



BlackBerry Smart Card Reader Security

Release 1.0

White Paper

Contents

BlackBerry Smart Card Reader.....	3
BlackBerry Enterprise Solution.....	3
Support for Bluetooth wireless technology.....	3
Application control.....	4
BlackBerry security.....	4
Bluetooth IT policy rules.....	4
BlackBerry Smart Card Reader IT policy rules.....	5
BlackBerry Smart Card Reader security.....	5
Secure pairing.....	6
BlackBerry Smart Card Reader password.....	7
BlackBerry Smart Card Reader upgrades.....	7
Examples of attacks prevented by the initial key establishment protocol.....	7
Examples of attacks prevented by the connection key establishment protocol.....	8
Bluetooth security.....	8
RAM only objects.....	9
Random number generation.....	9
Protecting the transport layer.....	9
Related resources.....	10
Appendix A: Cryptosystem parameters.....	10
Appendix B: Initial key establishment protocol algorithms.....	11
Appendix C: Initial key establishment protocol process.....	11
Appendix D: Connection key protocol establishment process.....	12
Appendix E: Transport protocol.....	13
Appendix F: Types of attacks.....	14

BlackBerry Smart Card Reader

The BlackBerry Smart Card Reader™ for BlackBerry® devices with the Secure Multi-Purpose Internet Mail Extension (S/MIME) Support Package is an accessory that, when used in proximity to certain Bluetooth®-enabled BlackBerry devices, integrates smart card use with the BlackBerry Enterprise Solution™. The BlackBerry Smart Card Reader is designed to communicate wirelessly with Bluetooth® version 1.1 (or later)-enabled BlackBerry devices using the Advanced Encryption Standard (AES) 256 encryption method on the transport layer, creating a reliable two-factor authenticated environment for granting access to BlackBerry and Public Key Infrastructure (PKI) applications without the use of passwords.

Through an Elliptic Curve Diffie-Hellman (ECDH) key exchange, the BlackBerry Smart Card Reader is designed to enable wireless digital signing and encryption of wireless email messages. All keys on the BlackBerry Smart Card Reader are stored only in RAM and are never written to flash memory. There is no password to contain the data (including the master key) on the BlackBerry Smart Card Reader.

BlackBerry Enterprise Solution

The BlackBerry Enterprise Solution is designed to use either the AES-256 or Triple Data Encryption Standard (DES) encryption algorithm to protect data while it is in transit between BlackBerry devices and the BlackBerry Enterprise Server™. All messages that BlackBerry devices send or receive are AES-256 or Triple DES encrypted. This encryption verifies that a BlackBerry message remains protected in transit to the BlackBerry Enterprise Server while it is outside the corporate firewall.

The BlackBerry Enterprise Server is designed to establish a secure, two-way link between the user's email account and the user's supported BlackBerry device. The BlackBerry Enterprise Server is designed to provide security features that help to preserve the confidentiality, integrity, and authenticity of your corporate data. The BlackBerry Smart Card Reader is designed so that it cannot communicate with the BlackBerry Enterprise Server directly. When the BlackBerry device pushes an IT policy to the BlackBerry Smart Card Reader, the BlackBerry Smart Card Reader preserves the BlackBerry Enterprise Server signature on the IT policy.

Support for Bluetooth wireless technology

BlackBerry devices that use Bluetooth wireless technology are designed to establish a wireless connection with other Bluetooth-enabled devices, such as a hands-free car kit or wireless headset, that are within an approximate 10-meter range of these BlackBerry devices.

Bluetooth profiles specify how applications on the Bluetooth-enabled BlackBerry devices and on other Bluetooth devices connect and are interoperable. The user implements the Bluetooth Serial Port Profile on Bluetooth-enabled BlackBerry devices to establish a serial connection between the device and a Bluetooth peripheral using a virtual serial port. The Bluetooth peripheral accesses the serial port through the BlackBerry Software Development Kit.

Bluetooth wireless technology is considered a non-secure wireless channel. Bluetooth-enabled BlackBerry devices running BlackBerry Handheld Software version 4.0 or later are designed by Research In Motion® (RIM®) to provide the following security measures:

- By default, the Bluetooth wireless radio is turned off on the BlackBerry device.
- Users must request a connection or pairing of the Bluetooth-enabled BlackBerry device with a Bluetooth device. Users must also type a password (called a passkey) to complete the pairing.
- By default, the BlackBerry device is prompted each time a Bluetooth-enabled device attempts to connect to the BlackBerry device.
- Users can specify whether Bluetooth connections with the BlackBerry device are encrypted. The passkey, a shared secret key, is used to encrypt data that the user enters.

You can use IT policies that are designed to provide the following security measures:

- simultaneously manage all Bluetooth-enabled BlackBerry devices
- prevent BlackBerry devices from establishing a connection to another Bluetooth-enabled BlackBerry device, or from connecting to another Bluetooth-enabled device

Application control

If you are running BlackBerry Enterprise Server Software version 4.0 or later, you can use IT policy to control how third-party applications connect to the Bluetooth-enabled BlackBerry device through the BlackBerry Smart Card Reader by performing the following actions:

- permit or prevent third-party applications from being downloaded onto BlackBerry devices
- create application control policies that define which features (for example, email, phone, and BlackBerry device key store) third-party applications can access on the BlackBerry device and the types of connections that a third-party application on the BlackBerry device can establish (for example, opening network connections inside the firewall)
- assign application control policies, which specify the third-party applications that the user can download onto a BlackBerry device
- send third-party applications to BlackBerry devices wirelessly

See the *BlackBerry Enterprise Server Handheld Management Guide* for more information.

Application control for third parties is designed to limit the use of Bluetooth wireless technology (and the Bluetooth profiles) to specific, permitted applications. If you want to limit the use of Bluetooth wireless technology by applications on the BlackBerry device, configure application control so that all Bluetooth profiles are unavailable for applications by default. You can then turn on the Bluetooth Serial Port Profile for the BlackBerry Smart Card Reader driver only. The necessary applications are enabled to use the driver. An unauthorized application, such as a game, cannot use the driver.

Users cannot load third-party applications onto the BlackBerry Smart Card Reader. Code signing on the BlackBerry Smart Card Reader allows users to load only RIM code on the BlackBerry Smart Card Reader. When RIM manufactures the BlackBerry device, it installs a public key into the secure boot ROM of the BlackBerry Smart Card Reader. The corresponding private key is used to sign the BlackBerry Smart Card Reader operating systems. When an operating system and Java™ Virtual Machine are loaded onto the BlackBerry Smart Card Reader, the boot ROM verifies the signature on the loaded operating system to verify that RIM approves it. If the boot ROM determines that the signature is not valid, it rejects the operating system.

BlackBerry security

RIM created the BlackBerry Enterprise Solution (consisting of a BlackBerry device, the BlackBerry Handheld Software, and the BlackBerry Enterprise Server) with corporate data security in mind. By encrypting data using a strong encryption algorithm and verifying that data remains encrypted in transit between the BlackBerry Enterprise Server and the BlackBerry device, the BlackBerry Enterprise Solution is designed to preserve the integrity, confidentiality, and authenticity of your corporate data.

Bluetooth IT policy rules

Using the BlackBerry Manager for BlackBerry Enterprise Server Software version 4.0 or later, you can configure the behaviour of Bluetooth-enabled BlackBerry devices using the following IT policy rules:

- **Disable Bluetooth:** turns off support for Bluetooth wireless technology
- **Disable Handsfree Profile:** prevents the use of the Bluetooth Hands Free Profile, which is required to enable wireless voice capabilities with most car kits and some headsets

- **Disable Headset Profile:** prevents the use of the Bluetooth Headset Profile, which is required to enable wireless voice capabilities with most headsets and some car kits
- **Disable Pairing:** prevents the ability to establish a relationship—or pair—with another Bluetooth-enabled device
- **Disable Serial Port Profile:** prevents the use of the Bluetooth Serial Port Profile, which is required for establishing a serial connection between the BlackBerry device and a Bluetooth peripheral using a serial port interface

BlackBerry Smart Card Reader IT policy rules

Using the BlackBerry Manager for BlackBerry Enterprise Server Software version 4.0 Service Pack 2 (with the S/MIME IT Policy template imported) or BlackBerry Enterprise Server Software version 4.0 Service Pack 3 or later, you can configure the behavior of the BlackBerry Smart Card Reader using the following IT policy rules:

- **Maximum BlackBerry Disconnected Timeout:** specifies the maximum time, in seconds, that the Bluetooth connection between a BlackBerry device and a BlackBerry Smart Card Reader can remain disconnected, before the Bluetooth pairing information is deleted from the BlackBerry device
- **Maximum BlackBerry Inactivity Timeout:** specifies the maximum time, in minutes, that a connection between a BlackBerry device and a BlackBerry Smart Card Reader can remain inactive before the Bluetooth pairing information is deleted from the BlackBerry device
- **Maximum Connection Heart Beat Period:** specifies the maximum heartbeat period required to establish a connection to the BlackBerry Smart Card Reader
- **Maximum Long Term Timeout:** specifies the maximum time, in hours, after the Bluetooth connection between a BlackBerry device and a BlackBerry Smart Card Reader is terminated, before the Bluetooth pairing information is deleted from the BlackBerry device
- **Maximum Number of BlackBerry Transactions:** specifies the maximum number of packets that the BlackBerry device can receive before the Bluetooth pairing information is deleted from the BlackBerry device
- **Maximum Smart Card Not Present Timeout:** specifies the maximum time, in seconds, that the smart card can be removed from the BlackBerry device before the Bluetooth pairing information is deleted from the BlackBerry device
- **Maximum Bluetooth Range:** specifies the maximum power level, as a value between 0 (shortest range) and 7 (longest range), used to transmit Bluetooth packets from the BlackBerry Smart Card Reader

Note: The BlackBerry Smart Card Reader also recognizes the IT policy rule Disable Radio When Cradled, which controls whether the wireless radio is turned off when the BlackBerry device is connected to USB peripherals. If this policy rule is enabled, the Bluetooth wireless radio of the BlackBerry Smart Card Reader is turned off whenever the BlackBerry Smart Card Reader is connected to a computer using USB.

See the *IT Policy Reference Guide* for more information.

BlackBerry Smart Card Reader security

The BlackBerry Smart Card Reader is designed to provide strong authentication to prevent offline and online dictionary attacks. The BlackBerry Smart Card Reader uses a process designed to pair the BlackBerry Smart Card Reader with the Bluetooth-enabled BlackBerry device and pair the BlackBerry Smart Card Reader with the smart card using a secure pairing key. The BlackBerry Smart Card Reader creates a master encryption key from the secure pairing key and a secret private key that the BlackBerry Smart Card Reader chooses.

Secure pairing

When you attempt an action on the BlackBerry device that requires the use of the smart card, such as importing certificates, signing or decrypting a message, or initializing two-factor authentication, the BlackBerry Smart Card Reader automatically initiates the secure pairing procedure. You can manually initiate secure pairing through the BlackBerry Smart Card Reader Options screen.

Before you initiate a secure pairing, you must complete the Bluetooth pairing of the BlackBerry Smart Card Reader with the BlackBerry device. For the Bluetooth pairing to begin, you must add the BlackBerry Smart Card Reader to the BlackBerry device.

In BlackBerry Handheld Software 4.0.2 and later versions, you have the following options:

- completing the Bluetooth pairing manually
- initiating the BlackBerry Smart Card Reader addition to the BlackBerry device automatically when you initiate a secure pairing

If the BlackBerry device is running BlackBerry Handheld Software 4.0.0, you must add the BlackBerry Smart Card Reader manually. See the *BlackBerry Smart Card Reader Getting Started Guide* for more information.

Perform a Bluetooth pairing

If you have already added the BlackBerry Smart Card Reader, proceed to "Perform a secure pairing" below.

1. Perform one of the following actions.
 - If you are using BlackBerry Handheld Software version 4.0.2, click **Options > BlackBerry Smart Card Reader**.
 - If you are using BlackBerry Handheld Software version 4.1, click **Options > Security Options > Smart Card > BlackBerry Smart Card Reader > Driver settings**.
2. Press the **Action** button on the BlackBerry Smart Card Reader.
3. In the BlackBerry Smart Card Reader options screen, type the address that appears on the BlackBerry Smart Card Reader LCD.
4. Click **OK**.
5. In the BlackBerry Smart Card Reader options screen, type the address that appears on the BlackBerry Smart Card Reader LCD.

Perform a secure pairing

If you initiated the secure pairing manually, you must go to the BlackBerry Smart Card Reader Options screen to complete this procedure.

Perform one of the following actions.

- If you completed the Bluetooth pairing on the BlackBerry Smart Card Reader options screen, type the secure pairing key that appears on the BlackBerry Smart Card Reader LCD.
- If you have completed the Bluetooth pairing manually,
 1. Press the **Action** button.
 2. Type the secure pairing key that appears on the BlackBerry Smart Card Reader LCD.

Note: You must complete a Bluetooth pairing only once. You must perform a secure pairing each time that the pairing information is deleted from the BlackBerry device.

You can configure multiple IT policy rules for the BlackBerry Smart Card Reader to control when the pairing information is deleted from the BlackBerry device. See the *IT Policy Reference Guide* for more information.

BlackBerry Smart Card Reader password

The first time that you press the Action button after the BlackBerry Smart Card Reader resets, a password (set to an unknown, random 32-character string) secures the BlackBerry Smart Card Reader. The password protects the encryption keys on the BlackBerry Smart Card Reader in the same way that the BlackBerry device password protects the data on the BlackBerry device. Any debugging tool or program that tries to connect to the BlackBerry Smart Card Reader over the USB connection cannot connect because it does not know the password. Ten unsuccessful password attempts erases the password and all BlackBerry Smart Card Reader data.

BlackBerry Smart Card Reader upgrades

If you want to upgrade the BlackBerry Smart Card Reader, you must first reset the BlackBerry Smart Card Reader, erasing the Bluetooth pairing information and the secure pairing key. See the *BlackBerry Smart Card Reader Getting Started Guide* for more information.

Examples of attacks prevented by the initial key establishment protocol

Attack type	Description
eavesdropping	<p>An eavesdropping event occurs when the attacker listens to the communication between the BlackBerry Smart Card Reader and the BlackBerry device. The goal of the attacker is to determine the master encryption key that the BlackBerry Smart Card Reader and the BlackBerry device share.</p> <p>To determine the master encryption key, the attacker must solve the ECDH problem. The ECDH problem is considered to be computationally infeasible.</p>
man-in-the-middle	<p>A man-in-the-middle attack occurs when the attacker intercepts and modifies messages in transit between the BlackBerry Smart Card Reader and the BlackBerry device. A successful man-in-the-middle attack results in each end not knowing that the attacker is sitting in the middle monitoring and changing traffic.</p> <p>Simple Password Exponential Key Exchange (SPEKE) is designed to prevent a man-in-the-middle attack through the use of a secure pairing password. For an attacker to successfully initiate a man-in-the-middle attack, the attacker must know the secure pairing key. The secure pairing key must be securely given only to the authorized user of the BlackBerry device and the BlackBerry Smart Card Reader and must be kept secret until after the protocol is complete.</p>
impersonating a BlackBerry device	<p>An impersonation of the BlackBerry device occurs when the attacker sends messages to the BlackBerry Smart Card Reader so that the BlackBerry Smart Card Reader believes it is communicating with the BlackBerry device. The attacker can only guess the secure pairing key. The BlackBerry Smart Card Reader creates a master encryption key from the secure pairing key and a secret private key that the BlackBerry Smart Card Reader chooses. The only way the attacker can compute the same master encryption key is to determine the secret private key held by the BlackBerry Smart Card Reader. To do this, the attacker must solve the discrete log problem, which is computationally infeasible, or initiate an online dictionary attack.</p>
impersonating a BlackBerry Smart Card Reader	<p>An impersonation of the BlackBerry Smart Card Reader occurs when the attacker sends messages to the BlackBerry device so that the BlackBerry device believes it is communicating with the BlackBerry Smart Card</p>

	Reader. The attacker can only guess the secure pairing key. The BlackBerry device constructs its master encryption key based on the secure pairing key and a secret private key that it chooses. The only way the attacker can compute the same master encryption key is to determine the secret private key held by the BlackBerry device. To do this, the attacker must solve the discrete log problem, which is computationally infeasible.
offline dictionary attack	An offline dictionary attack occurs when the attacker attempts all possible passwords and determines the correct password. The attacker can use any number of computational resources to determine the password. In theory, nothing limits the speed at which the attacker can force the password. SPEKE prevents a known offline dictionary attack through the use of a password (the secure pairing key).
online dictionary attack	An online dictionary attack is similar to an offline dictionary attack, but the attacker must rely on the BlackBerry device or the BlackBerry Smart Card Reader to determine if a key is the correct secure pairing key. The BlackBerry Smart Card Reader only supports one attempt to guess the secure pairing key. If the guess is incorrect, the BlackBerry Smart Card Reader changes the secure pairing key before the next attempt.
small subgroup attack	A small subgroup attack occurs when the attacker limits the key establishment protocol to generate master encryption keys from only a small subset of keys. To help prevent a small subgroup attack, the ECDH operations all use the cofactor in their calculations and verify that the result is not the point at infinity.

See "Appendix B: Initial key establishment protocol algorithms" on page 11 for more information.

Examples of attacks prevented by the connection key establishment protocol

Attack type	Description
man-in-the-middle	The ECDH protocol, combined with using the shared master key, prevents a man-in-the-middle attack. As long as the shared master key remains secret, this type of attack is computationally infeasible.
perfect forward secrecy	The ECDH protocol provides perfect forward secrecy, preventing the derivation of previous or subsequent encryption keys by the key that is protecting data. Each run of the ECDH protocol uses a unique and random ephemeral key pair to create the new connection key. Then, the key pair is discarded. Even if the ephemeral private keys from a particular protocol run are compromised, the connection keys from other protocol runs remain safe.

See "Appendix D: Connection key protocol establishment process" on page 12 for more information.

Bluetooth security

The existing protection of the Bluetooth wireless technology on the Bluetooth-enabled BlackBerry devices is enhanced in the BlackBerry Smart Card Reader. Visit <http://www.blackberry.com/knowledgecenterpublic/> for more information on Bluetooth security.

When the initial connection between the BlackBerry Smart Card Reader and the BlackBerry device takes place, the BlackBerry Smart Card Reader enters into discoverable mode long enough for the BlackBerry device to find it

and pair with it. After that pairing is complete, the BlackBerry Smart Card Reader is designed to enter discoverable mode if the Bluetooth pairing information is lost from the BlackBerry device or the BlackBerry Smart Card Reader. The BlackBerry device never enters into discoverable mode unless the user enables that feature.

The BlackBerry Smart Card Reader uses the Bluetooth Serial Port Profile only, enabling you to use application control to shut down all the other profiles and prevent third-party applications from using the BlackBerry Smart Card Reader.

The Bluetooth pairing process makes use of a random key (unlike the hard-coded keys that headsets and other Bluetooth peripherals use). The pairing process is always user-driven from the BlackBerry device. If a message prompts users to type a pairing password when they did not initiate the process, they know another device that they might not want to connect to initiated the pairing process. The pairing process helps prevent a passive attack in which an attacker attempts to find the PIN.

You can control the Bluetooth wireless radio power level on the BlackBerry Smart Card Reader using the IT policy rule Maximum Bluetooth Range. Setting the power level also controls the range of proximity between the BlackBerry Smart Card Reader and the BlackBerry device at which the Bluetooth connection terminates. The range value does not translate to a specific distance because the Bluetooth range is partially determined by the power level. The range value is also heavily influenced by environmental factors, including obstructions and electromagnetic radiation. As a general rule, the Bluetooth range at power setting $n+1$ is longer than the range at power setting n .

RAM only objects

There is no password to protect the sensitive data, such as the master key, that the BlackBerry Smart Card Reader contains. To help limit the risk of key disclosure, all keys on the BlackBerry Smart Card Reader are designed to be stored in RAM only; they are not written out to flash memory. To take the BlackBerry Smart Card Reader apart, the user must remove the battery thereby clearing all of the keys on the BlackBerry Smart Card Reader.

Random number generation

In any system that generates cryptographic keys, random number generation is crucial. In the BlackBerry Smart Card Reader, the following sources of entropy seed the random number generator.

1. RIM injects each BlackBerry Smart Card Reader with a random 64-byte seed at manufacturing time. This provides the BlackBerry Smart Card Reader with entropy before the wireless radio is turned on.
2. While the initial key establishment protocol and the connection key establishment protocol establish the keys, all sent and received packets are hashed with Secure Hash Algorithm (SHA) 512 and added to the entropy pool.
3. Each time keys are being negotiated during the initial key establishment protocol and the connection key protocol, the BlackBerry device sends a 64-byte random value to the BlackBerry Smart Card Reader. The BlackBerry Smart Card Reader adds this information to its random source.

These steps are performed in addition to the BlackBerry device random number generation process. See the *BlackBerry Security White Paper* for more information.

Protecting the transport layer

All data that is sent between the BlackBerry device and the BlackBerry Smart Card Reader is both encrypted and authenticated. The data is encrypted with AES 256 in cipher block chaining (CBC) mode by default, but the algorithm can be negotiated during the initial key establishment protocol. In addition, the data is also protected with a keyed hash message authentication code (HMAC) with SHA 512 by default, but the SHA algorithm can be negotiated during the initial key establishment protocol.

All of the keys used in the transport layer are derived from the shared connection key. See "Appendix E: Transport protocol" on page 13 for more information.

The keys protect the transport layer throughout the entire connection. When a connection ends, if the Bluetooth connection is lost, the keys must be renegotiated. A lost or terminated connection occurs if either the BlackBerry device or BlackBerry Smart Card Reader goes outside of a sufficient wireless coverage area or if the BlackBerry device wireless radio turns off for any reason. You can configure the Maximum Connection Heart Beat Period IT policy rule to control when the connection ends based on the secure heartbeat settings. Setting this IT policy rule can prevent wiping of pairing information if an attack attempts to keep the Bluetooth connection open on the BlackBerry Smart Card Reader for extended periods using a low-level Bluetooth heartbeat.

Related resources

Resource	Information
<i>BlackBerry Enterprise Server Administration Guide</i>	<ul style="list-style-type: none"> generating and changing master encryption keys enabling S/MIME encryption security best practices
<i>IT Policy Reference Guide</i>	<ul style="list-style-type: none"> IT policies
<i>BlackBerry Handheld Management Guide</i>	<ul style="list-style-type: none"> controlling third-party software applications application control IT policies
<i>BlackBerry Security White Paper</i>	<ul style="list-style-type: none"> preventing the decryption of information at an intermediate point between the BlackBerry device and the BlackBerry Enterprise Server or company LAN enabling you to manage security settings for all BlackBerry devices protecting data in transit between the BlackBerry device and BlackBerry Enterprise Server. algorithms provided by the RIM cryptographic application programming interface (Crypto API) TLS and WTLS standards that the RIM Crypto API currently supports memory scrub process that occurs on the BlackBerry device when content protection is enabled
<i>BlackBerry with the S/MIME Support Package User Guide</i> <i>BlackBerry with the S/MIME Support Package White Paper</i>	<ul style="list-style-type: none"> installing the S/MIME Support Package for BlackBerry devices managing certificates on the BlackBerry device and desktop computer setting S/MIME options for signing and encrypting messages sending and receiving S/MIME messages

Appendix A: Cryptosystem parameters

The BlackBerry device and the BlackBerry Smart Card Reader are designed to share the following cryptosystem parameters:

Parameter	Description
E(Fq)	The NIST-approved 521-bit random elliptic curve over Fq. This curve has a cofactor of 1.

Fq	A finite field of prime order q .
P	A point of E that generates a subgroup of $E(Fq)$ of prime order r .
xR	Represents elliptic curve scalar multiplication, where x is the scalar and R is a point on $E(Fq)$.
s	The secure pairing value that appears on the BlackBerry Smart Card Reader display.
S	The secure pairing value (s) converted to a point on $E(Fq)$.

All math operations are done in the group $E(Fq)$. This is the elliptic curve algorithm that the initial key establishment protocol uses.

Appendix B: Initial key establishment protocol algorithms

The initial key establishment process negotiates numerous algorithms for use in subsequent key exchanges. These algorithms include the elliptic curve for future ECDH exchanges and the encryption algorithm and hash algorithms used with the transport layer protection.

Algorithm type (in order of preference)	Algorithm
elliptic curve (default)	• 571-bit Koblitz Curve (EC571K1)
	• 521-bit Random Curve (EC521R1)
	• 283-bit Koblitz Curve (EC283K1)
	• 256-bit Random Curve (EC256R1)
	• 160-bit Random Curve (EC160R1)
encryption	• AES 256
	• AES 128
hash	• SHA 512
	• SHA 256
	• SHA 1

Appendix C: Initial key establishment protocol process

Each protocol begins with an initial echo to verify that both sides understand the protocols. To send an initial echo, the value 0xC1F34151520CC9C2 is transmitted in the echo.

1. The BlackBerry device sends an initial echo of the value to confirm a connection to a BlackBerry Smart Card Reader.
2. The BlackBerry Smart Card Reader receives the initial echo and replies with an echo transmission of the initial value.
3. The BlackBerry device receives the echo.
4. The BlackBerry device asks the BlackBerry Smart Card Reader for a list of supported algorithms.
5. The BlackBerry Smart Card Reader creates a list of all the supported algorithms (elliptic curves, cipher algorithms, and hashes).

6. The BlackBerry Smart Card Reader sends a list of the supported algorithms to the BlackBerry device.
7. The BlackBerry device processes the list to find a match with one of its own supported algorithms. If there is no match, the BlackBerry device sends an error to the BlackBerry Smart Card Reader and stops processing the list.
8. If there is a match, the BlackBerry device begins the key establishment by sending a pairing request using the selected algorithms and seed (64 bytes).
9. The BlackBerry Smart Card Reader verifies the selected algorithms.
10. The BlackBerry Smart Card Reader performs the following calculation:
 - picks a short term key
 - picks random y , $1 < y < r - 1$
 - calculates $Y = yS$
11. The BlackBerry Smart Card Reader sends Y to the BlackBerry device.
12. The BlackBerry device performs the following calculations:
 - picks a short term key
 - picks random x , $1 < x < r - 1$
 - calculates $X = xS$
 - calculates the master key (MK) using the following information:
 - $K = xY = xyS$
 - $H1 = \text{SHA512}(\text{sent packets})$
 - $H2 = \text{SHA512}(\text{received packets})$
 - $H = H1 + H2$
 - $MK = \text{SHA256}(H || K)$
13. The BlackBerry device sends X to the BlackBerry Smart Card Reader.
14. The BlackBerry Smart Card Reader calculates MK using the following information:
 - $K = yX = yxS$
 - $H1 = \text{SHA512}(\text{sent packets})$
 - $H2 = \text{SHA512}(\text{received packets})$
 - $H = H1 + H2$
 - $MK = \text{SHA256}(H || K)$

Appendix D: Connection key protocol establishment process

The BlackBerry device and the BlackBerry Smart Card Reader share a master key. For the BlackBerry device and the BlackBerry Smart Card Reader to transmit data, a connection key needs to be established.

1. The BlackBerry device sends an initial echo of the value 0xC1F34151520CC9C2 to confirm a connection to a BlackBerry Smart Card Reader.
2. The BlackBerry Smart Card Reader receives the initial echo and replies with an echo transmission of the initial value.
3. The BlackBerry device receives the echo.
4. The BlackBerry device begins the key establishment using the negotiated algorithm and includes the selected algorithms, a seed, and another seed for the BlackBerry Smart Card Reader.

Note: P is defined on the curve negotiated in the initial protocol.
5. The BlackBerry Smart Card Reader performs the following calculation:
 - picks a short term key

- picks random y , $1 < y < r - 1$
 - calculates $Y = y^P$
6. The BlackBerry Smart Card Reader sends Y to the BlackBerry device.
 7. The BlackBerry device performs the following calculation:
 - picks a short term key
 - picks random x , $1 < x < r - 1$
 - calculates $X = x^P$
 - calculates the connection key (CK) using the following information:
 - $K = xY = xy^P$
 - $H1 = \text{SHA512}(\text{sent packets})$
 - $H2 = \text{SHA512}(\text{received packets})$
 - $H = H1 + H2$
 - $CK = \text{SHA256}(MK || H || MK || K)$
 8. The BlackBerry device sends X to the BlackBerry Smart Card Reader.
 9. The BlackBerry device performs a hashing function to calculate CK .
 10. The BlackBerry Smart Card Reader calculates the connection key using the following information:
 - $K = xY = xy^P$
 - $H1 = \text{SHA512}(\text{sent packets})$
 - $H2 = \text{SHA512}(\text{received packets})$
 - $H = H1 + H2$
 - $CK = \text{SHA256}(MK || H || MK || K)$

Note: The connection key establishment protocol can stop at any point if an error occurs. If an error occurs, an error code is sent to the other party. The following errors might occur:

- negative length
- bad packet
- incomplete crypto specification
- bad public key
- no algorithms in common are permitted
- not paired
- not connected
- connection error
- decryption error

Appendix E: Transport protocol

Each packet that is sent between the BlackBerry device and the BlackBerry Smart Card Reader is authenticated and encrypted by the following methods:

- authenticated with HMAC using the negotiated SHA algorithm
- encrypted with AES of the negotiated key size using CBC mode

4 bytes	8 bytes	4 bytes	Variable	Based on SHA	Variable
IV	Random padding	Counter	Payload	HMAC-SHA	PKC5 padding
Area authenticated by HMAC					
Area encrypted with AES-256					

Formatted packet anatomy – transport protocol

In the connection key protocol, a shared connection key CK is established from which all of the keys used in the transport layer are derived to protect all data transferred. The CK produces the following four keys:

- $KeySendEnc = SHA256(CK || S1)$
- $KeyRecEnc = SHA256(CK || S2)$
- $KeySendAuth = SHA256(CK || S3)$
- $KeyRecAuth = SHA256(CK || S4)$

Note: $S1$, $S2$, $S3$, and $S4$ are four hard-coded strings used to make sure the four calculated keys are different from each other.

$KeySendEnc$ is the AES-256 key used to encrypt data being transported from the BlackBerry device to the BlackBerry Smart Card Reader. Similarly, $KeyRecAuth$ is used with HMAC to authenticate all data transported from the BlackBerry Smart Card Reader to the BlackBerry device.

Appendix F: Types of attacks

If an attacker learns the secure pairing key s after the key establishment protocol is complete, the mathematical hardness of the discrete log problem protects the master key. To determine the master key, an attacker must determine one of x or y . After the initial key generation algorithm is complete, s no longer needs to remain secret.

An attacker who knows s before the key establishment protocol begins and passively watches the protocol cannot gain knowledge of the master key.

It is imperative that s remain secret until the key establishment protocol is successful. An active attacker who knows s before the key establishment protocol occurs can initiate a man-in-the-middle attack.

It is imperative that the secure pairing key (the password) be protected for the lifetime of the initial key establishment protocol.

Attack type	Details
eavesdropping	To succeed, the attacker must determine MK given only xS and yS . This calculation is equivalent to solving the DH problem.
man-in-the-middle	To succeed, the attacker must know the secure pairing key. The attacker must remain in the middle (between the BlackBerry device and the BlackBerry Smart Card Reader) forever, not just for the duration of the key establishment protocol, for a man-in-the-middle attack to occur.
impersonating a BlackBerry device	To succeed, the attacker must send $X = xP$ instead of xS to the BlackBerry Smart Card Reader. The BlackBerry Smart Card Reader calculates $K = yX = yxP$. To calculate the same key, the attacker must determine y from Y . The

	attacker might attempt this because the attacker does not know the secret s . This problem is considered to be computationally infeasible.
offline attack	To succeed, the attacker must attempt to send $X = xP$, instead of xS to the BlackBerry Smart Card Reader. The BlackBerry Smart Card Reader replies with $Y = xS$ and calculates $K = yX = yxP$. Meanwhile, the attacker calculates $K = xY = yxS = yxzP$, for some z such that $S = zP$. Given that information, the problem of determining yxP from $yxzP$ without knowledge of z corresponds to solving the discrete logarithm problem for S . This problem is considered to be computationally infeasible.
small subgroup attack	To succeed, the attacker attempts to force the key agreement to originate from a small set of values. For example if the attacker chooses X as the point at infinity, then K is the point at infinity regardless of what the BlackBerry Smart Card Reader chose for Y . By checking that X is not at the point of infinity, 1, or -1, this threat is averted.

Part number: SWD_X_BES(EN)-147.001

©2005 Research In Motion Limited. All Rights Reserved. The BlackBerry and RIM families of related marks, images, and symbols are the exclusive properties of Research In Motion Limited. RIM, Research In Motion, "Always On, Always Connected", the "envelope in motion" symbol, and BlackBerry are registered with the U.S. Patent and Trademark Office and may be pending or registered in other countries.

The BlackBerry device, the BlackBerry Smart Card Reader, 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; D445,428; D433,460; D416,256. Other patents are registered or pending in various countries around the world. Visit www.rim.com/patents.shtml for a current listing of applicable patents.

The Bluetooth word mark and logos are owned by the Bluetooth SIG, Inc. and any use of such marks by Research In Motion Limited is under license. Java is either a registered trademark or trademark of Sun Microsystems, Inc. in the United States and other countries. All other brands, product names, company names, trademarks and service marks are the properties of their respective owners.

This document is provided "as is" and Research In Motion Limited and its affiliated companies ("RIM") assume 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 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, hardware or software, products or services and/or third party web sites (collectively the "Third-Party Information"). RIM does not control, and is not responsible for, any Third-Party Information, including, without limitation the content, accuracy, copyright compliance, compatibility, performance, trustworthiness, 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 Information or the third party in any way. Installation and use of Third Party Information 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. Any dealings with Third Party Information, including, without limitation, compliance with applicable licenses and terms and conditions, are solely between you and the third party. You are solely responsible for determining whether such third party licenses are required and are responsible for acquiring any such licenses relating to Third Party Information. To the extent that such intellectual property licenses may be required, RIM expressly recommends that you do not install or use Third Party Information until all such applicable licenses have been acquired by you or on your behalf. Your use of Third Party Information shall be governed by and subject to you agreeing to the terms of the Third Party Information licenses. Any Third Party Information that is provided with RIM's products and services is provided "as is". RIM makes no representation, warranty or guarantee whatsoever in relation to the Third Party Information and RIM assumes no liability whatsoever in relation to the Third Party Information even if RIM has been advised of the possibility of such damages or can anticipate such damages.