Security Guide

PRIV by BlackBerry

Contents

Introduction: Security and privacy, deep and wide

BlackBerry has an extensive legacy of integrating security and privacy into all of our products. As the power and complexity of mobile devices has increased, our focus has remained on ensuring device integrity and putting together the best security solution for our customers. We focus on building mobile devices that embed security into the hardware itself, creating secure, trusted end points for enterprise mobility.

PRIV by BlackBerry is a professional and secure device that runs the Android™ OS. Just as we've always built security into every layer of our products, PRIV brings the renowned security features of BlackBerry to the Android OS, resulting in a device that you can trust to give you better protection from threats against your apps, data, and networks.

First and foremost, our world-renowned approach to mobile device security, as embodied in our security solution for BlackBerry 10 devices and now PRIV, is both deep and wide: we harden all layers of the device stack (deep) and we build security into all aspects of the end-to-end mobile device solution (wide).

This guide describes the privacy and security of PRIV hardware and software, including:

- The value of embedding security into the end points to create a hardware Root of Trust

- Layered defenses we've added throughout the mobile device stack, including the hardware platform, firmware, mobile OS, and secure communications and collaboration apps

- How we've secured the Android OS

- The flexibility of various deployment models that allow you to secure devices regardless of who owns them, which network they're on, and which EMM solution you use

- The end-to-end BlackBerry security platform, including device security, app security, secure device management, secure network connectivity, security patch and upgrade management, and more

# Device security: Layered defenses throughout the stack

2

PRIV is designed with security as one of its key features. We build security into every layer of the device, resulting in a layered defense approach that provides maximum protection against any attempts to attack the device and compromise your organization's information.

PRIV ensures the integrity of the Android™ platform. We secure PRIV starting with the device hardware and continuing through every layer of the device. We incorporate vulnerability mitigations and reduce attack vectors to harden the platform against security compromises.

We use various security measures to protect device hardware and the Android OS, and to establish a Root of Trust. Encryption and authentication processes then use the Root of Trust to create encryption and signing keys that protect your apps and data. This extensive security model keeps your apps, data, and network safe from attacks and gives you the peace of mind that you need so that you can focus on your business.

Device architecture

BlackBerry leverages our extensive experience securing mobile platforms to harden all layers of the device stack on PRIV.
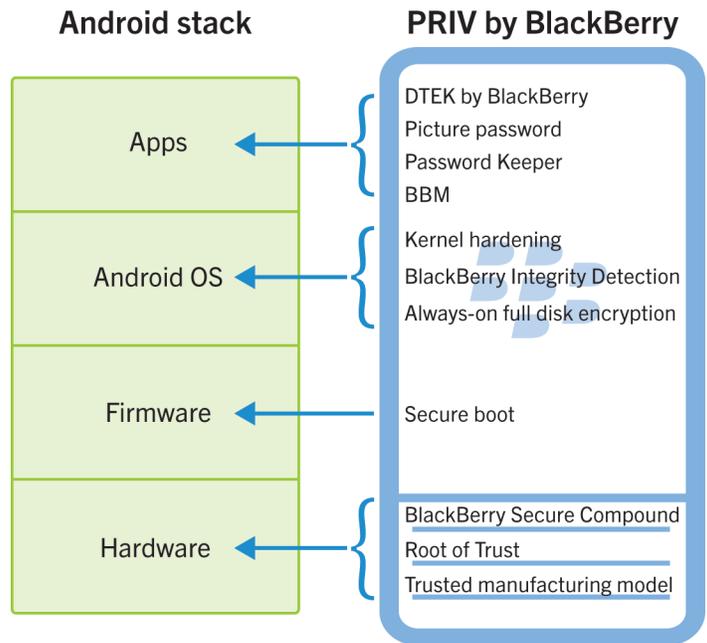
From hardware right through to apps, PRIV brings Android™ to a new level of security. Every area of the device works together to protect the privacy, integrity, and confidentiality of your apps and data.

Hardware

You need to know that the mobile devices that connect to your organization's network are trustworthy and not counterfeit, spoofed, or compromised. Trustworthiness needs a solid foundation, which for computers or mobile devices ultimately means the hardware itself should be the foundation of trust.

Manufacturing model

We've enhanced our end-to-end manufacturing model to securely connect the supply chain, BlackBerry manufacturing partners, our network, and devices, which allow us to build trusted devices anywhere in the world.

During manufacturing, we use the device's hardware-based keys to track, verify, and provision each device as it goes through the manufacturing process.

Root of Trust

A hardware-based Root of Trust is established during processor manufacturing by injecting cryptographic material that's later used for device authentication and secure boot.

Firmware

We use various security measures in the firmware to validate and ensure the integrity of the software running on PRIV.

Secure boot

The secure boot process ensures that only a BlackBerry signed OS can be loaded on PRIV and that it hasn't been tampered with. Each stage of the secure boot process verifies that the next component hasn't been tampered with before loading it.

Verifying the boot loader

The bootchain on PRIV is validated in multiple stages.

Stage	Description
Primary boot loader	The primary boot loader is part of the CPU and is write-protected. It validates the BlackBerry security shim using a key that's provisioned during processor manufacturing (using RSA-2048 with SHA-256). PRIV locks the boot media and locks the primary boot loader to load only the BlackBerry security shim.
BlackBerry security shim	The BlackBerry security shim resides between the primary and secondary boot loaders. It verifies the cryptographic signature on the secondary boot loader (using ECC-521 and SHA-512) and enforces downgrade prevention. It's located in the primary boot partition of the eMMC and is write-protected.
Secondary boot loader	The secondary boot loader is a vendor-supplied component that consists of a hardware device image residing in the CPU internal memory. The secondary boot loader is loaded into the CPU internal memory locations and executes from there. The secondary boot loader validates the tertiary boot loader and BlackBerry Secure Compound using RSA-2048 with SHA-256. There are two signed copies of the secondary boot loader image: • A main image is stored in the user partition and is used during the normal boot process; it's not write-protected and can be updated. • A backup image is stored in the boot partition and is write-protected.
Tertiary boot loader	The tertiary boot loader runs from external DDR instead of internal RAM, so it's not memory-constrained like the other images. It calls and validates the boot image (ECC-521 and SHA-256). There are two copies of the tertiary boot loader image: • A main image is stored in the user partition and can be upgraded as part of the standard update process. • A backup image is stored in the boot partition and is write-protected.
Boot image	The boot image is the actual system kernel, located in the user partition of eMMC, on the boot partition. Before the boot image mounts the dm-verity protected read-only file system, it's validated with the dm-verity key (RSA-2048 using SHA-256). It then starts the Android OS. For more information about dm-verity, see https://source.android.com/devices/tech/security/verifiedboot/index.html

Downgrade prevention

Downgrade prevention stops a user from loading an old OS version on PRIV after the device is upgraded. This protects against situations such as a user loading an OS version that doesn't have the latest security fixes or a malicious user exploiting a vulnerability that exists in an older OS version.

BlackBerry Integrity Detection

BlackBerry Integrity Detection continuously monitors for events or configuration changes that could indicate a compromise to the security of PRIV. These include validating that unauthorized apps haven't acquired escalated privileges (for example, rooting), performing checks on the integrity of the kernel, monitoring file system mounting permissions, unauthorized changes to the SELinux policy, and the disabling of security sensitive applications such as pathtrust. EMM and other third-party monitoring solutions can integrate with BlackBerry Integrity Detection to request integrity reports to monitor PRIV for compromises.

DTEK by BlackBerry integrates with BlackBerry Integrity Detection for the operating system integrity sensor.

If your devices are managed by an EMM solution that's integrated with BlackBerry Integrity Detection (such as BES12), an administrator can configure remediation action if a potential compromise is detected, such as generating an alert, quarantining the device from accessing work resources, or wiping the device.

The BlackBerry Integrity Detection architecture leverages a trusted application running in the BlackBerry Secure Compound to provide a trusted anchor to ensure the integrity of the solution and generate signed integrity reports. Integrity sensors are deployed as both a kernel module and Java application.

The integrity reports are digitally signed by the trusted application with ECC-256 and backed by a certificate that chains up to a BlackBerry CA so that EMM solutions and monitoring apps that aren't developed by BlackBerry can verify their authenticity. The private key is protected by BlackBerry Secure Compound.

The Android OS

We've leveraged our extensive experience securing mobile platforms to increase security resilience on PRIV. Increasing the integrity of the Android OS is a cornerstone of BlackBerry's integration with the Android ecosystem. To minimize surface vulnerability and reduce attack vectors, we've implemented enhanced security measures for the Android OS.

The Android OS security features

PRIV runs the Android OS version 5.1 or later (Lollipop). The Android OS version 5.1 includes several security features, such as improved full-disk encryption, Android sandbox reinforced with SELinux, updates to WebView without OTA, and updated cryptography for HTTPS and TLS/SSL.

For more information about the security features in the Android OS, see https://source.android.com/devices/tech/security/enhancements/enhancements50.html.

Kernel hardening

PRIV runs a Linux kernel that's been hardened with patches and configuration changes to decrease the likelihood of a compromise due to a security vulnerability.

The kernel was modified to remove unneeded functionality, reducing the attack surface on PRIV. Unused kernel configuration parameters were made read-only to user space processes, forcing a known-good configuration. Additional hardening is provided by the integration of several kernel patches. This hardening results in a kernel that's more restrictive than other Android devices, increasing resilience against unknown vulnerabilities.

Additional custom security verification is embedded in the kernel which restricts both privileged loading and execution of any content that's not integrity-verified.

As part of our hardening process, we reviewed public root exploits against other Android devices in an effort to identify and create generic approaches to mitigate against future attacks.

Related information
Secure boot, on page 7

Enhanced memory protection

PRIV supports the native address space layout randomization offered in the Android OS to prevent the exploitation of device memory corruption.

By default, the memory positions of all areas of a program are randomly arranged in the address space of a process. Address space layout randomization is a technique that randomizes the location of system components in memory. This makes it more difficult for an attacker to know where a vulnerability exists, perform an attack that involves predicting target addresses to execute arbitrary code, and essentially exploit a device and run their own code.

PRIV reinforces address space layout randomization by randomizing all executable memory segments and using different and varying memory layout for system and non-system applications.

BlackBerry Secure Compound

BlackBerry Secure Compound provides a trusted execution environment to protect sensitive data and run security-focused apps. On PRIV, BlackBerry Secure Compound is leveraged by the secure boot process, to generate and protect keys and the device password, and to run the BlackBerry Integrity Detection trusted app.

Full-disk encryption

PRIV encrypts user data using Android full-disk encryption. By default, data encryption is turned on and automatic.

PRIV enhances the security of Android full-disk encryption by using a FIPS 140-2 compliant Certicom/BlackBerry Cryptographic Kernel encrypting user data using AES-128 (AES-CBC-ESSIV:SHA-256) and protecting the key with BlackBerry Secure Compound.

For more information about how Android full-disk encryption works, see https://source.android.com/devices/tech/security/encryption/.

Data protection

PRIV supports various methods that you can use to keep data private and secure while it's stored on the device.

Passwords

Passwords protect access to your users' information and your organization's information stored on PRIV.

PRIV adds the following security features to the Android OS to enhance protection of the information stored on the device:

Item	Description
BlackBerry Secure Compound	BlackBerry Secure Compound handles secure password generation and protection on the device. The passwords are derived using PBKDF2 as the key derivation function with HMAC-SHA-512 and stored in NVRAM on the device. The data related to the password, such as the salt and the number of iterations, is also stored in NVRAM.
	This approach is designed to make it harder to access the password hash to then perform a brute force attack on the HMAC.
Wipe all user data after 10 incorrect password attempts	If the device is password-protected, a user has 10 attempts to enter the correct password. After the tenth incorrect attempt, the device deletes all user information and app data, and returns the device to factory default settings. If another user profile owner types their profile password incorrectly more than 10 times, their user profile is removed from the device.
	If the device is managed by an EMM solution, the EMM solution might determine how many incorrect password attempts a user can make before the device is wiped. If another user profile owner types their profile password incorrectly more times than the EMM solution allows, their user profile is removed from the device.

If your devices are managed by an EMM solution, you can enforce password protection and control password requirements, such as complexity and length, to ensure that a device meets the requirements of your organization. Your EMM solution may

also provide management options for a lost device, including the ability to lock it remotely. You can do this, for example, if a device is lost or if a user forgets their password.

Picture password

In addition to numeric and alphanumeric passwords, PRIV offers another level of password security with a picture password option. A picture password provides a method of securing a device that allows a user to use a combination of a number and picture to unlock their device instead of typing a password.

A picture password not only provides a user with a quick and easy way to unlock their device, it also helps prevent an attacker from breaking into a device using methods, including the following:

Method	Description
Using smudges on the device screen	A picture password always shows a random number grid whenever a user unlocks their device, which means a user never follows the same pattern. Because a user always moves their number from a different location on the grid, an attacker won't see a smudge pattern.
Looking over a user's shoulder	When using a simple password, someone could look over a user's shoulder while they enter it. A picture password prevents this situation from occurring by drawing a random number grid and varying the size of the grid. For example, in addition to a random number grid, the grid size also randomly changes, increasing and decreasing the number of rows and columns to reduce the shoulder-attack vulnerability.
Brute force attack	A picture password addresses brute force attacks by limiting the number of guesses, varying the size, location, and pattern of the grid numbers, and requiring minimum movement of the number grid.

Media card protection

PRIV protects data by controlling access to media cards. Media card access depends on the management option of the device:

Management option	Description
Unmanaged	If a device has multiple user profiles configured, only the primary user profile can use the device's media card.
Android for Work: Profile Owner mode	The user has read-only access to the media card when using apps in the work profile. Outside the work profile, the user has read/write access to the media card.
Android for Work: Device Owner mode	Because only one user profile is allowed with this type of management option, the device user has full access to the media card.

Related information

Data wipe

To protect your organization's data and user information on PRIV, a user can delete their device data, including data on the media card.

If your devices are managed by an EMM solution, an administrator can control when a device must wipe its data.

PRIV performs a full device wipe or work data wipe as follows:

- If the device is password-protected and the device owner types the device password incorrectly more times than an EMM solution or device settings allow, the device deletes all user information and app data, and returns the device to factory default settings.

- If a secondary profile or guest profile user types their profile password incorrectly more times than an EMM solution or device settings allow, the profile is removed from the device.

- If a user performs a factory reset on their device, the device permanently deletes all data so that it can't be recovered.

- If a user has a remote device management app, such as Android Device Manager, set up on their device, they may be able to perform a remote device wipe.

When a device wipe occurs, all data on the device is permanently deleted, including email accounts, downloaded apps, media files, documents, browser bookmarks, and settings.

For more information about user options for data wipe, see the PRIV user guide.

Apps

PRIV integrates a number of apps to enhance productivity, while maintaining control and protection of user information:

- DTEK by BlackBerry to assess device security by helping a user monitor, track, and control the level of security on their device from an easy-to-use app

- BBM for a secure and useable mobile instant messaging app

- BlackBerry Password Keeper to securely store a user's security-related information, such as passwords, usernames, and security questions, in one password-protected app

- Remote device management apps to protect a lost or stolen device

Related information

DTEK by BlackBerry

DTEK by BlackBerry is a visual tool that helps a user monitor and control the level of security on PRIV, by performing the following functions:
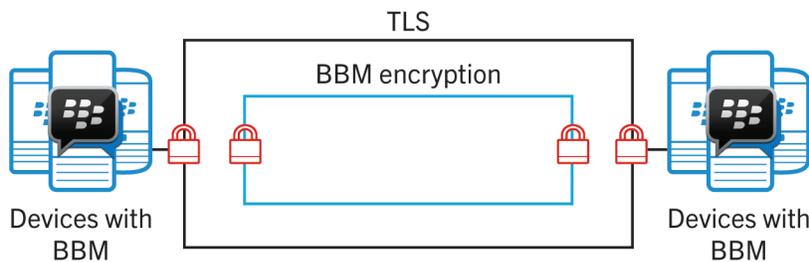
- Evaluates how or if a user has set up security features on their device, including screen lock, factory reset protection, remote device management, and trusted app sources.

- Assigns an overall security rating to the device along with a rating for each of the security features that it monitors. If a security feature receives a poor or good rating, DTEK recommends how the user can improve their security settings to achieve a better rating. A user can improve the overall security rating for their device by adjusting the settings of individual security features on their device.

- Monitors third-party apps that a user downloads onto their device or that their service provider pushes to the device. It doesn't monitor preloaded apps. It also doesn't monitor apps that an administrator might push to the device if the device is managed by an EMM solution.

- Lets a user see what third-party apps do on the device, such as using the camera, accessing contacts or the device's location, or sending a text message from the device. Some apps must access these features to work correctly. Other apps might access features on the device without the user's knowledge.

- Allows a user to view the details of when an app used a device feature to access their data. A user can also set up notifications to monitor future access, stop the app from running, or uninstall the app from the device.

For more information about DTEK, see http://help.blackberry.com/detectLang/dtek-by-blackberry/.

BBM

BBM brings users together in the moment with friends and family through instant chats, voice calls, picture sharing, voice notes, and more. With BBM, what a user shares is theirs to control:

- Timed messages: A user can set how long contacts have access to messages and pictures shared in a chat before they disappear from the screen.

- Message retraction: A user can retract a message to remove it from their BBM chat.

- A user can choose how to share their information: BBM uses PINs instead of phone numbers or email addresses so that it's more private, and a user always controls who can contact them.

- A user can choose their contacts: Two-way opt-in means that a user has control over who's able to message them.

For more information about the security of BBM, see http://help.blackberry.com/detectLang/bbm-security/latest/.

Password Keeper

A user can use BlackBerry Password Keeper to store all passwords, usernames, and security questions in one place on PRIV. Password Keeper protects the passwords with a master password, and a user is required to remember only the master password. In Password Keeper, a user can perform the following actions:

- Type a password and its identifying information (for example, which app or service the password is for), and save the information

- Generate secure random passwords that contain numbers, letters, and symbols and improve password strength

- Copy passwords and paste them into an app or a password prompt for a website

- Create backup files by exporting Password Keeper records into an encrypted (PKB2) or non-encrypted (CSV) file and securely store them where they want, for total control

- View a password strength meter when choosing their master password or entering new passwords to store, based on a proprietary algorithm that also considers commonly used passwords

The first time that a user opens Password Keeper on their device, they must create a master password for the app. When they sign into Password Keeper after the initial setup, they have 10 attempts to enter the correct master password. After the tenth incorrect attempt, Password Keeper wipes all stored password information from the device. Limiting incorrect master password attempts to 10 not only stops an attacker from having too many chances to guess a user's password, but also protects Password Keeper data from brute-force attacks while it's stored on the device. Password Keeper also offers extra protection for a user's sensitive data by not allowing screen shots when Password Keeper is open.

Password Keeper randomly generates a master key to lock and unlock Password Keeper data using AES-256 encryption. It also randomly generates a separate key to verify the encrypted data's integrity, ensuring that the data remains uncorrupted. The master password that the user sets for the app, combined with randomly generated data, protects the master key, which means that Password Keeper data can't be decrypted without the master password.

Remote device management apps

PRIV supports remote device management apps, such as Android Device Manager, that allows a user to safeguard their device and data in situations where the device is lost or stolen. A remote device management app typically provides a user with several options to locate their device. If the user can't locate their device, stronger steps can keep the data safe from an unauthorized user.

To locate a lost device, remote device management apps may allow a user to:

- View the current location of the device on a map
- Make the device ring, even if it's in silent mode
- Display a phone number or custom message on the locked device to provide contact instructions

To protect a stolen device, remote device management apps may allow a user to:

- Remotely lock it
- Change the password
- Delete all of the data on the device

If the device is managed by an EMM solution, an administrator may also be able to perform these tasks.

Protection of data in transit

Because many of your employees work outside the office, any mobile solution you use must protect data in transit across your entire network.

Wi-Fi connections

PRIV can connect to Wi-Fi networks securely using industry-standard Wi-Fi protocols, including WPA2-Enterprise. PRIV supports multiple encryption and authentication methods including:

- 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

A device stores the encryption keys and passwords in an encrypted form. To connect to a Wi-Fi network, the device first authenticates and then sends data in an encrypted form using the authenticated connection.

If your devices are managed by an EMM solution, an administrator may be able to send sensitive Wi-Fi information, such as encryption keys, passwords, security settings, and any required certificates, to a device so that it can connect to your Wi-Fi network.
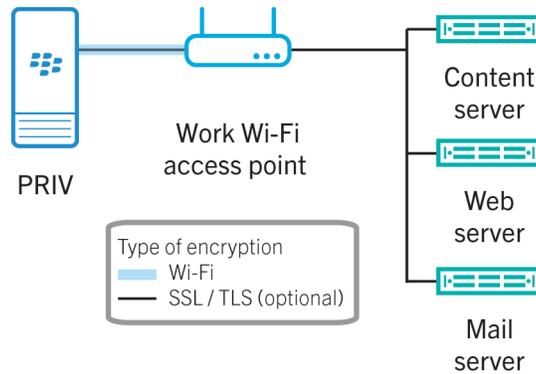
Wi-Fi authentication

When PRIV authenticates with the network, it uses a dual-layered connection, which gives the credentials an extra layer of protection. The outer authentication method of EAP protects the connection tunnel. Device credentials are sent within the tunnel and protected with the inner authentication method. When a device uses EAP authentication with a username and password, we recommend that a valid server certificate be configured so that the device can validate the Wi-Fi network that it's connecting to.

When the device opens a Wi-Fi connection using WPA-Enterprise or WPA2-Enterprise security, it can use the following authentication methods:

Cryptographic protocol	Encryption	Outer EAP method	Inner EAP method
WPA2	TKIP, AES-CCMP	PEAP, EAP-TTLS, EAP-FAST, EAP-TLS, EAP-AKA, EAP-SIM	MS-CHAPv2, EAP-GTC, PAP

Wi-Fi encryption

PRIV connects to your organization's resources through a Wi-Fi connection that an administrator sets up. Wi-Fi is used if the wireless access point was set up to use it.

VPN

PRIV supports a number of native and third-party VPN solutions to provide secure connectivity to your organization's network from the outside:

- PPTP with user authentication by password

- L2TP/IPSec with user authentication by password and device authentication by shared secret or RSA certificate

- IPSec with user authentication by password and device authentication by shared secret or RSA certificate

- BlackBerry Secure Connect Plus (when managed by BES12)

- VPN clients installed through Google Play™ or Google Play for Work from suppliers such as Checkpoint, Cisco, Fortinet, Juniper, OpenVPN, and Palo Alto Networks

PRIV supports per-user VPN on multiuser devices. VPNs are applied to each user to allow a user to route all network traffic through a VPN without affecting other users on the device. On an Android for Work device, an administrator can configure PRIV to route all work profile network traffic through a VPN without affecting other users on the device.

PRIV also supports always-on VPN so that apps can't access the network until a VPN connection is established. This prevents apps from sending data across other networks.

VPN encryption

The following diagram shows how data is encrypted when PRIV uses a VPN.
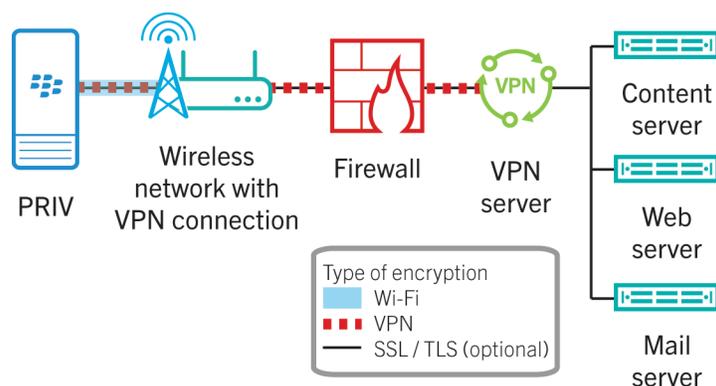
BlackBerry Secure Connect Plus

BlackBerry Secure Connect Plus is a BES12 component that provides a secure IP tunnel between work space apps on PRIV and your organization's network. This tunnel gives a user access to work resources behind your organization's firewall while ensuring the security of data using standard protocols and end-to-end encryption.

BlackBerry Secure Connect Plus and a device establish a secure IP tunnel when it's the best available option for connecting to the organization's network. If a device is assigned a Wi-Fi profile or VPN profile, and the device can access the work Wi-Fi network or VPN, the device uses those methods to connect to the network. If those options aren't available (for example, if the user is offsite and out of range of the work Wi-Fi network), then BlackBerry Secure Connect Plus and the device establish a secure IP tunnel.

Supported devices communicate with BES12 to establish the secure tunnel through the BlackBerry Infrastructure. One tunnel is established for each device. The tunnel supports standard IPv4 protocols (TCP and UDP). As long as the tunnel is open, any apps in the work profile can access network resources. When the tunnel is no longer required (for example, the user is in range of the work Wi-Fi network), it's terminated.

BlackBerry Secure Connect Plus offers the following advantages:

- The IP traffic that's sent between a device and BES12 is encrypted end-to-end, ensuring the security of work data.

- BlackBerry Secure Connect Plus provides a secure, reliable connection to work resources when a device can't access the work Wi-Fi network or VPN.

- BlackBerry Secure Connect Plus is installed behind your organization's firewall, so data travels through a trusted zone that follows your organization's security standards.

For more information about BlackBerry Secure Connect Plus, see http://help.blackberry.com/detectLang/bes12/current/administration/.

Certificates

A certificate is a digital document that binds the identity and public key of a certificate subject. Each certificate has a corresponding private key that's stored separately. A CA signs the certificate to verify that it can be trusted. Many certificates used for different purposes can be stored on PRIV.

PRIV can use certificates to:

- Authenticate using SSL/TLS when it connects to webpages that use HTTPS

- Authenticate with a work mail server

- Authenticate with a work Wi-Fi network and, for devices that support it, VPN

- Encrypt and sign email messages using S/MIME protection

Private keys are protected by BlackBerry Secure Compound. A user can import certificates into the device's certificate store. The certificates can be imported from various locations, including a computer, an email, or a smart card.

Certificates can be provided to a device in several ways. An administrator might need to distribute certificates to a device if the device uses certificate-based authentication to connect to a network or server in your organization, or if your organization uses S/MIME. An EMM solution may give you several options to send certificates to devices.

Bluetooth technology

Bluetooth technology allows a user to create a direct connection between PRIV and another Bluetooth device. Although files can be transferred over a Bluetooth connection, because of its ability to stream content, Bluetooth connections are more commonly used for actions such as playing the music on a device through a separate speaker or making calls from a headset that uses the device's mobile network connection.

A user must request a pairing with another Bluetooth device. Depending on the remote Bluetooth device, a user may also need to enter a passkey to complete the pairing. A device prompts the user each time a new device tries to set up a Bluetooth connection to their device. Device settings allow a user to decide what to allow Bluetooth devices to have access to on their device, such as contacts and messages.

PRIV enforces Security Mode 2 and Mode 4 (Level 2) and supports the following Bluetooth profiles:

- Hands-Free Profile 1.6

- Advanced Audio Distribution Profile 1.2

- Audio/Video Remote Control Profile 1.3

- Message Access Profile 1.1 (SMS & Email)

- Personal Area Networking Profile 1.0

- Multi Profile 1.0

- Human Interface Device Profile 1.0

- Device ID Profile 1.3

- Remote SIM Access Profile 1.0

- Object Push Profile 1.2

- Phone Book Access Profile 1.1

- BLE - GATT Profile

- BLE — HID over GATT Profile

If your devices are managed by an EMM solution, check the documentation for the EMM solution to see which Bluetooth controls it supports.

NFC

NFC is a short-range wireless technology that can be used for quickly creating connections between PRIV and another NFC-enabled device or NFC tag. With NFC a user doesn't need to enter pairing information to make a connection, so it's useful for on-the-go actions such as transferring contact cards with other people, or getting information from a poster that contains an NFC tag. Depending on wireless service providers and the apps that are installed on a device, NFC can also be used to turn a device into a digital wallet and allow a user to do things, such as make payments, with their device.

On PRIV, a user must authorize NFC-related activities on the device, such as browsing to URIs or accepting incoming file transfers over NFC.

If your devices are managed by an EMM solution, you may be able to control what devices can do with NFC. For example, you may be able to control whether a device can use NFC.

Platform security: End-to-end defenses

In addition to many device security features, PRIV also offers support for various EMM deployment models, data in transit protection, and plug-ins that help provide end-to-end security for devices and your organization's resources.

Secure device management

PRIV supports a number of options for enterprise management. Building on the hardware and platform security features provided by PRIV, the following management options are available:

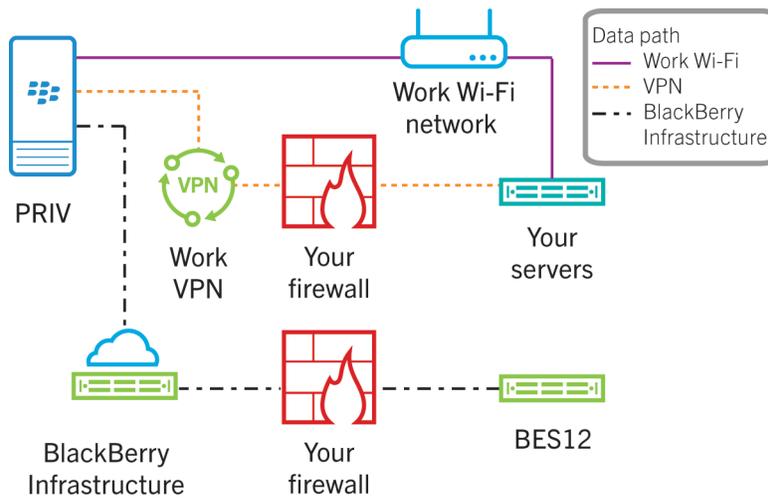| Management option	Description
MDM controls	A device can be managed using native Android IT administration commands and IT policy rules, or the administrative controls provided by BlackBerry specifically for PRIV. A separate work space isn't installed on the device and there's no added security for work data. During activation, a user must grant device administrator permissions to install the app. As part of this activation, it's possible that a VPN app (or equivalent) will be installed to manage secure network communication between PRIV and your organization's network. This is required to allow secure connectivity for email, calendar, contacts, and any additional apps that maybe pushed by the administrator.
Container	A device has an encrypted container that includes a separate file system for work apps and data. A user accesses the container through a container app and the container is typically protected by a password. The container separates work apps and data from personal apps and data and prevents any data leakage from the container to the personal space, unless explicitly enabled by an administrator. For example, for some containers, your organization can specify that a user can access personal contact information from inside the container. An EMM solution that supports Android devices and provides a container solution is required.
Android for Work: Profile Owner mode	A device has a work profile that's isolated on the device. An administrator can manage the work profile and your organization's policies apply only to the work profile. When a device is activated to use this Android for Work option, the activation process creates a work profile on the device. Work apps and data are isolated in the work profile.

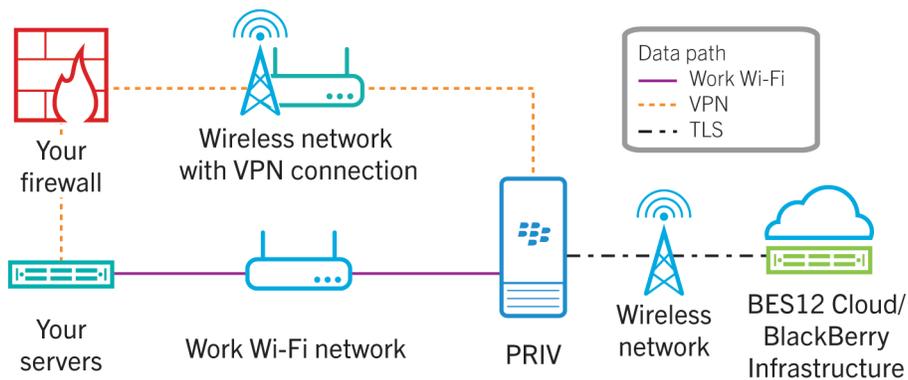| Management option	Description
	The work profile includes the following apps:
	• A device policy controller app that connects to the EMM server to receive management commands for the work profile
	• Email and organizer apps that you select for installation in the work profile
	• Google Play for Work where a user can download and install work apps that an administrator has approved
	• Work apps that you specify can run in the work profile. If a device has the same app installed outside the work profile, each instance of the app is kept separate from the other and operates under the rules and restrictions that apply inside or outside the work profile.
	• A VPN app that you select for installation and configuration in the work profile
	An EMM solution that supports Android for Work is required.
Android for Work: Device Owner mode	A device has a single profile that an administrator controls. An administrator can manage the entire device and your organization's policies apply to the entire device.
	When a device is activated to use this Android for Work option, the device policy controller app has full control of the device. Work apps and data are isolated in the work profile.
	The following apps are added to a device:
	• Device policy controller app that connects to the EMM server to receive management commands
	• Email and organizer apps that you select for installation on the device
	• Google Play for Work, where a user can download and install work apps that you've approved
	• Work apps that you permit a device to use
	• VPN app that you select for installation and configuration on the device
	An EMM solution that supports Android for Work is required.

Our end-to-end solution

BlackBerry offers complete end-to-end solutions that allow you to securely manage PRIV in your organization. You can choose to install BES12 in your organization's network, or register with our cloud EMM solution, BES12 Cloud.

The following diagrams and table describe the components that make up our solutions:

End-to-end solution using BES12

End-to-end solution using BES12 Cloud

Component	Description
PRIV	PRIV has a carefully controlled manufacturing process, and security applied to each level of the product, such as bootloader checks, OS checks, app authorization, and access control.
Wireless network	The wireless network provides the conduit for data flow between devices and your organization. Devices can use mobile, Wi-Fi, or VPN networks. Devices encrypt all data using AES encryption.
Your organization's firewall	Your organization's firewall controls access to your organization's network.
	For BES12, the BlackBerry end-to-end solution uses default port 3101 through your organization's firewall. Your administrator can set up the BlackBerry Router or TCP proxy in the DMZ, if required for additional security.
BES12	BES12 is our EMM solution that you can install in your organization's network. It allows you to activate and manage devices, manage apps, and control access to content. The connection between devices and BES12 is secured using TLS.
BES12 Cloud	BES12 Cloud is the EMM solution that BlackBerry hosts in our data centers. It allows you to activate and manage devices, manage apps, and control access to content. The connection between devices and BES12 Cloud is secured using TLS.
Your organization's servers	Your organization's servers are the content servers, mail servers, CAs, or other servers that host your organization's data or enhance your organization's security.

For more information about the security of BES12 see http://help.blackberry.com/detectLang/bes12/current/security/. For more information about the security of BES12 Cloud see http://help.blackberry.com/detectLang/bes12-cloud/latest/security/.

BlackBerry in the enterprise

BlackBerry offers many enterprise mobility solutions, including tools that provide secure file-sharing, identity management and protection, user authentication, and secure voice and data. Your organization can use these solutions with PRIV to provide users with secure, productive, and effective tools to get work done.

BBM Protected

BBM Protected adds an additional layer of security between devices to the existing BBM security model. BBM uses BBM Protected encryption for messages that are sent between BBM Protected users, inside or outside of your organization.

Protected Plus is an additional feature of BBM Protected that forces all of your users' chats to use BBM Protected, even if their recipients don't have BBM Protected turned on. After you turn on Protected Plus, BBM uses BBM Protected encryption for all messages in chats.

Because BBM Protected uses FIPS 140-2 validated cryptographic libraries and advanced ECC encryption, it's ideal for organizations in highly regulated environments that still want to allow their employees to keep in touch using an instant messaging app.
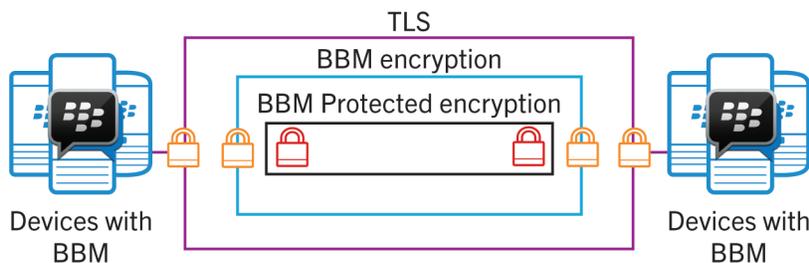
For more information about the security of BBM Protected, see http://help.blackberry.com/detectLang/bbm-protected-security/latest/.

BBM Meetings

BBM Meetings is a cloud-based collaboration tool that allows your users to schedule, host, and participate in meetings. It's optimized for a mobile experience and includes a mobile-friendly UI that allows a user to easily schedule and join meetings. A participant can join BBM Meetings from their device, phone, or computer.

BBM Meetings includes various enhanced features such as:

- A participant can switch to a meeting from an existing BBM chat, BBM Video chat, BBM Voice chat, or BBM group chat.

- A participant can share their screen, share documents, and create notes that everyone can see.

- A participant can easily join meetings by answering a call (no conference IDs or passcodes are required).

- Meetings can include HD video and voice conferencing for up to 25 participants.

WatchDox

WatchDox by BlackBerry is a secure, easy-to-use, file-sharing solution that was built from the ground up by a team of security experts. WatchDox provides device, computer, and web apps that allow a user to access, synchronize, and edit their files and folders and share them with others. All files are fully protected at all times. WatchDox also provides an administration console that allows an administrator to apply security controls and manage your organization's WatchDox service.

WatchDox offers many security features including:

- Granular document controls and permissions

- Watermarks on files to deter screen shots

- Ability to revoke, wipe, or expire file access at any time, even after a document has been downloaded or shared

- Tracking all document activities for compliance and audit, including who views, forwards, edits, or prints

- Encrypting each file with its own unique key, using FIPS 140-2 certified 256-bit AES encryption

For more information about WatchDox, see http://www2.watchdox.com/help/.

Enterprise Identity

Enterprise Identity by BlackBerry uses the BlackBerry Identity service in the BlackBerry Infrastructure to provide your organization with managed authentication and authorization services.

BlackBerry Identity is a service within the BlackBerry Infrastructure that provides an identity management platform that authenticates and authorizes a user for access to products and services. BlackBerry Identity allows a user to create a single BlackBerry ID to use with any supported product or service, including BBM, BlackBerry World, BlackBerry Protect, and Enterprise Identity.

You can use Enterprise Identity to provide employees and other users with a BlackBerry ID and control which cloud-based apps they have access to with that BlackBerry ID. You can also control the strength of the credentials that a user must provide for each service. A user can use their BlackBerry ID to gain single sign-on access to the cloud-based apps an administrator chooses, including BlackBerry services, such as BBM Meetings and BBM Protected, and SaaS apps, such as Box, Salesforce, and Workday.

Enterprise Identity offers many security features including:

- Never sharing company directory information with the cloud
- Not storing or sharing personally identifiable information
- Encrypted credential storage
- Unique user identifiers for each cloud app
- Bearer token holder identification
- Key rolling and storage

For more information about Enterprise Identity, see http://help.blackberry.com/detectLang/enterprise-identity/latest/.

VPN Authentication

VPN is one of the key methods that a user can use to access your organization's content when they're on the go. When you permit users to connect to your network from the outside, you must make sure that only authenticated users can access content freely. In the past, security conscious organizations implemented two-factor authentication using hardware tokens to strongly authenticate users. However, hardware tokens can be costly to implement, are difficult to use, and aren't well-aligned with mobility or cloud-based trends.

VPN Authentication by BlackBerry takes a different approach to VPN authentication. It uses PRIV as the second-factor for authentication. By using the device that a user has already activated, VPN Authentication provides the following benefits:

- Strong security based on PKI authentication and hardware Root of Trust
- Better user experience because a user doesn't need a hardware token and doesn't need to remember additional shared secrets or passcodes
- Improved cost structure because you can use something a user already has, reduce support costs, and you don't need to purchase or replace additional hardware

For more information about VPN Authentication, see http://help.blackberry.com/detectLang/vpn-authentication/.

SecuSUITE for Enterprise

SecuSUITE for Enterprise is an anti-eavesdropping solution that provides the highest level of security for voice and text messaging communications. SecuSUITE provides complete end-to-end protection against electronic eavesdropping and third-party attacks for all voice calls and text messages.

The SecuSUITE for Enterprise app for Android offers secure call and text messaging sessions that are hosted in the secure BlackBerry Infrastructure. All encryption and authentication processes run seamlessly and safely in the background on PRIV, without impacting phone quality, performance, or usability.

Your organization can implement their own security guidelines, so that all business-related data and processes on the device can be protected from electronic eavesdropping.

For more information about SecuSUITE, see http://help.blackberry.com/detectLang/secusuite-for-enterprise-app/.

BlackBerry: Your partner for Android security and privacy

BlackBerry provides the most secure Android platform for enterprises. However, security isn't only about having the best technology, it's about having a partner who lives and breathes security and can be trusted to look out for your enterprise security as well. Buying a PRIV means having the world-renowned BlackBerry security support infrastructure behind your business.

World-class product security

BlackBerry Product Security begins with our front-line responders. BlackBerry's Security Incident Response Team (BBSIRT) is the industry's gold standard in security incident response, ensuring that public and private reports of vulnerabilities are rapidly received, triaged, analyzed, and mitigated in order to protect your organization. An essential part of the daily work of BBSIRT includes collaborating with customers, partners, vendors, governments, academics, and the security research community, with a triage team monitoring the Android threat landscape 365 days a year from several top private and industry sources. This ongoing resource engagement helps BlackBerry deliver a unique level of security that customers depend on, by building collaborative relationships across the industry, responding rapidly to emerging incidents, and providing the guidance and tools customers need to protect their systems and devices.

The Security Research Group (SRG) within BlackBerry Product Security provides groundbreaking insights into both the hardware and software security we're developing and the malware and hacking tools constantly coming to light in the field. A global team of ethical hackers, their mandate is to ensure and extend the security of BlackBerry products and remove security-specific barriers to success related to product security. SRG identifies security issues in the BlackBerry product portfolio and works closely with development teams to get issues resolved. They also actively conduct research into advanced security threats to BlackBerry products and recommend defensive technologies.

Security patching

BlackBerry's security patching approach includes security maintenance releases and hotfixes.

Security maintenance releases

Each month, Google™ releases a security bulletin containing a list of recently discovered Android vulnerabilities to BlackBerry and other Android OEMs. BlackBerry will release these security maintenance releases (SMRs) to users that have purchased PRIV through shopblackberry.com and to PRIV resellers (carriers and other authorized dealers) that have agreed to participate in our regular SMR program and deliver our SMRs OTA to their subscribers.

Hotfixes

Some critical Android vulnerabilities, for example, one that can be easily and remotely exploited with a publicly disclosed method to execute "root" privileged malware, simply can't wait for a monthly SMR cycle. Depending on the severity of the problem, complexity of the fix, and timing relative to the SMR cycle, BlackBerry will opt to perform a hotfix, where the code to address only the specific critical problem is pushed to customers. Because a hotfix is typically limited in scope, the balance between a longer testing and approval process and the risk from the critical flaw makes this approach an important addition to helping keep users safe and secure. BlackBerry works with our partners on the approval and delivery of hotfixes.

Glossary

AES	Advanced Encryption Standard
AES-CCMP	Advanced Encryption Standard Counter Mode CBCMAC Protocol
BBSIRT	BlackBerry Security Incident Response Team
BLE	Bluetooth Low Energy
CA	certification authority
CBC	cipher block chaining
DDR	double data rate
DMZ	A demilitarized zone (DMZ) is a neutral subnetwork outside of an organization's firewall. It exists between the trusted LAN of the organization and the untrusted external wireless network and public Internet.
EAP	Extensible Authentication Protocol
EAP-AKA	Extensible Authentication Protocol Authentication and Key Agreement
EAP-GTC	Extensible Authentication Protocol Generic Token Card
ECC	Elliptic Curve Cryptography
EMM	Enterprise Mobility Management
eMMC	embedded MultiMediaCard
ESSIV	encrypted salt-sector initialization vector
FAST	Flexible Authentication via Secure Tunneling
FIPS	Federal Information Processing Standards
GATT	General Attribute Profile
HID	Human Interface Device
HMAC	keyed-hash message authentication code
HTTPS	Hypertext Transfer Protocol over Secure Sockets Layer
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
MAC	message authentication code
MDM	mobile device management
MS-CHAP	Microsoft Challenge Handshake Authentication Protocol

NFC	Near Field Communication
NVRAM	nonvolatile random access memory
OEM	original equipment manufacturer
OTA	over the air
PAP	Password Authentication Protocol
PBKDF2	password-based key derivation function 2
PEAP	Protected Extensible Authentication Protocol
PIN	personal identification number
PKI	Public Key Infrastructure
S/MIME	Secure Multipurpose Internet Mail Extensions
SaaS	Software as a Service
SHA	Secure Hash Algorithm
SIM	Subscriber Identity Module
SMR	Security Maintenance Release
SMS	Short Message Service
SRG	Security Research Group
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TTLS	Tunneled Transport Layer Security
URI	Uniform Resource Identifier
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access
UDP	User Datagram Protocol

Legal notice

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 BLACKBERRY 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 BLACKBERRY PRODUCTS OR SERVICES, DOWNTIME COSTS, LOSS OF THE USE OF BLACKBERRY 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 BLACKBERRY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, BLACKBERRY 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 BLACKBERRY AND ITS AFFILIATED COMPANIES, THEIR SUCCESSORS, ASSIGNS, AGENTS, SUPPLIERS (INCLUDING AIRTIME SERVICE PROVIDERS), AUTHORIZED BLACKBERRY 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 BLACKBERRY OR ANY AFFILIATES OF BLACKBERRY 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 BlackBerry'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 BlackBerry'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 BlackBerry and BlackBerry 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 BlackBerry.

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

BlackBerry Enterprise Software incorporates certain third-party software. The license and copyright information associated with this software is available at http://worldwide.blackberry.com/legal/thirdpartysoftware.jsp.

BlackBerry Limited
2200 University Avenue East
Waterloo, Ontario
Canada N2K 0A7

BlackBerry UK Limited
200 Bath Road
Slough, Berkshire SL1 3XE
United Kingdom

Published in Canada