Wi-Fi® enabled BlackBerry® smartphones

WLAN Support and Security Features
## Table of Contents

**Contents**

- Executive Summary ................................................................. 1
- Section One – BlackBerry Enterprise Solution Overview .............. 1
  - BlackBerry Enterprise Solution Architecture .......................... 2
  - The BlackBerry Enterprise Solution Security Model ................. 3
- Section Two – The BlackBerry Smartphone—Joining Wi-Fi and Cellular in One Device .......... 2
  - The BlackBerry smartphone Capabilities ................................. 2
  - Wi-Fi Security Features ...................................................... 8
- Glossary .................................................................................... 11
  - Appendix A: The BlackBerry Enterprise Solution Security Model 11
  - Appendix B: Glossary .......................................................... 14
Executive Summary

In the years since its launch, the BlackBerry® Enterprise Solution has proven itself to be an end-to-end cellular solution for the enterprise mobile user. Now, with the introduction of the Wi-Fi enabled BlackBerry smartphones, organizations can leverage capabilities, superb usability and centralized management over 802.11 a/b/g wireless LAN (WLAN) networks in addition to cellular networks. This paper provides an overview of BlackBerry platform functionality and a discussion of WLAN support and security features.

Section One – BlackBerry Enterprise Solution Overview

Wireless access to communications and information is no longer a luxury reserved for top executives — it is a business necessity for mobile workers and corridor warriors throughout your organization. The BlackBerry Enterprise Solution helps boost business performance by increasing overall productivity and allowing workers to make timely decisions based on the most accurate information available. The BlackBerry Enterprise Solution allows mobile users to access communications and information wirelessly, including:

Messaging and Collaboration Tools – Proven BlackBerry technology makes it easy for mobile workers to stay connected with colleagues and information:

- Email – Wirelessly extends enterprise email using automatic BlackBerry push delivery.
- Instant Messaging – Increase communication and collaboration with mobile access to enterprise instant messaging systems.
- Personal Information Management – Complete wireless synchronization of calendar, address book, tasks and notes keeps mobile workers up-to-date.

Enterprise Data – Enables wireless access to enterprise applications, intranets, data stores and back-end systems, including customer relationship management (CRM), sales force automation (SFA), field service automation (FSA), network and systems management (NSM), business intelligence and more.

Personal Productivity Tools – Users gain seamless access to information using best-in-class wireless smartphones that integrate:

- Phone
- Web
- MMS and SMS
- Multimedia Player
- Expandable Memory via Micro-SD
- GPS
- Voice Activated Dialing
Section Two: Wi-Fi enabled BlackBerry smartphones—Joining Wi-Fi and Cellular in One Device

Wi-Fi enabled BlackBerry smartphones brings WLAN-Mobile Convergence (WMC) to the enterprise, providing users with more choices on how and where to use their devices. WMC combines the strengths of both Wi-Fi and cellular networks to expand the functionality of BlackBerry smartphones. Wi-Fi offers high-speed, low latency capabilities of broadband connectivity without cables in the local area networks for the enterprise, home, and public hotspots. Mobile cellular networks provide wide area coverage, albeit with a more limited throughput. WMC allows users to take advantage of new services offered by carriers, such as UMA/GAN (described later in this document) and enterprise applications from the increased network capacity and coverage. The BlackBerry smartphone capitalizes on the widespread deployments of Wi-Fi infrastructure and the affordability and versatility of Wi-Fi technology. The BlackBerry smartphone leverages convergence as it brings broadband connectivity and provides the convenience of a single handset resulting in lower procurement and management costs.

Wi-Fi has rapidly developed in response to the demand to support converged applications and devices. Three key enablers of convergence emerge:

- **Quality of Service (QoS)**
  QoS enhances support for real-time applications such as voice or other multimedia, by making it possible to prioritize traffic from different applications.

- **Advanced power save mechanisms**
  Power save techniques significantly extends the battery life of Wi-Fi mobile devices and paves the way for the mass adoption of Wi-Fi in mobile phones and other devices with multiple wireless interfaces.

- **Security**
  Security standards and certifications for enterprise and public access devices bring advanced security to Wi-Fi devices, bringing the parity of security to mobile devices found in wired desktops and laptops.

The BlackBerry Smartphone Capabilities

The First Converged BlackBerry smartphone

When in Wi-Fi coverage areas, the BlackBerry smartphone utilizes the broadband connection to transmit and receive the data between the smartphone and the BlackBerry Enterprise Server. Whether browsing the Internet or intranets, accessing back-end applications or receiving PIM information, the BlackBerry smartphone exploits the increased capabilities of the Wi-Fi connection, reducing the time it takes to complete data transmissions. The larger, faster data connection afforded by Wi-Fi broadens the range of content and applications that can be accessed more quickly and efficiently by the BlackBerry smartphone. This includes video, large sets of data or other multimedia.

While connected to the BlackBerry Enterprise Server via a Wi-Fi connection, the BlackBerry smartphone has ability to complete data transactions while on a cellular voice call. This capability allows the user to be more productive during a phone call. For example, allowing the user to create/respond to email, check PIM, and carry on an enterprise messaging conversation or access corporate information on the Intranet all while on a conference call.
**Wi-Fi enabled BlackBerry smartphones:**
*A converged Wi-Fi and Cellular Device*

![Diagram of Wi-Fi enabled BlackBerry smartphones' connectivity to BlackBerry Enterprise Server](image)

**UMA/GAN Support**
The BlackBerry smartphone can use Wi-Fi where available and the cellular network nearly everywhere else. Some cellular carriers have the infrastructure and subscriber plans that support voice over Wi-Fi with Unlicensed Mobile Access (UMA). With the carriers that have deployed UMA, handover between the two networks can allow BlackBerry smartphone users to continue a conversation without even being aware that the phone has switched between Wi-Fi and cellular networks. The BlackBerry smartphone is designed to seamlessly switch to the cellular network when Wi-Fi is not available, without requiring subscriber intervention. The BlackBerry smartphone can also switch between networks if congestion occurs or if coverage diminishes. For example, at home or in the office, the BlackBerry smartphone can provide voice and data connectivity via Wi-Fi in areas with limited cellular coverage.

**IEEE Standards**
The BlackBerry smartphone leverages Wi-Fi frequency standards as published by the IEEE 802.11 working group. Providing dual band capabilities (2.4 GHz or 5 GHz), the BlackBerry smartphone offers organizations the flexibility to assign specific applications to different frequencies. For example, voice traffic is more sensitive to interference and latency than data. There are up to 23 non-overlapping channels available in 802.11a for the 5GHz range while there are only 3 non-overlapping channels available for 802.11b/g in the 2.4 GHz range. If voice over Wi-Fi is a major driver for mobility in the enterprise, the BlackBerry smartphone can be configured to use the 802.11a frequency and channels. Using 802.11a allows for a more flexible network design by allowing for many more overlapping coverage cells while avoiding co-channel interference with 802.11b and 802.11g, which operate in the increasingly crowded 2.4GHz range with just three non-overlapping channels. The many available channels used by 802.11a allow organizations to design for very dense, overlapping coverage.

The BlackBerry smartphone is compliant with regulatory requirements for international use. It supports IEEE 802.11d, which provides a mechanism for the Access Point (AP) to advertise regulatory information. It also supports IEEE 802.11h, which provides for radar detection and avoidance, Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC) requirements to ensure the coexistence of Wi-Fi and other types of radio frequency devices.
Wi-Fi enabled BlackBerry smartphones:  
A converged Wi-Fi and Cellular Device

Wi-Fi Alliance Certifications

Quality of Service
Due to the inherent shared media of Wi-Fi and the stringent requirements of certain applications, a Wi-Fi requires Quality of Service (QoS) capabilities. QoS enables Wi-Fi access points and client devices to prioritize traffic and optimizes the way shared network resources are allocated among different applications. Without QoS, all applications running on different devices have equal opportunity to transmit data. That works well for data traffic from applications such as web browsers or email, but it is inadequate for multimedia applications. For example, Voice over Internet Protocol (VoIP), is highly sensitive to latency, delay and jitter, and requires QoS. These QoS requirements are addressed by the BlackBerry smartphone by certifying with the Wi-Fi Alliance Wi-Fi Multimedia (WMM) program.

WMM is based on the EDCA (enhanced distributed channel access) mechanism defined by IEEE 802.11e. It prioritizes traffic demands from different applications and extends Wi-Fi’s high quality end-user experience from data connectivity to multimedia applications under a wide variety of environment and traffic conditions. WMM defines four access categories (voice, video, best effort, and background) that are used to prioritize traffic so that these applications have access to the necessary network resources. WMM adds prioritized QoS capabilities to Wi-Fi networks and optimizes their performance when multiple concurring applications, each with different latency and throughput requirements, compete for network resources. By using WMM, the BlackBerry smartphone user satisfaction is maintained in a wider variety of environments and traffic conditions. WMM makes it possible for enterprise network managers to decide which data streams are most important and assign them a higher traffic priority.

In a Wi-Fi network, WMM functionality requires that both the access point (AP) and the clients running applications that require QoS are certified for WMM and have WMM enabled. At the same time, it is important to realize that WMM-enabled devices can take advantage of their QoS functionality only when using applications that support WMM and can assign the appropriate priority level to the traffic streams they generate.

Power-Save
A major challenge to integrating Wi-Fi in mobile devices is the impact on battery life. BlackBerry solutions and smartphones have always been committed to best-of-breed battery life, and the BlackBerry continues this practice. The BlackBerry smartphone supports legacy IEEE 802.11 power-save modes as well as WMM-Power Save (WMM-PS) which is based on the Unscheduled Automatic Power Save Delivery (U-APSD) mechanism defined by IEEE 802.11e. WMM-PS addresses the challenge by offering advanced power management mechanisms that are optimized for mobile devices. It was introduced in answer to demand from manufacturers, application developers and service providers who want to take advantage of the opportunity that Wi-Fi mobile devices offer for new capabilities and services.

WMM-PS is a solution well suited to the dynamic environments where Wi-Fi is typically deployed and allows the client to trigger the delivery of all or some of the frames buffered by the access point during unscheduled service periods. It allows devices to spend more time in a “dozing” state, which consumes less power, while improving performance by minimizing transmission latency. U-APSD also enables more efficient and flexible over-the-air transmission and power management by enabling individual applications to control capacity and delay requirements. A VoIP application does not need high throughput, but it is extremely sensitive to delays. An increase in latency in a data application may result in an additional few seconds needed to download large emails or data files, or a longer time to load a web page, while in a VoIP application it can make the speech flow fragmented or the call altogether unintelligible. Increased latency is typically the side effect of power-save mechanisms that work well on data but that can be disruptive for VoIP applications. U-APSD utilizes a different approach that gives individual applications the ability to tailor network transmissions to specific requirements, without a significant impact on network latency.
Protected Setup
For the Wi-Fi home user, security is just as important as in the enterprise, especially if the home network is to be used for remote access to the enterprise. Due to complexity and lack of knowledge, many home users fail to adequately secure their Wi-Fi network. The Wi-Fi Alliance has recognized this issue and has instituted a certification program to reduce the barriers of setting up home Wi-Fi security. This program termed Wi-Fi Protected Setup, applies to typical home networks in which devices communicate via an access point (AP) or router. It does not support “ad hoc” networks in which devices directly communicate with one another, independently of an AP. The BlackBerry smartphone is certified to be compliant with Wi-Fi Protected Setup. The certification ensures the process can easily configure the network name (SSID) and WPA2 security key for the Access Point and Wi-Fi Protected Setup certified BlackBerry on a network. Wi-Fi Protected Setup’s simple, standardized approaches allow typical Wi-Fi users to set up and expand their Wi-Fi networks with security features enabled, even if they do not understand the underlying technologies or processes involved. Wi-Fi Protected Setup uses Wi-Fi Protected Access 2 (WPA2) Personal technology and is compatible with legacy devices that are certified for WPA/WPA2 Personal.

Additional Features and Capabilities

Scan for Networks
The BlackBerry smartphone has the ability to scan for available Wi-Fi networks that are within the range of the device, similar to the process recognizable on laptops. The BlackBerry smartphone has the capability to store profiles matching Wi-Fi networks. It periodically scans for Wi-Fi networks and can be configured to automatically connect to a network that matches a configured profile.

The BlackBerry smartphone also has a built-in wizard that allows the user to scan and authenticate to those Wi-Fi networks that are not pre-loaded in a profile or would not be known while away from the enterprise network, for example hotspots or municipal Wi-Fi locations.

Cisco Compatible Extensions (CCX)
With the Cisco® Compatible Extensions program, Wi-Fi client suppliers are certified against Cisco Wi-Fi technology innovations. The BlackBerry smartphone participates and is certified within the Cisco Compatible Extension program. The BlackBerry smartphone has implemented the required elements of the specification and has undergone extensive testing at an independent third party test lab. The testing helps to ensure support for innovative features developed by Cisco, as well as interoperability with Cisco Wi-Fi infrastructure products.

The Cisco Compatible Extensions program helps ensure that a broad range of Wi-Fi client devices interoperate with and support features of Cisco Wi-Fi infrastructure products. The Cisco Compatible Extensions program for Wi-Fi devices:

- Provides tested compatibility with licensed Cisco infrastructure innovations
- Accelerates the availability of features while maintaining interoperability through wireless standards
- Enables widespread availability of wireless devices that interoperate with Cisco Wi-Fi infrastructure products

Cisco provides pre-standard features through the Cisco Compatible Extensions program to fulfill customers’ enterprise application requirements. IT managers can confidently deploy their Wi-Fi networks, even if they serve different client device types, when Cisco Compatible client devices are used. The BlackBerry smartphone is certified to be compatible with version 3 of the program. Each subsequent version of the Cisco Compatible Extensions includes features of the previous versions. Below are a few of the features of the Cisco Compatible Extensions by version (list is not exhaustive).
Features of Cisco Compatible V1 include:

- Compliance with IEEE 802.11 and Wi-Fi Alliance
- Support for the 802.1X authentication type: Cisco LEAP
- Ability to interoperate with an access point that supports multiple Service Set Identifiers (SSIDs) tied to multiple VLANs, providing benefits such as flexible security schemes in a mixed client environment

Features of Cisco Compatible V2 include:

- Compliance with Wi-Fi Protected Access (WPA), including support for WPA Temporal Key Integrity Protocol (TKIP) encryption
- Support for the 802.1X authentication type: Protected EAP (PEAP) with EAP-GTC
- Fast, secure roaming through support of the 802.1X key management protocol: Cisco Centralized Key Management (CCKM)
- Radio frequency (RF) scanning, with scanned data sent to the access point for analysis and performance of RF management functions such as intrusion detection, assisted site survey, and detection of interference sources

Features of Cisco Compatible V3 include:

- Compliance with Wi-Fi Protected Access 2 (WPA2), including support for Advanced Encryption Standard (AES) encryption
- Support for the 802.1X authentication type: EAP-FAST
- Support for Wi-Fi Multimedia (WMM), a Quality of Service (QoS) standard defined by the Wi-Fi Alliance

Captive Portal Support

A captive portal is a Web-based authentication page that the user of a public-access or semi-private network is obliged to view and interact with before access is granted. Captive portals are typically used by business centers, airports, hotel lobbies, coffee shops, and other venues that offer free Wi-Fi hot spots for Internet users. A user connecting to one of these networks is required to launch their browser prior to gaining access to network services. Data traffic is filtered until the user is authorized and optionally authenticated by the captive portal. The BlackBerry smartphone has a Wi-Fi connection wizard that allows the user to complete this authentication during the profile setup process. Additionally, the BlackBerry® Browser allows for this authentication to be accessed on subsequent connections.

Native Wi-Fi Browser

The BlackBerry smartphone has the ability to utilize the Wi-Fi connection for a native browsing connection to the Internet. This alternative allows the BlackBerry smartphone to send and receive data directly without any enterprise server or BlackBerry Infrastructure interactions. Native browsing does not utilize the BlackBerry Infrastructure or BlackBerry Mobile Data System for the session, therefore data to and from the device is not optimized, compressed or encrypted. To take advantage of these capabilities and enable access an organization’s internal network resources, the BlackBerry smartphone would have to initiate an authenticated session with BlackBerry Mobile Data System.

Extensive Management via BlackBerry Enterprise Server IT Policies

To reduce the administrative tasks associated with device deployment and management, all BlackBerry smartphones incorporate numerous features to streamline deployment and management tasks. Cradle-less provisioning allows users to self-activate and provision their devices wirelessly, while IT administrators retain secure global control over assets, third party application distribution and deployment criteria. Enterprise-grade management reporting tools provide a solid platform for stable information exchange within organizations, thus requiring minimal IT involvement in routine tasks.
Wi-Fi enabled BlackBerry smartphones:
A converged Wi-Fi and Cellular Device

The BlackBerry platform provides a robust infrastructure that supports communication with BlackBerry smartphones. It does this over the cellular wireless or the protected enterprise Wi-Fi network through a secure connection from behind the firewall. It monitors BlackBerry users’ mailboxes for email, pushes data out to end users, and also manages data requests, messages, and organizer items that are submitted from the device. These capabilities ensure a rich, positive end user experience and provide seamless, uninterrupted workflow, wirelessly synchronizing organizer data and messages generated by the users’ enterprise accounts.

Wireless management of BlackBerry smartphones gives administrators an edge by helping to ensure that corporate security and best practices are maintained. Critical management functions, such as remote password setting, device locking and data wiping, can be performed wirelessly. End users can also self-provision their BlackBerry smartphone wirelessly without relying on a cradle. Administrators gain flexibility in supporting an extended workforce and reduced effort in maintaining the security and availability of corporate data.
Wi-Fi Security Features

Overview

The BlackBerry smartphone includes full support for IEEE 802.11i and all of the Wi-Fi security methods offered by the enterprise-grade Wi-Fi vendors. The range of Wi-Fi authentication and encryption features built into the BlackBerry smartphone helps ensure compliance with all the applicable Wi-Fi standards and certifications, but also affords security-conscious organizations the flexibility to choose the method that fits their security requirements. Figure 2, below describes the high-level process of a Wi-Fi client authenticating to a Wi-Fi. Depending on the authentication mechanism employed, differing levels of security and encryption methods are utilized. For example, when using an Extensible Authentication Protocol (EAP) method, the user is authenticated against a RADIUS server.

Also, some of the available Wi-Fi EAP authentication methods build a secure tunnel to provide a protected process to exchange credential information, drastically reducing the risk of attacks on authentication credentials. Within this secured tunnel, there are many options for exchanging client credentials, these options are commonly known as the inner authentication. It can also required that the Wi-Fi client is exchanging its credential with a trusted authentication server, therefore many of the EAP options provide the ability to ensure mutual authentication between client and authentication server (RADIUS or other AAA platform).

The BlackBerry smartphone also includes support for a number of mechanisms to reduce the overhead when roaming between APs on the same network. To do this, the device supports methods such as Cisco CCKM, PMK key caching and opportunistic keying, pre-authentication, and fast re-authentication (using RADIUS, if supported by the EAP method). These methods enable the device to have a seamless roaming experience between AP’s, reducing application timeout issues introduced by the re-authentication to different AP’s while mobile. This capability is especially critical for real time mobile communications, such as voice.

Table 1 below lists the Wi-Fi authentication options available on the BlackBerry smartphone out of the box, including the inner authentication methods supported on the device. To better understand which Wi-Fi security method is best suited for your environment, it is recommended to work with your Wi-Fi vendor and security organization to establish the appropriate Wi-Fi security policy.

Figure 2. - EAP Authentication
Wi-Fi enabled BlackBerry smartphones:
A converged Wi-Fi and Cellular Device

<table>
<thead>
<tr>
<th>Authentication Type</th>
<th>TLS Tunnel</th>
<th>Authentication Credentials</th>
<th>Mutual Authentication</th>
<th>Encryption Key Mgmt</th>
</tr>
</thead>
<tbody>
<tr>
<td>WEP</td>
<td>No</td>
<td>Static Key</td>
<td>No</td>
<td>None</td>
</tr>
<tr>
<td>LEAP</td>
<td>No</td>
<td>Username &amp; Password</td>
<td>Yes</td>
<td>802.1X WEP WPA – Enterprise (TKIP) WPA2 – Enterprise (AES)</td>
</tr>
<tr>
<td>PEAP</td>
<td>Yes</td>
<td>Username &amp; Password Token</td>
<td>Yes</td>
<td>802.1X WEP WPA – Enterprise (TKIP) WPA2 – Enterprise (AES)</td>
</tr>
<tr>
<td>EAP-TLS</td>
<td>Yes</td>
<td>Username &amp; Client Certificate</td>
<td>Yes</td>
<td>802.1X WEP WPA – Enterprise (TKIP) WPA2 – Enterprise (AES)</td>
</tr>
<tr>
<td>EAP-TTLS</td>
<td>Yes</td>
<td>Username &amp; Password</td>
<td>Yes</td>
<td>802.1X WEP WPA – Enterprise (TKIP) WPA2 – Enterprise (AES)</td>
</tr>
<tr>
<td>EAP-FAST</td>
<td>Yes</td>
<td>Username &amp; Password Token</td>
<td>Yes</td>
<td>802.1X WEP WPA – Enterprise (TKIP) WPA2 – Enterprise (AES)</td>
</tr>
<tr>
<td>EAP-SIM</td>
<td>No</td>
<td>SIM Card</td>
<td>Yes</td>
<td>802.1X WEP WPA – Enterprise (TKIP) WPA2 – Enterprise (AES)</td>
</tr>
</tbody>
</table>

Table 1. - Authentication Methods Available in BlackBerry smartphone

Secure Wi-Fi Data to the BlackBerry Infrastructure
If made available by the mobile network provider, BlackBerry smartphone users also have the ability to access the BlackBerry Infrastructure via a reliable and secure transport when using Wi-Fi connections. This ensures the user can be confident that their data communication is secured when using an un-trusted Wi-Fi network and the public Internet. When a user associates to a Wi-Fi network, a Secured Sockets Layer (SSL on port 443) tunnel will be created between the BlackBerry smartphone and the BlackBerry Infrastructure, protecting the communication throughout the unprotected networks. This allows access to the BlackBerry® Internet Service, PIN-to-PIN messaging, BlackBerry Enterprise Server services and BlackBerry® Messenger services all over a configured Wi-Fi connection.
Integrated VPN Client
A Virtual Private Network (VPN) differs from the previously presented Wi-Fi security methods in that the access point is only involved in encryption of data from the wireless client to access point. Past the access point, the data is unencrypted. A VPN provides strongly-encrypted “tunnel” from the client device, through the access network and onto the core enterprise network. A VPN is commonly used by organizations to provide remote users secure access to an enterprise network. The BlackBerry smartphone includes an optional, built-in VPN client for most of the industry-leading VPN solutions, shown in table 2. If the VPN client is utilized, it allows the BlackBerry smartphone to establish a protected connection to the enterprise network when associated with an “un-trusted” Wi-Fi network such as home network or Wi-Fi hotspot, utilizing the public Internet for access to the enterprise network. The optional VPN clients are integrated with the BlackBerry smartphone system software and do not require additional software to be purchased or deployed separately. By integrating the VPN into the BlackBerry smartphone, the VPN configuration and profile association can all be controlled and managed via the BlackBerry Enterprise Server IT policy settings. The VPN client can be assigned to specific Wi-Fi profiles (ie, Home or Hotspot) and automatically launched once the BlackBerry smartphone successfully associates to the Wi-Fi identified within a Wi-Fi profile.

### Table 2. - BlackBerry smartphone Integrated VPN Clients

<table>
<thead>
<tr>
<th>VPN Client</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Avaya® VSU™ Series</td>
</tr>
<tr>
<td>• Check Point® Software Technologies VPN-1</td>
</tr>
<tr>
<td>• Cisco® VPN Concentrator</td>
</tr>
<tr>
<td>• 3000 Series</td>
</tr>
<tr>
<td>• Cisco Secure PIX Firewall VPN</td>
</tr>
<tr>
<td>• Cisco IOS with Easy VPN Server</td>
</tr>
<tr>
<td>• Lucent Firewall Brick Family</td>
</tr>
<tr>
<td>• Netscreen Systems</td>
</tr>
<tr>
<td>• Nortel Networks Contivity VPN Switch Series</td>
</tr>
<tr>
<td>• Secure Computing® Sidewinder® Firewall</td>
</tr>
<tr>
<td>• Symantec™ Raptor Firewall and PowerVPN</td>
</tr>
</tbody>
</table>

Wi-Fi enabled BlackBerry smartphones

To find out which models of BlackBerry smartphones support Wi-Fi, please visit [http://na.blackberry.com/eng/atatglance/networks/#tab_ddetail_subtab_wifi](http://na.blackberry.com/eng/atatglance/networks/#tab_ddetail_subtab_wifi)
Appendices

Appendix A: The BlackBerry Enterprise Solution Security Model

Whether Wi-Fi or cellular networks are being used, security features and capabilities are built into the BlackBerry Enterprise Solution and help establish end-to-end security for all BlackBerry smartphones. Below is a description of the security features inherent to the BlackBerry Enterprise Solution.

See Section Two of this white paper for a discussion of Wi-Fi-specific security available on the BlackBerry smartphone.

BlackBerry Security Features for Wireless Data

End-to-end Wireless Encryption
The BlackBerry Enterprise Solution offers two transport encryption options, Advanced Encryption Standard (AES) and Triple Data Encryption Standard (Triple DES)* encryption, for all data transmitted between BlackBerry Enterprise Server and BlackBerry smartphones.

Private encryption keys are generated in a two-way authenticated environment and are assigned to each BlackBerry smartphone user. Each secret key is stored only in the user’s secure Microsoft® Exchange, IBM® Lotus® Domino® or Novell® GroupWise® mailbox and on their BlackBerry smartphone, and can be regenerated by the user wirelessly.

Data sent to the BlackBerry smartphone is encrypted by the BlackBerry Enterprise Server using the private key retrieved from the user’s mailbox. The encrypted information travels across the network to the device where it is decrypted with the key stored there.

RSA SecurID Authentication for Two-Factor Authentication
BlackBerry Mobile Data System services on the BlackBerry Enterprise Server support RSA SecurID authentication, providing organizations with additional authorization when users access application data or corporate intranets on their BlackBerry smartphones. BlackBerry Mobile Data System Services utilize RSA ACE/Agent® Authorization API 5.0 to interface to RSA ACE Servers®. When a user navigates to a site or application requiring authorization, they are prompted for their Username Token Passcode.

HTTPS for Secure Data Access
BlackBerry Mobile Data System services act as a security-enabled gateway between the wireless network and corporate intranets and the Internet. They leverage the AES or Triple DES* encryption transport and also enable HTTPS connections to application servers.

BlackBerry smartphones support HTTPS communication in one of two modes, depending on corporate security requirements:

- Proxy Mode: an SSL/TLS connection is created between the BlackBerry Enterprise Server and the application server on behalf of the BlackBerry smartphone. Data from the application server is then AES or Triple DES* encrypted and sent over the wireless network to the BlackBerry smartphone.
- End-to-End Mode: encrypts data over SSL/TLS for the entire connection between the BlackBerry smartphone and the application server, making End-to-End Mode connections most appropriate for applications where only the transaction end-points are trusted**.

© 2008 Research In Motion Limited. All rights reserved.
S/MIME Support Package for BlackBerry smartphones
For organizations that already make use of S/MIME (Secure Multipurpose Internet Mail Extensions) to protect their data, the BlackBerry solution has optional support for this protocol***. Leveraging an organization's existing S/MIME capabilities, the S/MIME Support Package for BlackBerry smartphones is designed to enable BlackBerry smartphones users to store and retrieve private and public keys so they can read, sign and encrypt S/MIME messages on the go.

PGP Support Package for BlackBerry smartphones
The PGP® Support Package† for BlackBerry smartphones is designed to augment the security features provided by the BlackBerry Enterprise Solution. The PGP Support Package for BlackBerry smartphones is third party software for BlackBerry smartphones that adds PGP Desktop and PGP Universal support. This support allows companies with existing PGP infrastructure in place to extend this infrastructure wirelessly using BlackBerry smartphones.

Lotus Notes Email Encryption Support‡
BlackBerry Enterprise Solution support for Lotus Notes® email encryption is designed to increase usability of the BlackBerry Enterprise Solution. BlackBerry® Enterprise Server v4.1 provides support for Lotus Notes Encryption so that BlackBerry smartphones are able to read Lotus Notes encrypted email.

BlackBerry Application Security - Code Signing and Digital Certificates
BlackBerry smartphone applications created using the BlackBerry® Java® Development Environment (BlackBerry JDE) which have certain functionality, such as the ability to execute on startup or to access potentially sensitive BlackBerry application data, require developers to sign and register their applications with Research In Motion (RIM). This adds protection by providing a greater degree of control and predictability to the loading and behavior of applications on BlackBerry smartphones. Additionally, the BlackBerry Signing Authority Tool can help protect access to the functionality and data of third party applications by enabling a corporate developer or administrator to manage to specific sensitive Applications Programming Interfaces (APIs) and data stores through the use of server-side software and public and private signature keys. To help protect a BlackBerry® MDS Studio Application from tampering, corporate developers can sign an application bundle with a digital certificate described by an alias. They can use either a trusted certificate authority (CA) or a generated (self-signed) certificate. BlackBerry MDS Studio generates and signs applications with certificates that are compliant with the Public Key Infrastructure (X.509) standard.

BlackBerry Smart Card Reader
The BlackBerry® Smart Card Reader is a lightweight, wearable smart card reader that makes it easier for personnel to meet operational requirements for using multifactor authentication with computers, BlackBerry smartphones, PKI applications and for secure web browsing—without negatively impacting the user experience. It is designed to meet strict public sector and IT requirements while enhancing the security posture of organizations.
BlackBerry Security Features for Stored Data

Strong IT Policy Enforcement and Management for BlackBerry Smartphones
The BlackBerry Enterprise Solution extends corporate security policies to BlackBerry smartphones and provides administrators with tools to manage these policies. To protect information stored on BlackBerry smartphones, password authentication can be made mandatory through the customizable IT policies of the BlackBerry Enterprise Server. By default, password authentication is limited to ten attempts after which the device’s memory is erased. Local encryption of all data (messages, address book entries, calendar entries, memos and tasks) can also be enforced via IT policy. And with the Password Keeper, password entries can be securely stored on the device (e.g. banking passwords, PINs, etc.) using AES encryption technology.

Additionally, system administrators can create and send wireless commands to remotely change BlackBerry smartphone passwords, and lock or delete information from lost or stolen BlackBerry smartphones.

BlackBerry Enterprise Server Permits Only Trusted Connections
The BlackBerry Enterprise Server does not store any email or data. To increase protection from unauthorized parties, there is no staging area between the server and the BlackBerry smartphone where data is decrypted. To further enhance the security features of the solution, the BlackBerry Enterprise Server is designed to allow only authenticated, outbound-initiated connections through port 3101 of the firewall. Unauthorized commands cannot be executed on the system because no inbound traffic is permitted from sources other than the BlackBerry smartphone or the email server. Only communications that can be decrypted with a valid encryption key are permitted between the server and the wireless network.

Security Certifications

BlackBerry smartphones feature advanced embedded encryption technology. As a result, the cryptographic software kernel in BlackBerry smartphones and the BlackBerry Enterprise Server have received the FIPS 140-2 validation, signifying their adherence to strict government security standards.

* Available for BlackBerry Enterprise Server for Microsoft Exchange and BlackBerry Enterprise Server for IBM Lotus Domino only.
** Certain features outlined require a minimum version of BlackBerry software.
*** Available for BlackBerry Enterprise Server for Microsoft Exchange only.
† PGP Support Package for BlackBerry devices is available only with BlackBerry Enterprise Server version 4.0 or higher for Microsoft Exchange or for IBM Lotus Domino, and requires BlackBerry Device Software v4.1 or higher.
‡ Available for BlackBerry Enterprise Server for IBM Lotus Domino only.
Appendix B: Glossary

**802.1x** - IEEE 802.1X is an IEEE standard for port-based network access control. It provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails.

**802.11a** - A revision to the IEEE standard that operates in the unlicensed 5 GHz band. 802.11a products have data rates up to 54 Mbps and must support 6, 12, & 24 Mbps.

**802.11b** - A wireless networking standard offering transmission speeds of up to 11 megabits per second (Mbps); it operates on three non-overlapping channels in the unlicensed 2.4 GHz radio frequency (RF) range.

**802.11e** - A standard that defines a set of Quality of Service enhancements for LAN applications, in particular the 802.11 standard. The standard is considered of critical importance for delay-sensitive applications, such as Voice over Wireless IP. The protocol enhances the IEEE 802.11 Media Access Control (MAC) layer.

**802.11d** - Wireless modulation configuration can be fine-tuned at the Media Access Control layer (MAC layer) level to comply with the rules of the country or district in which the network is to be used. Rules subject to variation include allowed frequencies, allowed power levels, and allowed signal bandwidth.

**802.11g** - A wireless networking standard offering transmission speeds of up to 54 Mbps; it operates on three non-overlapping channels at the 2.4 GHz RF range, and is backward compatible with 802.11b.

**802.11h** - Intended to resolve interference issues introduced by the use of 802.11a in some locations, particularly with military radar systems and medical devices.

**802.11i** - Is an amendment to the 802.11 standard specifying increased security mechanisms for wireless networks.

**802.11n** - In January 2004 IEEE announced that it had formed a new 802.11 Task Group to develop a new amendment to the 802.11 standard for wireless local-area networks. The data throughput is estimated to reach a theoretical 540 Mbit/s (which may require an even higher raw data rate at the physical layer), and should be up to 50 times faster than 802.11b, and well over 10 times faster than 802.11a or 802.11g.

**A**

**Access Points (APs)** - A layer-2 networking device that serves as an interface between the wireless network and a wired network and can control medium access. Access points combined with a distribution system (e.g. Ethernet) support the creation of multiple radio cells that enable roaming throughout a facility.

**AES** - The Advanced Encryption Standard is the new standard cryptographic algorithm for use by US government organizations to protect sensitive (unclassified) information.

**Authentication** - the process a station uses to announce its identity to another station.

**C**

**Call Admission Control (CAC)** - Set of actions taken by the network during the call set-up phase (or during call re-negotiation phase) in order to determine whether a connection request can be accepted or should be rejected (or whether a request for re-allocation can be accommodated).

**Cisco Centralized Key Management (CCKM)** - Using CCKM, authenticated Wi-Fi client devices can roam from one access point to another without any perceptible delay during reassociation.

**Counter-Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP)** - Wireless encryption protocol based on the Advanced Encryption Standard (AES) and defined in the IEEE 802.11i specification.
Wi-Fi enabled BlackBerry smartphones: A converged Wi-Fi and Cellular Device

D

**Delay** - The transfer delay is defined as the amount of time elapsed from the time a frame exits the source to the time it reaches the destination.

**Direct Sequence Spread Spectrum (DSSS)** - Combines a data signal at the sending station with a higher data rate bit sequence, which many refer to as a chip sequence (also known as processing gain). A high processing gain increases the signal’s resistance to interference.

**Dynamic Frequency Selection (DFS)** - A mechanism to allow unlicensed devices to share spectrum with existing radar systems.

E

**Enhanced Distributed Channel Access (EDCA)** - A mechanism to provide differentiated, distributed access for up to four access categories for each wireless station.

**Encryption** - The process of coding data so that a specific code or key is required to restore the original data, used to make transmissions secure from unauthorized reception.

**Extensible Authentication Protocol (EAP)** - The Extensible Authentication Protocol is a general protocol for authentication that supports multiple authentication mechanisms. EAP does not select a specific authentication mechanism at link control phase, but rather postpones this until the authentication phase. This allows the authenticator to request more information before determining the specific authentication mechanism. This also permits the use of a “back-end” server, which actually implements the various mechanisms while the PPP authenticator merely passes through the authentication exchange.

**Extensible Authentication Protocol Method for GSM Subscriber Identity Module (EAP-SIM)** - Is an EAP mechanism for authentication and session key distribution using the Global System for Mobile Communications (GSM) SIM card.


**Extensible Authentication Protocol-Tunneled Transport Layer Security (EAP-TTLS)** - Similar to PEAP in authenticating to a WLAN. EAP-TTLS does not require a client-side certificate.

**Ethernet** - A 10 Mbps LAN medium-access method that uses CSMA to allow the sharing of a bus-type network. IEEE 802.3 is a standard that specifies Ethernet.

F

**FAST** - is a two-phase Wi-Fi authentication protocol developed by Cisco. Phase 0, provision client with a credential called PAC (Protected Access Credentials). Phase 1, uses the PAC to establish a tunnel with the server and authenticate the username and password.

**Federal Communications Commission (FCC)** - The Federal Communications Commission (FCC) is an independent United States government agency, directly responsible to Congress. The FCC was established by the Communications Act of 1934 and is charged with regulating interstate and international communications by radio, television, wire, satellite and cable. The FCC’s jurisdiction covers the 50 states, the District of Columbia, and U.S. possessions.

G

**Gigahertz (GHz)** - One billion hertz.

I

**Institute of Electrical and Electronic Engineers (IEEE)** - A United States-based standards organization participating in the development of standards for data transmission systems. IEEE has made significant progress in the establishment of standards for LANs, namely the IEEE 802 series of standards.
**Internet Protocol (IP)** - A protocol that specifies the format of packets and how they are sent; it is often used in combination with TCP.

**IP telephony** - Transmission of voice calls over data networks that use IP.

**Jitter** - Jitter is a measure of the variability over time of the delay across a network. A very low amount of jitter is important for real-time applications using voice and video.

**Local Area Network (LAN)** - A data network that connects computers, peripherals, terminals, and other devices in a single building or other geographically limited area.

**Layer 2 access security** - Security provided by encryption on the 802.11 network through one or more encryption protocols used on the access point(s).

**Layer 3 access security** - Security provided at the application level within a data network. (for example, a VPN connection).

**Lightweight Extensible Authentication Protocol (LEAP)** - A protocol used for layer 2 access security through mutual authentication and the use of dynamic WEP keys; it is also called EAP-LEAP.

**ms** - Millisecond is one thousandth of a second.

**Man-in-the-middle (MITM)** - A man-in-the-middle is an attack in which an attacker is able to read, insert and modify at will, messages between two parties without either party knowing that the link between them has been compromised.

**Medium Access Control layer (MAC Layer)** - Provides medium access services for IEEE 802 LANs.

**Megahertz (MHz)** - One million cycles per second.

**Orthogonal Frequency Division Multiplexing (OFDM)** - A method of digital modulation in which a signal is split into several narrowband channels at different frequencies.

**Packet loss** - The loss of data in a packet based network, usually due to congestion and consequent buffer overflow.

**Pairwise Master Key (PMK) caching** - PMK Key Caching lets a station reuse previously-established encryption keys when roaming between APs that support this option.

**Pre-Authentication** - This is a feature that allows a mobile device to authenticate with other access points that it believes it may roam to in the future.

**Protected EAP (PEAP)** - Is a method to securely transmit authentication information, including passwords, over wired or wireless networks. PEAP uses only server-side public key certificates to authenticate clients by creating an encrypted tunnel between the client and the authentication server, protecting the exchange of authentication information.

**PSK (Pre-shared Key)** - A shared secret key used for layer 2 access security.

**Quality of Service (QoS)** - The concept of applying and ensuring specific, quantifiable performance levels on a shared network. The methods by which network traffic is prioritized, and on how the network is managed.

**Remote Authentication Dial In User Service (RADIUS)** - A protocol used for single point authentication of dialup systems, wireless LANs, and applications roaming within a wireless LAN, moving from one AP coverage area to another.
**Wi-Fi enabled BlackBerry smartphones:**
**A converged Wi-Fi and Cellular Device**

**RC4** - A widely deployed symmetric key stream cipher.

**Radio Frequency (RF)** - A generic term for radio-based technology.

**Roaming** - The process of moving from one access point to another without having to re-authenticate to the wireless network.

**S**

**Site survey** - The act of surveying an area to determine the contours of RF coverage in order to ensure proper wireless LAN operation through appropriate wireless LAN hardware placement.

**Service Set Identifier (SSID)** - A sequence of up to 32 letters or numbers that is the name of a wireless local area network.

**Subnet** - An interconnected, but independent segment of a network that is identified by its Internet Protocol (IP) address.

**T**

**TCP/IP** - Transmission Control Protocol/Internet Protocol are combined communication protocols used to connect hosts and transmit data on data networks.

**Temporal Key Integrity Protocol (TKIP)** - A protocol used by EAP to improve data encryption.

**Transmit Power Control (TPC)** - A mechanism used within 802.11h devices to prevent unwanted interference. The mechanism automatically reduces transmission output power when other networks are within range.

**U**

**Unscheduled Automatic Power Save Delivery (U-APSD)** - A feature that provides a dramatic improvement in talk time for battery-powered handsets.

**Unlicensed Mobile Access (UMA)** - Unlicensed Mobile Access (UMA) technology provides access to GSM and GPRS mobile services over unlicensed spectrum technologies, including Bluetooth and 802.11.

**V**

**VLAN** - The term VLAN was specified by IEEE 802.1Q; it defines a method of differentiating traffic on a LAN by tagging the Ethernet frames. It provides the ability to associate different LAN-attached workstations as being part of the same LAN independent of where the workstation is physically attached to the LAN.

**Voice over IP (VoIP)** - Voice calls over an IP network, also called IP telephony.

**Voice over WLAN (VoWLAN)** - VoIP calls over a wireless LAN

**Virtual Private Network (VPN)** - A network that uses access security to prevent unauthorized users from accessing the network and intercepting data.

**W**

**Wi-Fi®** - short for "Wireless Fidelity", is a set of product compatibility standards for wireless local area networks (WLAN) based on the IEEE 802.11 specifications. Trademarked by the Wi-Fi™ Alliance.

**Wi-Fi® Alliance** - Founded in 1999, this organization's charter is to certify interoperability of IEEE 802.11a/b/g products and to promote Wi-Fi™ as the global wireless LAN standard across all market segments.

**WMM** - Wireless Multimedia Extensions (WME), also known as Wi-Fi Multimedia (WMM) is a Wi-Fi Alliance interpretability certification, based on the IEEE 802.11e draft standard. It provides basic Quality of service (QoS) features to IEEE 802.11 networks. WMM prioritizes traffic according to 4 AC (Access Categories), however it does not provide guaranteed throughput.
**Wi-Fi enabled BlackBerry smartphones:**
**A converged Wi-Fi and Cellular Device**

**Wireless Multimedia Power Save (WMM-PS)** - Targets power consumption when using real time applications by increases the efficiency and flexibility of data transmission.

**WLAN** - A wireless LAN is one in which a mobile user can connect to a local area network (LAN) through a wireless (radio) connection. A standard, IEEE 802.11, specifies the technologies for wireless LANs.

**Wired Equivalent Privacy (WEP)** - A security protocol designed to provide the same level of security as that of a wired LAN.

**WPA** - Wi-Fi® Protected Access is the Wi-Fi Alliance's certification that uses the TKIP encryption method and EAP or PSK authentication.

**WPA2** - Wi-Fi® Protected Access 2 is the Wi-Fi Alliance’s certification that uses the CCMP & AES encryption method and EAP or PSK authentication.
Wi-Fi enabled BlackBerry smartphones:
A converged Wi-Fi and Cellular Device

*Check with service provider for availability, roaming arrangements and service plans. Certain features outlined in this document require a minimum version of BlackBerry Enterprise Server software, BlackBerry Desktop Software, and/or BlackBerry Device Software. May require additional application development. Prior to subscribing to or implementing any third party products or services, it is your responsibility to ensure that the airtime service provider you are working with has agreed to support all of the features of the third party products and services. Installation and use of third party products and services with RIM’s products and services may require one or more patent, trademark or copyright licenses in order to avoid infringement of the intellectual property rights of others. You are solely responsible for determining whether such third party licenses are required and are responsible for acquiring any such licenses. To the extent that such intellectual property licenses may be required, RIM expressly recommends that you do not install or use these products and services until all such applicable licenses have been acquired by you or on your behalf. Your use of third party software shall be governed by and subject to you agreeing to the terms of separate software licenses, if any, for those products or services. Any third party products or services that are provided with RIM’s products and services are provided “as is”. RIM makes no representation, warranty or guarantee whatsoever in relation to the third party products and services and RIM assumes no liability whatsoever in relation to the third party products and services even if RIM has been advised of the possibility of such damages or can anticipate such damages.

© 2007 Research In Motion Limited. All rights reserved. Research In Motion, the RIM logo, BlackBerry, and the BlackBerry logo, are registered with the U.S. Patent and Trademark Office and may be pending or registered in other countries. These marks, images and symbols are owned by Research In Motion Limited. All other brands, product names, company names, and trademarks are the properties of their respective owners. All other brands, product names, company names and trademarks are the properties of their respective owners.

The handheld and/or associated software are protected by copyright, international treaties and various patents, including one or more of the following U.S. patents: 6,278,442; 6,271,605; 6,219,694; 6,075,470; 6,073,318; D,445,428; D,433,460; D,416,256. Other patents are registered or pending in various countries around the world. Please visit www.rim.net/patents.shtml for a current listing of applicable patents.

This document is provided “as is” and Research In Motion Limited (RIM) assumes no responsibility for any typographical, technical or other inaccuracies in this document. RIM reserves the right to periodically change information that is contained in this document; however, RIM makes no commitment to provide any such changes, updates, enhancements or other additions to this document to you in a timely manner or at all. RIM MAKES NO REPRESENTATIONS, WARRANTIES, CONDITIONS OR COVENANTS, EITHER EXPRESS OR IMPLIED (INCLUDING WITHOUT LIMITATION, ANY EXPRESS OR IMPLIED WARRANTIES OR CONDITIONS OF FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, MERCHANTABILITY, DURABILITY, TITLE, OR RELATED TO THE PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE REFERENCED HEREIN OR PERFORMANCE OF ANY SERVICES REFERENCED HEREIN). IN CONNECTION WITH YOUR USE OF THIS DOCUMENTATION, NEITHER RIM NOR ITS AFFILIATED COMPANIES AND THEIR RESPECTIVE DIRECTORS, OFFICERS, EMPLOYEES OR CONSULTANTS SHALL BE LIABLE TO YOU FOR ANY DAMAGES WHATSOEVER BE THEY DIRECT, ECONOMIC, COMMERCIAL, SPECIAL, CONSEQUENTIAL, INCIDENTAL, EXEMPLARY OR INDIRECT DAMAGES, EVEN IF RIM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, INCLUDING WITHOUT LIMITATION, LOSS OF BUSINESS REVENUE OR EARNINGS, LOST DATA, DAMAGES CAUSED BY DELAYS, LOST PROFITS, OR A FAILURE TO REALIZE EXPECTED SAVINGS.

This document might contain references to third party sources of information and/or third party web sites (“Third-Party Information”). RIM does not control, and is not responsible for, any Third-Party Information, including, without limitation the content, accuracy, copyright compliance, legality, decency, links, or any other aspect of Third-Party Information. The inclusion of Third-Party Information in this document does not imply endorsement by RIM of the third party in any way. Any dealings with third parties, including, without limitation, compliance with applicable licenses and terms and conditions, are solely between you and the third party. RIM shall not be responsible or liable for any part of such dealings.