monitored by default on your organization's firewall unavailable.	Consider configuring your organization's firewall to filter packets that are addressed to TCP port 1433, addressed to UDP port 1434, or associated with named instances.
Protect the sa account using a password.	Consider assigning a password to the sa account on the Microsoft SQL Server, even on servers that require Windows authentication. The password is designed to prevent an empty or weak password for the sa account from being exposed if an administrator of the database resets the Microsoft SQL Server for mixed mode authentication.
Protect the Microsoft SQL Server installation from Internet-based attacks.	<p>Consider the following guidelines:</p> <ul style="list-style-type: none"> <li>• Require Windows Authentication Mode for connections to the Microsoft SQL Server to restrict connections to Windows user accounts and domain user accounts, and turn on credentials delegation. Windows Authentication Mode does not require you to store passwords on the computer.</li> <li>• Use stronger authentication protocols, required password complexity, and required expiration times.</li> </ul>
Use a secure file system.	<p>Consider the following guidelines:</p> <ul style="list-style-type: none"> <li>• Use NTFS for the Microsoft SQL Server because it is more stable and recoverable than FAT file systems, and NTFS permits security options such as file and directory ACLs and EFS.</li> <li>• Do not change the permissions that the Microsoft SQL Server specifies during the Microsoft SQL Server installation process. The Microsoft SQL Server creates appropriate ACLs on registry keys and files if it detects NTFS.</li> <li>• If you must change the account that runs the Microsoft SQL Server, decrypt the files that you could access using the old account and encrypt them again for access using the new account.</li> </ul>

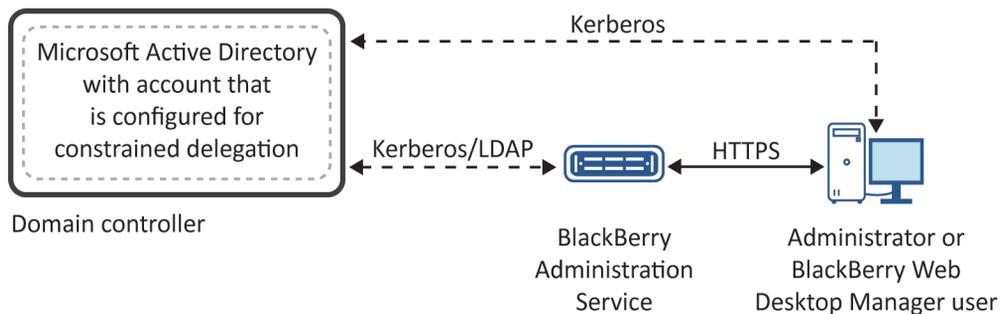
Best practice	Description
Use Microsoft SQL Server Management Studio.	<p data-bbox="554 215 893 239">Consider the following guidelines:</p> <ul data-bbox="554 263 1315 562" style="list-style-type: none"><li data-bbox="554 263 1315 406">• Use Microsoft SQL Server Management Studio to change the account that is associated with a Microsoft SQL Server service, if required. Microsoft SQL Server Management Studio configures the appropriate permissions on the files and registry keys that the Microsoft SQL Server uses.</li><li data-bbox="554 420 1315 562">• Do not use the Microsoft Management Console Services applet to change the account that is associated with a Microsoft SQL Server service. To use this applet, you must manually change the Windows registry, the permissions for the NTFS file system, and Windows user rights.</li></ul> <p data-bbox="554 590 1208 644">For more information, visit <a href="http://support.microsoft.com">support.microsoft.com</a> to read article KB283811.</p>

# Configuring single sign-on authentication for the BlackBerry Administration Service and BlackBerry Web Desktop Manager

You can configure the BlackBerry Administration Service so that administrators or BlackBerry Web Desktop Manager users must log in to the BlackBerry Administration Service console or BlackBerry Web Desktop Manager using Microsoft Active Directory authentication. If you configure the BlackBerry Administration Service to support Microsoft Active Directory authentication, you can also configure single sign-on so that administrators or users can access the BlackBerry Administration Service console or BlackBerry Web Desktop Manager directly without logging in.

If you configure single sign-on, the BlackBerry Administration Service uses the Kerberos protocol and constrained delegation to help protect your organization’s environment and authenticate and authorize administrators and users. The Kerberos protocol is designed to permit the BlackBerry Administration Service to verify administrator accounts and user accounts in Microsoft Active Directory. Constrained delegation is designed to limit the resources that the BlackBerry Administration Service can provide authenticated administrators and users access to.

## Architecture: BlackBerry Administration Service single sign-on



Component	Description
BlackBerry Administration Service	The BlackBerry Administration Service permits you to manage the BlackBerry Domain, which includes BlackBerry Device Service components, user accounts, and features for administering BlackBerry PlayBook tablet.
Domain controller	A domain controller is a server that authenticates and authorizes Windows users and Windows servers with a Windows domain.

Component	Description
Microsoft Active Directory	Microsoft Active Directory is an LDAP directory that stores user information.

## How BlackBerry Administration Service single sign-on uses Kerberos to help protect your organization's resources

BlackBerry Administration Service single sign-on implements Kerberos authentication, which permits the BlackBerry Administration Service to authenticate administrators and BlackBerry Web Desktop Manager users in your organization's network in a highly secure manner.

The BlackBerry Administration Service includes two Kerberos services that the BlackBerry Administration Service uses to authenticate with browsers. The BlackBerry Administration Service application server and BlackBerry Administration Service web server host the Kerberos services. The BlackBerry Administration Service requires two Kerberos services so that it can authenticate the web layer and application layer. The Kerberos service that the BlackBerry Administration Service web server hosts verifies requests from browsers to access the web layer. The Kerberos service that the BlackBerry Administration Service application server hosts verifies requests from the BlackBerry Administration Service web server to access the application layer.

The Kerberos services are identified using SPNs that you create and assign to a Microsoft Active Directory account. You must create the Microsoft Active Directory account as a Kerberos service account in the Microsoft Active Directory domain that includes the BlackBerry Administration Service and configure constrained delegation for the Microsoft Active Directory account. You must configure the Microsoft Active Directory account to trust only the Kerberos service that the BlackBerry Administration Service application server hosts for constrained delegation. You must configure the trust only when the BlackBerry Administration Service application service is using Kerberos.

If your organization's environment includes multiple Microsoft Active Directory account forests, you must configure a Microsoft Active Directory account for each account forest. You do not need to configure constrained delegation for the Microsoft Active Directory accounts that you configure in the account forests.

## How the BlackBerry Administration Service completes Kerberos authentication

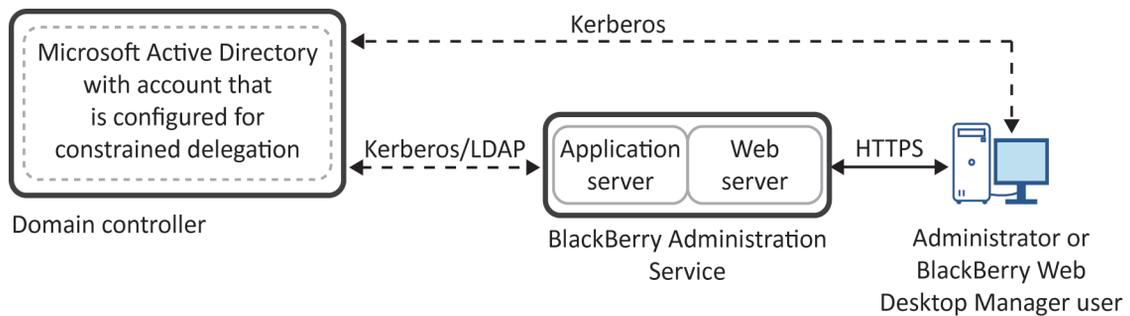
When the BlackBerry Administration Service starts, it authenticates with the Microsoft Active Directory domain using the Microsoft Active Directory account. The domain controller issues the Kerberos keys and Kerberos service ticket for the two Kerberos services. The Kerberos keys permit the BlackBerry Administration Service to verify the Kerberos service tickets that browsers send during single sign-on.

Browsers that support Integrated Windows authentication can obtain the Kerberos service ticket automatically for the BlackBerry Administration Service when administrators or users browse to the BlackBerry Administration Service console or BlackBerry Web Desktop Manager.

The Kerberos service that the BlackBerry Administration Service web server hosts uses its Kerberos keys to verify the Kerberos service tickets that browsers send when they request access to the BlackBerry Administration Service console or BlackBerry Web Desktop Manager. If the Kerberos service tickets are valid, the BlackBerry Administration Service web server delegates the request to the BlackBerry Administration Service application server.

To delegate the request, the BlackBerry Administration Service web server creates a service ticket using its identity for the Kerberos service that the BlackBerry Administration Service application server hosts. When the Kerberos service that the BlackBerry Administration Service application server hosts verifies the service ticket, the BlackBerry Administration Service completes the Kerberos authentication process for the administrators or users and they can view the BlackBerry Administration Service console home page or BlackBerry Web Desktop Manager home page.

## Data flow: Accessing the BlackBerry Administration Service console and BlackBerry Web Desktop Manager when you configure BlackBerry Administration Service single sign-on



1. An administrator or a BlackBerry Web Desktop Manager user uses a browser to navigate to the BlackBerry Administration Service web page ([https://<BAS\\_FQDN>/webconsole/login](https://<BAS_FQDN>/webconsole/login)) or BlackBerry Web Desktop Manager web page ([https://<BAS\\_FQDN>/webdesktop/login](https://<BAS_FQDN>/webdesktop/login)).
2. The BlackBerry Administration Service web server sends an HTTP Negotiate request to the browser to start single sign-on authentication.

For more information about the HTTP Negotiate request, see <http://msdn.microsoft.com/en-us/library/ms995330.aspx>.

3. The browser retrieves the TGT of the administrator or user from the ticket cache on the computer that the administrator or user is using.  
The browser uses the TGT to request the service ticket for the BlackBerry Administration Service web server (which is named HTTP/<BAS\_FQDN>) from the domain controller.
4. The domain controller provides the browser with the service ticket for the BlackBerry Administration Service web server.
5. The browser sends the service ticket to the BlackBerry Administration Service web server in response to the HTTP-Negotiate request.
6. The BlackBerry Administration Service web server performs the following actions:

- It validates the service ticket using the Kerberos key that it received from the domain controller when the BlackBerry Administration Service services started.
  - It requests a service ticket for the BlackBerry Administration Service application server (which is named `BASPLUGIN111/<BAS_FQDN>`) on behalf of the user.
7. The domain controller provides the BlackBerry Administration Service web server with the service ticket for the BlackBerry Administration Service application server.
  8. The BlackBerry Administration Service web server sends the service ticket to the BlackBerry Administration Service application server.
  9. The BlackBerry Administration Service application server performs the following actions:
    - It validates the service ticket using the Kerberos key that it received from the domain controller when the BlackBerry Administration Service services started. If the service ticket is valid, the administrator or user is authenticated successfully with the BlackBerry Administration Service using Kerberos.
    - It checks if the administrator or user is a BlackBerry device user or a BlackBerry Administration Service administrator.
    - It checks the role of the administrator or user and assigns the administrator or user the permissions that are associated with the role.
    - It sends a security session to the BlackBerry Administration Service web server for the administrator or user.
    - It stores the service ticket for future authentications. By default, the service ticket expires 80 minutes from the session idle time. If the session does not remain idle for more than 30 minutes, the ticket life time is 24 hours.
  10. The BlackBerry Administration Service web server redirects the administrator or user to the BlackBerry Administration Service console home page or BlackBerry Web Desktop Manager home page.

# How a tablet is designed to prevent BlackBerry Runtime for Android apps from accessing work data or work applications

12

The BlackBerry PlayBook tablet considers Android applications to be personal applications and installs them in the personal perimeter on tablets. Android applications can only access personal data that is located in the personal perimeter. Android applications do not have access to the work applications and work data that are located in the work perimeter. If the tablet is connected to a BlackBerry smartphone using BlackBerry Bridge technology, Android applications do not have access to the BlackBerry Bridge applications or BlackBerry Bridge data that are located in the BlackBerry Bridge perimeter.

You cannot manage or remove the Android applications that users install on their tablets.

## Protecting a tablet from malicious applications that are written for Android

Applications are tested to make sure that they do not interfere with the core functionality of the BlackBerry PlayBook tablet before they are approved by Research In Motion and made available on the BlackBerry App World storefront. RIM can remove any applications from BlackBerry App World that were identified as potentially malicious or do not follow the BlackBerry App World Vendor Agreement.

# Protecting user information

13

The BlackBerry PlayBook tablet is designed to allow you or a user to delete all user information and application data from the tablet memory. You or a user can delete all data from all perimeters on the tablet. You can also delete all data from only the work perimeter on the tablet.

## Using the tablet password

The BlackBerry PlayBook tablet permits the user to set a tablet password. If the user sets a tablet password, the user must provide the password to log in to the tablet. The user can configure the tablet password and timeout options using the Password option in the Security settings on the tablet. By default, if the user types the tablet password incorrectly 10 times, the tablet deletes all of the data on the tablet. For more information about setting the tablet password, see the tablet help.

The BlackBerry Device Service permits an administrator to use IT policy rules to enforce the use of a password for the work perimeter or for the entire tablet. These IT policy rules are called "Password Required for Work Perimeter" and "Password Required for Tablet." If the administrator enforces the use of a password for the work perimeter, the user can also set a separate tablet password.

The administrator can use IT policy rules to enforce password requirements, including minimum password length, complexity, and other restrictions. Any password requirement that is enforced by an IT policy overrides the corresponding settings on the device for the password that is affected by the IT policy.

For example, if the administrator sets an IT policy rule for the tablet password that restricts the number of password attempts to 3, this setting overrides the default setting on the tablet of 10 attempts. If the administrator sets an IT policy rule for the work perimeter password, the IT policy rule does not affect the corresponding settings on the tablet for the tablet password.

For more information about IT policies, see the *BlackBerry Device Service Policy Reference Guide*.

## Deleting all data from a tablet

The BlackBerry PlayBook tablet is designed to delete data from the tablet memory when any of the following events occurs. If the tablet is connected to a BlackBerry smartphone using the BlackBerry Bridge app when any of the following events occurs, the tablet also deletes all data from the BlackBerry Bridge perimeter.

- The user uses the Security Wipe option in the Security settings on the tablet
- The user types the tablet password incorrectly more times than the Maximum Password Attempts IT policy rule
- You send the "Delete all device data and remove device" IT administration command to the tablet

The tablet deletes the following data from each of the perimeters on the tablet.

Perimeter	Item	Description
Personal	Personal email messages	<ul style="list-style-type: none"> <li>Email messages that are sent to the user's personal email account and email messages that the user sends from their personal email account</li> <li>Draft email messages that the user creates using their personal email account</li> </ul>
	Attachments	Attachments that are sent to the user's personal email account and the attachments that the user sends from their personal email account
	Calendar entries	Calendar entries that the user creates using their personal calendar
	Contacts	Contact entries that the user creates using their personal contacts
	Personal files	Personal files that a user created or downloaded from a network other than your organization's network
	Personal videos, music, photos, and voice notes	Personal videos, music, photos, and voice notes that a user created or downloaded from a network other than your organization's network
	Personal applications	Personal applications that a user downloaded and installed on a tablet
	Personal data	Personal data that is associated with personal applications on the tablet (for example, game scores, saved maps, and the browser cache)
	Wi-Fi profiles	Wi-Fi profiles that the user configures on the tablet
	Tablet password	Password that the user set for the tablet
Work	Work email messages	<ul style="list-style-type: none"> <li>Email messages that are sent to the user's work email account and</li> </ul>

Perimeter	Item	Description
		<p>email messages that the user sends from the work email account</p> <ul style="list-style-type: none"> <li>• Draft email messages that the user creates using their work email account</li> </ul>
	Attachments	Attachments that are sent to the user's work email account and the attachments that the user sends from the work email account
	Calendar entries	Calendar entries that the user creates using their work calendar
	Contacts	Contacts that the BlackBerry Device Service synchronizes with the user's work email account
	Browser cache	Although the tablet specifies the Browser for personal use, the cache is deleted when you delete data from the work perimeter
	Files	Files that the user accessed and downloaded from your organization's network
	IT policy	IT policy that is associated with your organization
	Device transport key	References to the device transport key, which prevents the tablet from communicating with the BlackBerry Device Service
	Work applications	Work applications that a user downloaded and installed on a tablet
	Work data	Work data that is associated with work applications on the tablet
BlackBerry Bridge	Encrypted BlackBerry Bridge data	Encrypted BlackBerry Bridge data from the local cache on the tablet
	BlackBerry Bridge perimeter key	BlackBerry Bridge perimeter key from the tablet memory
	Bluetooth pairing	Bluetooth pairing with the smartphone

Perimeter	Item	Description
	Bluetooth key and BlackBerry Bridge pairing key	Bluetooth key and BlackBerry Bridge pairing key from the tablet memory

## Deleting all data from the work perimeter on a tablet

To protect your organization's data on a BlackBerry PlayBook tablet, you can delete all data from only the work perimeter on the tablet. For example, you can do this if a user no longer works at your organization.

The tablet is designed to delete all data from the work perimeter on the tablet when any of the following events occurs:

- The user types the password for the work perimeter incorrectly more times than the Maximum Password Attempts IT policy rule permits. The default value is ten attempts.
- You send the "Delete only the organization data and remove device" IT administration command to the tablet.

A BlackBerry device user can use the tablet while the tablet deletes the data in the work perimeter.

The tablet permanently deletes the following work data:

Item	Description
Work email messages	<ul style="list-style-type: none"> <li>• Email messages that are sent to the user's work email account and email messages that the user sends from the work email account</li> <li>• Draft email messages that the user creates using their work email account</li> </ul>
Attachments	Attachments that are sent to the user's work email account and the attachments that the user sends from the work email account
Calendar entries	Calendar entries that the user creates using their work calendar
Contacts	Contacts that the BlackBerry Device Service synchronizes with the user's work email account
Browser cache	Browser cache, Bookmarks, History, and Cookies.
Files	Files that the user accessed and downloaded from your organization's network
IT policy	IT policy that is associated with your organization
Device transport key	References to the device transport key, which prevents the tablet from communicating with the BlackBerry Device Service
Work data	Work data that is associated with work applications on the tablet
Wi-Fi and VPN profiles	Wi-Fi and VPN profiles that the user configures on the tablet

## Using IT policy rules to specify when all data must be deleted from a tablet

If you use the **Password Required for Tablet** IT policy rule to require that a BlackBerry PlayBook tablet user set a password on a BlackBerry PlayBook tablet, this password protects both the personal and work perimeters on the tablet and there will not be a separate password for the work perimeter.

You can then use the **Maximum Password Attempts for Work Perimeter** and **Wipe the Work Perimeter without Connectivity** IT policy rules to require that a tablet delete all data from the tablet under specific conditions.

For more information, see the *BlackBerry Device Service Policy Reference Guide*.

## Using IT policy rules to specify when all data on the work perimeter of a tablet must be deleted

You can configure the following IT policy rules to require that a BlackBerry PlayBook tablet deletes all data from the work perimeter on the tablet under specific conditions.

IT policy rule	Description
Maximum Password Attempts for Work Perimeter	This rule specifies the number of times that a BlackBerry PlayBook tablet user can try an incorrect password before a tablet deletes the data in the work perimeter.
Wipe the Work Perimeter without Connectivity	<p>This rule specifies the time in hours that must elapse without a tablet connecting to your organization's network before the tablet deletes the data in the work perimeter.</p> <p>Use this IT policy rule to make the tablet delete the data in the work perimeter if it cannot receive updates or commands. If you set this rule to a null value, the tablet does not delete the data from the work perimeter. By default, this rule is set to a null value.</p>

For more information, see the *BlackBerry Device Service Policy Reference Guide*.

# Cryptographic algorithms, codes, protocols, and APIs that a tablet supports

14

The BlackBerry PlayBook tablet supports the following types of cryptographic algorithms, codes, protocols, and APIs:

- Symmetric encryption algorithms
- Asymmetric encryption algorithms
- Hash algorithms
- Message authentication codes
- Signature scheme algorithms
- Key agreement scheme algorithms
- Cryptographic protocols
- Cryptographic APIs
- VPN cryptographic support
- Wi-Fi cryptographic support

## Symmetric encryption algorithms

Algorithm	Key length (in bits)	Modes
AES	128, 192, and 256	CBC, ECB, CTR
AES	512	XTS
Blowfish	40 to 448	CBC, CFB, ECB, OFB
Camellia	128 to 256	CBC
Camellia	256	ECB
CAST	40 to 128	CBC, CFB, ECB, OFB
CCMP	128	—
DES	56	CBC, CFB, ECB, EDE, OFB
RC4	128	—
Skipjack	80	—

Algorithm	Key length (in bits)	Modes
Triple DES	168	EDE, CBC, CFB, OFB
Twofish	128 to 256	CBC

## Asymmetric encryption algorithms

Algorithm	Key length (in bits)
ECC	163, 192, 256, 283, 384, and 512
RSA	a minimum of 512

## Hash algorithms

Algorithm	Digest size (in bits)
MD2	128
MD4	128
MD5	128
MDC-2	128
RIPEMD-160	160
SHA-1	160
SHA-2	224, 256, 384, 512

## Message authentication codes

Codes	Use with	Key length (in bits)
AES-XCBC-MAC	—	128
HMAC	MD5	128
HMAC	SHA-1	160

Codes	Use with	Key length (in bits)
HMAC	RIPEMD-160	160

## Signature scheme algorithms

Algorithm	Key length (in bits)	Type
ECDSA	521	Elliptic Curve (curve secp521r1)
RSA	512, 1024, 2048, and 4096	Integer factorization

## Key agreement schemes

Scheme	Key length (in bits)	Type
RSA	512, 1024, 2048, and 4096	Integer factorization
Diffie-Hellman	Maximum of 1024	Discrete logarithm
ECDH	256	(Elliptic curve) discrete logarithm
EC-SPEKE	256	(Elliptic curve) discrete logarithm
ECMQV	256	(Elliptic curve) discrete logarithm

## Cryptographic protocols

- SSL
- TLS
- IPSec
- WEP
- WPA
- WPA2

## Cipher suites that a tablet supports for opening TLS connections

A BlackBerry PlayBook tablet supports various cipher suites for direct mode TLS when the tablet opens TLS connections to the BlackBerry Infrastructure or to web servers that are internal or external to your organization.

The tablet supports the following cipher suites, in order, when it opens TLS connections:

- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA
- TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA
- TLS\_DHE\_DSS\_WITH\_AES\_256\_CBC\_SHA
- TLS\_ECDH\_RSA\_WITH\_AES\_256\_CBC\_SHA
- TLS\_ECDH\_ECDSA\_WITH\_AES\_256\_CBC\_SHA
- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA
- TLS\_ECDHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA
- TLS\_ECDHE\_ECDSA\_WITH\_3DES\_EDE\_CBC\_SHA
- TLS\_DHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA
- TLS\_DHE\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA
- TLS\_ECDH\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA
- TLS\_ECDH\_ECDSA\_WITH\_3DES\_EDE\_CBC\_SHA
- TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA
- TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA
- TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA
- TLS\_ECDH\_RSA\_WITH\_AES\_128\_CBC\_SHA
- TLS\_ECDH\_ECDSA\_WITH\_AES\_128\_CBC\_SHA
- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA
- TLS\_ECDHE\_RSA\_WITH\_RC4\_128\_SHA
- TLS\_ECDHE\_ECDSA\_WITH\_RC4\_128\_SHA
- TLS\_ECDH\_RSA\_WITH\_RC4\_128\_SHA
- TLS\_ECDH\_ECDSA\_WITH\_RC4\_128\_SHA

- TLS\_RSA\_WITH\_RC4\_128\_SHA
- TLS\_RSA\_WITH\_RC4\_128\_MD5

## Cryptographic APIs

- libeap
- libipsec
- PF-Key
- Security Builder® Crypto™-C
- OpenSSL

## VPN cryptographic support

Protocol	Authentication types	IKE IPsec DH group	IKE IPsec cipher	IKE IPsec hash	IKE PRF
IKE	PSK, PKI, XAUTH-PSK, XAUTH-PKI	1, 2, 5, 7 to 26	DES (56-bit key), Triple DES (168-bit key), AES (128, 192, 256-bit keys)	AES-XCBC, MD5, SHA-1, SHA-256, SHA-384, SHA-512	HMAC
IKEv2	PSK, PKI, EAP-TLS, EAP-MS-CHAPv2	1, 2, 5, 7 to 26	DES (56-bit key), Triple DES (168-bit key), AES (128, 192, 256-bit key)	AES-XCBC, MD5, SHA-1, SHA-256, SHA-384, SHA-512	AES-XCBC, HMAC-MD5, HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512

## Wi-Fi cryptographic support

Cryptographic protocol	Encryption protocol	EAP outer method	EAP inner method
WEP	RC4	—	—
WPA	TKIP	PEAP, EAP-TTLS, EAP-FAST, EAP-TLS	MSCHAPv2, EAP-GTC
WPA2	TKIP, CCMP (AES)	PEAP, EAP-TTLS, EAP-FAST, EAP-TLS	MSCHAPv2, EAP-GTC

## Related resources

15

To read the following guides, visit [www.blackberry.com/go/serverdocs](http://www.blackberry.com/go/serverdocs) .

Resource	Information
<i>BlackBerry Device Service Feature and Technical Overview</i>	<ul style="list-style-type: none"> <li>• Architecture diagrams</li> <li>• Description of features and components</li> <li>• Data flows</li> </ul>
<i>BlackBerry Bridge App and BlackBerry PlayBook Tablet Security Technical Overview</i>	<ul style="list-style-type: none"> <li>• Description of how work data is protected on BlackBerry PlayBook tablets when you use the BlackBerry Bridge app</li> <li>• Description of how work data is protected when it is in transit between a tablet and a BlackBerry smartphone</li> <li>• Description of attacks that the BlackBerry Bridge pairing process is designed to prevent</li> </ul>
<i>BlackBerry Administration Service Help and BlackBerry Device Service Administration Guide</i>	<ul style="list-style-type: none"> <li>• Instructions for creating user accounts, groups, roles, administrator accounts, and so on</li> <li>• Instructions for activating tablets</li> <li>• Instructions for creating and sending IT policies and profiles</li> <li>• Instructions for sending and managing applications on tablets</li> </ul>
<i>BlackBerry Device Service Policy Reference Guide</i>	<ul style="list-style-type: none"> <li>• Description of available IT policy rules and profile settings</li> </ul>
<i>BlackBerry PlayBook Tablet Print To Go Security Note</i>	<ul style="list-style-type: none"> <li>• Description of how data is protected when using Print To Go</li> <li>• Instructions for preventing the use of Print To Go</li> </ul>
<i>BlackBerry Device Service Release Notes</i>	<ul style="list-style-type: none"> <li>• Description of known issues and potential workarounds</li> </ul>

# Glossary

16

<b>ACL</b>	An access control list (ACL) is a list of permissions that are associated with an object, such as a file, directory, or other network resource. It specifies which users or components have permission to perform specific operations on an object.
<b>AES</b>	Advanced Encryption Standard
<b>AES-CCMP</b>	Advanced Encryption Standard Counter Mode CBCMAC Protocol
<b>AES-XCBC-MAC</b>	Advanced Encryption Standard extended cipher block chaining message authentication code
<b>API</b>	application programming interface
<b>ARC4</b>	Alleged Rivest's Cipher 4
<b>CAST</b>	Carlisle Adams Stafford Tavares
<b>CBC</b>	cipher block chaining
<b>CCKM</b>	Cisco Centralized Key Management
<b>CFB</b>	cipher feedback
<b>CKIP</b>	Cisco Key Integrity Protocol
<b>CSR</b>	certificate signing request
<b>CTR</b>	Counter
<b>DES</b>	Data Encryption Standard
<b>DH</b>	Diffie-Hellman
<b>DRBG</b>	deterministic random bit generator
<b>DSA</b>	Digital Signature Algorithm
<b>EAP</b>	Extensible Authentication Protocol
<b>EAP-FAST</b>	Extensible Authentication Protocol Flexible Authentication via Secure Tunneling
<b>EAP-GTC</b>	Extensible Authentication Protocol Generic Token Card
<b>EAPoL</b>	Extensible Authentication Protocol over LAN
<b>EAP-MS-CHAP</b>	Extensible Authentication Protocol Microsoft Challenge Handshake Authentication Protocol
<b>EAP-TLS</b>	Extensible Authentication Protocol Transport Layer Security
<b>EAP-TTLS</b>	Extensible Authentication Protocol Tunneled Transport Layer Security

<b>ECB</b>	electronic code book
<b>ECC</b>	Elliptic Curve Cryptography
<b>ECDH</b>	Elliptic Curve Diffie-Hellman
<b>ECDSA</b>	Elliptic Curve Digital Signature Algorithm
<b>ECMQV</b>	Elliptic Curve Menezes-Qu-Vanstone
<b>EC-SKEPE</b>	Elliptic Curve – Simple Password Exponential Key Exchange
<b>EDE</b>	Encryption-Decryption-Encryption
<b>EFS</b>	Encrypting File System
<b>FQDN</b>	fully qualified domain name
<b>HMAC</b>	keyed-hash message authentication code
<b>HTML</b>	Hypertext Markup Language
<b>HTTP</b>	Hypertext Transfer Protocol
<b>HTTPS</b>	Hypertext Transfer Protocol over Secure Sockets Layer
<b>IEEE</b>	Institute of Electrical and Electronics Engineers
<b>IETF</b>	Internet Engineering Task Force
<b>IKE</b>	Internet Key Exchange
<b>IPsec</b>	Internet Protocol Security
<b>IT policy</b>	An IT policy consists of various IT policy rules that control the security features and behavior of BlackBerry smartphones, BlackBerry PlayBook tablets, the BlackBerry Desktop Software, and the BlackBerry Web Desktop Manager.
<b>IT policy rule</b>	An IT policy rule permits you to customize and control the actions that BlackBerry smartphones, BlackBerry® PlayBook™ tablets, the BlackBerry® Desktop Software, and the BlackBerry® Web Desktop Manager can perform.
<b>LAN</b>	A local area network (LAN) is a computer network shared by a group of computers in a small area, such as an office building. Any computer in this network can communicate with another computer that is part of the same network.
<b>LDAP</b>	Lightweight Directory Access Protocol
<b>MD</b>	Message Digest Algorithm
<b>MDC</b>	Modification Detection Code
<b>MS-CHAP</b>	Microsoft Challenge Handshake Authentication Protocol
<b>NIST</b>	National Institute of Standards and Technology

<b>NTFS</b>	New Technology File System
<b>NTLM</b>	NT LAN Manager
<b>NV</b>	nonvolatile
<b>OFB</b>	output feedback
<b>PAC</b>	Protected Access Credential
<b>PEAP</b>	Protected Extensible Authentication Protocol
<b>PIN</b>	personal identification number
<b>PKCS</b>	Public-Key Cryptography Standards
<b>PKI</b>	Public Key Infrastructure
<b>PRNG</b>	pseudorandom number generator
<b>PSK</b>	pre-shared key
<b>RACE</b>	Research and Development in Advanced Communications Technologies in Europe
<b>RC</b>	Rivest's Cipher
<b>RFC</b>	Request for Comments
<b>RIM signing authority system</b>	The RIM <sup>®</sup> signing authority system is used by third-party developers to cryptographically sign their applications.
<b>RIPEMD</b>	RACE Integrity Primitives Evaluation Message Digest
<b>SCEP</b>	simple certificate enrollment protocol
<b>SHA</b>	Secure Hash Algorithm
<b>SPN</b>	A Service Principal Name (SPN) is an attribute of a user or group in Microsoft Active Directory that supports mutual authentication between a client of a Kerberos enabled service and the Kerberos enabled service. A Microsoft Active Directory account can have one or more SPNs.
<b>SRP</b>	Server Routing Protocol
<b>SSL</b>	Secure Sockets Layer
<b>TCP</b>	Transmission Control Protocol
<b>TCP MD5</b>	Transmission Control Protocol message digest algorithm 5
<b>TGT</b>	The Ticket Granting Ticket (TGT) is a service ticket that a client of a Kerberos enabled service sends to the TGS to request the service ticket for the Kerberos enabled service.
<b>TKIP</b>	Temporal Key Integrity Protocol
<b>TLS</b>	Transport Layer Security
<b>Triple DES</b>	Triple Data Encryption Standard

<b>UID</b>	unique identifier
<b>VPN</b>	virtual private network
<b>WAP</b>	Wireless Application Protocol
<b>WEP</b>	Wired Equivalent Privacy
<b>WPA</b>	Wi-Fi Protected Access
<b>XEX</b>	Xor-Encrypt-Xor
<b>XTS</b>	XEX-based Tweaked CodeBook mode with CipherText Stealing

## Legal notice

17

©2012 Research In Motion Limited. All rights reserved. BlackBerry®, RIM®, Research In Motion®, and related trademarks, names, and logos are the property of Research In Motion Limited and are registered and/or used in the U.S. and countries around the world.

Adobe and Reader are trademarks of Adobe Systems Incorporated. Bluetooth is a trademark of Bluetooth SIG. Security Builder is a trademark of Certicom Corp. Documents To Go is a trademark of Dataviz, Inc. Android is a trademark of Google Inc. Kerberos is a trademark of the Massachusetts Institute of Technology. IEEE 802.11, IEEE 802.11i, and IEEE 802.1X are trademarks of the Institute of Electrical and Electronics Engineers, Inc. Microsoft, ActiveSync, ActiveX, Internet Explorer, SQL Server, and Windows are trademarks of Microsoft Corporation. RSA is a trademark of RSA Security. Wi-Fi, WPA, WPA2, WPA-Personal, WPA2-Personal, WPA-Enterprise, and WPA2-Enterprise are trademarks of the Wi-Fi Alliance. All other trademarks are the property of their respective owners.

This documentation including all documentation incorporated by reference herein such as documentation provided or made available at [www.blackberry.com/go/docs](http://www.blackberry.com/go/docs) is provided or made accessible "AS IS" and "AS AVAILABLE" and without condition, endorsement, guarantee, representation, or warranty of any kind by Research In Motion Limited and its affiliated companies ("RIM") and RIM assumes no responsibility for any typographical, technical, or other inaccuracies, errors, or omissions in this documentation. In order to protect RIM proprietary and confidential information and/or trade secrets, this documentation may describe some aspects of RIM technology in generalized terms. RIM reserves the right to periodically change information that is contained in this documentation; however, RIM makes no commitment to provide any such changes, updates, enhancements, or other additions to this documentation to you in a timely manner or at all.

This documentation might contain references to third-party sources of information, hardware or software, products or services including components and content such as content protected by copyright and/or third-party web sites (collectively the "Third Party Products and Services"). RIM does not control, and is not responsible for, any Third Party Products and Services including, without limitation the content, accuracy, copyright compliance, compatibility, performance, trustworthiness, legality, decency, links, or any other aspect of Third Party Products and Services. The inclusion of a reference to Third Party Products and Services in this documentation does not imply endorsement by RIM of the Third Party Products and Services or the third party in any way.

EXCEPT TO THE EXTENT SPECIFICALLY PROHIBITED BY APPLICABLE LAW IN YOUR JURISDICTION, ALL CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS, OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS OR WARRANTIES OF DURABILITY, FITNESS FOR A PARTICULAR PURPOSE OR USE, MERCHANTABILITY, MERCHANTABILITY, NON-INFRINGEMENT, SATISFACTORY QUALITY, OR TITLE, OR ARISING FROM A STATUTE OR CUSTOM OR A COURSE OF DEALING OR USAGE OF TRADE, OR RELATED TO THE DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN, ARE HEREBY EXCLUDED. YOU MAY ALSO HAVE OTHER RIGHTS THAT VARY BY STATE OR PROVINCE. SOME JURISDICTIONS MAY NOT ALLOW THE EXCLUSION OR LIMITATION OF IMPLIED WARRANTIES AND CONDITIONS. TO THE EXTENT PERMITTED BY LAW, ANY IMPLIED WARRANTIES OR CONDITIONS RELATING TO THE DOCUMENTATION TO THE EXTENT THEY CANNOT BE EXCLUDED AS SET OUT ABOVE, BUT CAN BE LIMITED, ARE HEREBY LIMITED TO NINETY (90) DAYS FROM THE DATE YOU FIRST ACQUIRED THE DOCUMENTATION OR THE ITEM THAT IS THE SUBJECT OF THE CLAIM.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, IN NO EVENT SHALL RIM BE LIABLE FOR ANY TYPE OF DAMAGES RELATED TO THIS DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN INCLUDING WITHOUT LIMITATION ANY OF THE FOLLOWING DAMAGES: DIRECT, CONSEQUENTIAL, EXEMPLARY, INCIDENTAL, INDIRECT, SPECIAL, PUNITIVE, OR AGGRAVATED DAMAGES, DAMAGES FOR LOSS OF PROFITS OR REVENUES, FAILURE TO REALIZE ANY EXPECTED SAVINGS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, LOSS OF BUSINESS OPPORTUNITY, OR CORRUPTION OR LOSS OF DATA, FAILURES TO TRANSMIT OR RECEIVE ANY DATA, PROBLEMS ASSOCIATED WITH ANY APPLICATIONS USED IN CONJUNCTION WITH RIM PRODUCTS OR SERVICES, DOWNTIME COSTS, LOSS OF THE USE OF RIM PRODUCTS OR SERVICES OR ANY PORTION THEREOF OR OF ANY AIRTIME SERVICES, COST OF SUBSTITUTE GOODS, COSTS OF COVER, FACILITIES OR SERVICES, COST OF CAPITAL, OR OTHER SIMILAR PECUNIARY LOSSES, WHETHER OR NOT SUCH DAMAGES WERE FORESEEN OR UNFORESEEN, AND EVEN IF RIM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, RIM SHALL HAVE NO OTHER OBLIGATION, DUTY, OR LIABILITY WHATSOEVER IN CONTRACT, TORT, OR OTHERWISE TO YOU INCLUDING ANY LIABILITY FOR NEGLIGENCE OR STRICT LIABILITY.

THE LIMITATIONS, EXCLUSIONS, AND DISCLAIMERS HEREIN SHALL APPLY: (A) IRRESPECTIVE OF THE NATURE OF THE CAUSE OF ACTION, DEMAND, OR ACTION BY YOU INCLUDING BUT NOT LIMITED TO BREACH 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. Some airtime service providers might not offer Internet browsing functionality with a subscription to the BlackBerry® Internet Service. Check with your service provider for availability, roaming arrangements, service plans and 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.

Certain features outlined in this documentation require a minimum version of BlackBerry® Enterprise Server, BlackBerry® Desktop Software, and/or BlackBerry® Device Software.

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  
Centrum House  
36 Station Road  
Egham, Surrey TW20 9LF  
United Kingdom

Published in Canada