



BlackBerry Wireless Enterprise Activation

Release 4.0

Technical Overview

Contents

Overview	2
About wireless enterprise activation	2
About the wireless enterprise activation password	2
Enabling wireless enterprise activation	2
Regenerating new master encryption keys	5
Enabling wireless data synchronization	5
Wireless service book updates.....	5
Understanding the BlackBerry key establishment protocols.....	6
Security benefits of the initial key establishment protocol.....	8
Security benefits of the BlackBerry key rollover protocol	9
Appendix A: BlackBerry initial key establishment protocol.....	10
Initialization	10
Activation	10
Appendix B: BlackBerry key rollover protocol	13

Overview

This document describes how administrators can enable wireless enterprise activation for users on the BlackBerry Enterprise Server™, and how users can initiate wireless enterprise activation from their handhelds. This document pays particular attention to the key establishment protocols that secure the connection between the BlackBerry Enterprise Server and the handheld. Finally, the security benefits are discussed.

About wireless enterprise activation

Wireless enterprise activation enables a user to remotely activate a handheld on the BlackBerry Enterprise Server without a physical network connection. Users must ensure that they are in an area with sufficient wireless coverage when the wireless enterprise activation is attempted. Wireless enterprise activation can also be used to deploy a large quantity of BlackBerry® handhelds.

For example, when remote users purchase new or replacement BlackBerry handhelds, they telephone their administrators. The administrators provide the activation passwords to the users over the telephone. Users then open the enterprise activation program, on their handhelds, enter the activation passwords and their corporate email addresses. Within a few seconds of the BlackBerry system beginning the activation protocol, the users are authenticated, the BlackBerry security parameters are negotiated, and users can send and receive email messages.

Using the BlackBerry Enterprise Server Management console, the administrator sets the activation password for the user.

About the wireless enterprise activation password

The activation password is only used once initially to activate the handheld. That is, once the user is successfully activated on the BlackBerry Enterprise Server, the password is no longer required. More importantly, the password cannot be re-used to establish another activation.

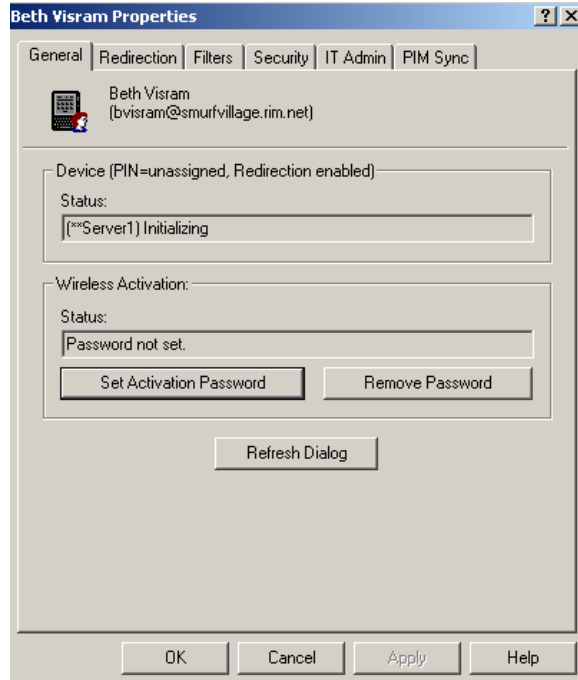
The protocol ensures that an online and an offline dictionary attack is not feasible; hence, the password can be short. Typical activation passwords are 4 to 8 characters long. The password should be no longer than 32 characters.

The passwords must be given securely to authenticated users perhaps via telephone or via internal email. If the users receive the password but have not activated their accounts on the BlackBerry Enterprise Server, then attackers with the passwords will be able to connect their handhelds to the BlackBerry Enterprise Server and assume the identities of the intended users.

Enabling wireless enterprise activation

1. **New BlackBerry handheld:** A user receives or purchases a new BlackBerry and contacts the IT department to activate it.
2. **Administrator creates the password:** The administrator sets the password on the user's account in the BlackBerry Manager by clicking **Set Activation Password** on the General tab, in the user properties dialog box, and entering the password in the **Activation Password** field. The administrator then communicates the password to the user.

The password applies to the user's account only. The password is invalid after five unsuccessful activation attempts, and if the user does not activate a handheld 48 hours after the password is created, the password expires and cannot be used. When the handheld is successfully activated, the password is removed from the BlackBerry Enterprise Server.



1. BlackBerry Manager: Click Set Activation Password

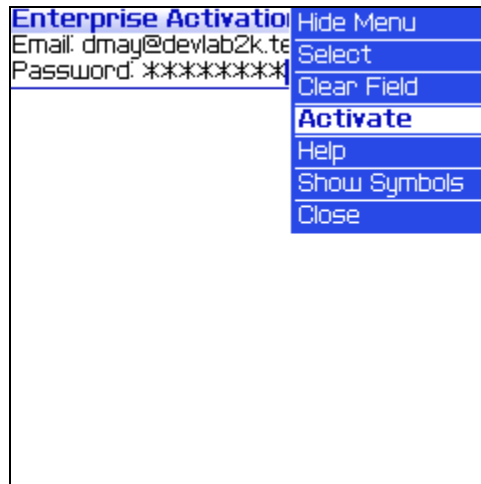


2. Enter wireless activation password

3. **User initiates wireless enterprise activation:** The user opens the enterprise activation program on the handheld and types the appropriate corporate email address and activation password.

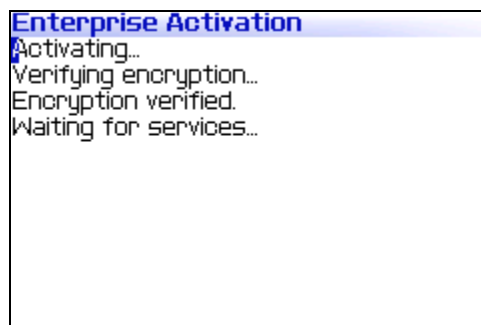


3. Wireless Enterprise Activation application: Enter password



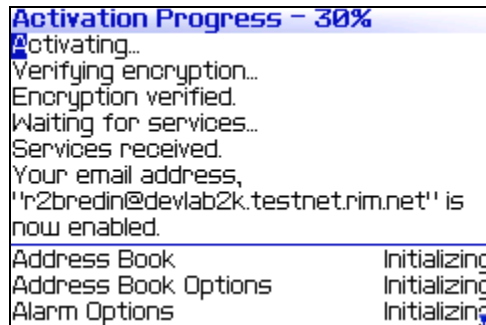
4. Wireless Enterprise Activation application: Click Activate

4. **Handheld sends activation request:** The handheld sends an activation request email to the user's corporate email account. This email contains information about the handheld such as routing information and the handheld's activation public keys.
5. **Server sends activation response:** The BlackBerry Enterprise Server sends the handheld an activation email response that contains routing information about the BlackBerry Enterprise Server and the server's public keys.
6. **Establish and verify keys:** The BlackBerry Enterprise Server and the handheld establish a master encryption key. Both the BlackBerry Enterprise Server and the handheld verify their knowledge of the master key to each other. If key confirmation succeeds, the activation proceeds and further communication is encrypted.

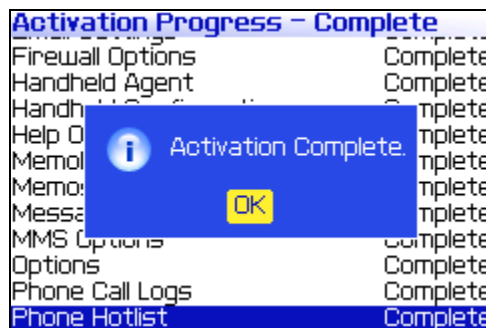


5. BlackBerry handheld displays verification status

7. **Service books sent:** The BlackBerry Enterprise Server sends appropriate service books (for example, messaging service book, wireless calendar service book, browser service book) to the handheld. The user can now send and receive messages on the handheld.
8. **Data loaded:** If the user is configured for wireless PIM synchronization and wireless backup, the BlackBerry Enterprise Server sends the following data to the user's handheld:
 - calendar entries
 - address book entries
 - tasks
 - memos
 - email messages
 - existing handheld options (if applicable) that were backed up through automatic wireless backup



6. BlackBerry handheld receives data



7. BlackBerry handheld displays activation status

Regenerating new master encryption keys

It is recommended that you generate a new master encryption key periodically.

An active user can generate a new master encryption key at any point by clicking **Options > Security > Regenerate Encryption Key** on the handheld.

After a user requests a new key from the handheld, the key request is sent to the BlackBerry Enterprise Server. The encryption key is then renegotiated and generated.

In addition, an administrator can send an IT admin command to the handheld that instructs it to start key regeneration.

The BlackBerry Enterprise Server automatically requests a key regeneration every 30 days.

Enabling wireless data synchronization

To perform wireless data synchronization between the BlackBerry Enterprise Server and the handheld, the administrator must enable the following options on the user's account in the BlackBerry Manager:

- **Wireless Synchronization**
- **Automatic Wireless Backup**

Wireless service book updates

After wireless enterprise activation is enabled, the BlackBerry Enterprise Server can update and remove service books wirelessly from the handheld in the following manner:

User scenario	Action taken	Key management
Remove a user from the BlackBerry Enterprise Server	The BlackBerry Enterprise Server sends a delete service notification to the handheld. The handheld removes all service books that correspond to the BlackBerry Enterprise Server.	Decryption key is set to expire in 7 days.
Move a user from BlackBerry Enterprise Server A to BlackBerry Enterprise Server B.	BlackBerry Enterprise Server B sends the handheld a notification to associate the enterprise encryption key for BlackBerry Enterprise Server A with the service UID for BlackBerry Enterprise Server B. In addition, the handheld receives new service books from BlackBerry Enterprise Server B.	BlackBerry Enterprise Server B uses the encryption key for BlackBerry Enterprise Server A to encrypt and decrypt packets.

Understanding the BlackBerry key establishment protocols

A key establishment protocol enables a handheld and a BlackBerry Enterprise Server to negotiate a common key in such a way that an unauthorized third party cannot calculate the same key.

To establish and manage keys wirelessly, BlackBerry Enterprise Server uses two protocols: the initial key establishment protocol, and the key rollover protocol. Refer to Appendix A on page 10, and Appendix B on page 13 for more information on the protocols.

The BlackBerry Enterprise Server key establishment protocols use Elliptic Curve Cryptography (ECC) to provide strong security.

Initial key establishment protocol

The initial key establishment protocol enables a handheld user to establish a strong, cryptographically protected connection with a BlackBerry Enterprise Server by bootstrapping from the activation password. The protocol provides strong authentication and is secure from online and offline dictionary attacks.

To establish the initial master encryption key, the Simple Password Exponential Key Exchange (SPEKE) scheme is used. SPEKE provides strong authentication and prevents offline dictionary attacks on the activation password. Refer to IEEE P1363.2 Password Based Public Key Cryptography¹ for more information on SPEKE.

The data integrity provided by SPEKE is also leveraged to exchange long term public keys. These public keys provide the strong authentication needed in the key rollover protocol described in the next section.

¹ See <http://grouper.ieee.org/groups/1363/passwdPK/index.html>.

The initial key establishment protocol achieves the following goals:

- provides strong authentication and integrity: only an authorized user can activate a handheld on the BlackBerry Enterprise Server
- prevents offline dictionary attacks: it is computationally infeasible for an attacker to determine the user's password by viewing the protocol packets that are sent between the handheld and the BlackBerry Enterprise Server
- prevents online dictionary attacks: the BlackBerry Enterprise Server will prevent an attacker from activating if the attacker types an incorrect activation password on more than five occasions
- exchanges long term public keys: keys are exchanged in a secure manner for use in the key rollover protocol

Key rollover protocol

The key rollover protocol uses an existing master encryption key to establish a new master encryption key. The protocol provides perfect forward secrecy. That is, the new master key is independent of the previous key, and knowledge of the previous master key will not enable an attacker to learn the new master encryption key.

To regenerate an existing master key, the Menezes-Qu-Vanstone (MQV) protocol is used.

Refer to NIST: Special Publication 800-56: Recommendation on Key Establishment schemes, Draft 2.0² and to the Guide to Elliptic Curve Cryptography³ for more information on the MQV protocol.

The key rollover protocol achieves the following goals:

- Strong authentication: Only an authorized handheld or BlackBerry Enterprise Server can initiate the key rollover protocol. That is, an attacker's handheld cannot impersonate a valid handheld to the BlackBerry Enterprise Server and incorrectly re-establish a master key with the attacker's handheld.
- Password independent: An activation password is not needed and the administrator does not need to be involved in the key rollover protocol.
- Flexible initiation: The handheld user or the administrator can initiate the key rollover protocol at any time.
- Perfect forward secrecy: Each new master key is independent of the previous master key. That is, a master encryption key will not help the attacker decrypt messages protected with another master encryption key.
- Automatic updates: The BlackBerry Enterprise Server will automatically initiate the key rollover protocol after 30 days.

² NIST Special Publication 800-56: Recommendation on Key Establishment Schemes, Draft 2.0.
<http://csrc.nist.gov/CryptoToolkit/tkkeygmt.html>, January 2003.

³ D. Hankerson, A. Menezes, and S. Vanstone. Guide to Elliptic Curve Cryptography. Springer-Verlag, New York, New York, 2004.

Security benefits of the initial key establishment protocol

The initial key establishment protocol was designed to provide strong authentication and to prevent offline and online dictionary attacks.

See "Appendix A" on page 10 for more information.

Eavesdropping attack

An eavesdropping attack occurs when the attacker is able to listen to the communication between the BlackBerry Enterprise Server and the handheld. The goal of the attacker is to determine the master encryption key that both the BlackBerry Enterprise Server and the handheld share.

For attackers to determine the master encryption key, they must solve the Diffie-Hellman (DH) problem. The DH problem is considered to be computationally infeasible.

Man-in-the-middle attack

A man-in-the-middle attack occurs when the attacker is able to intercept and modify messages in transit between the BlackBerry Enterprise Server and the handheld. 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.

SPEKE prevents a man-in-the-middle attack. For an attacker to successfully mount a man-in-the-middle attack, the attacker must know the activation password. Thus, the activation password must be securely given only to the authorized user.

Impersonating a handheld

For an attacker to impersonate the handheld, the attacker must send messages to the BlackBerry Enterprise Server so that the BlackBerry Enterprise Server believes it is communicating with the handheld. The first message that the attacker sends is a function of the activation password. Note that the attacker can only guess the activation password. The BlackBerry Enterprise Server will construct its master encryption key based on the message sent by the attacker and a secret private key chosen by the BlackBerry Enterprise Server. The only way the attacker can compute the same master encryption key is to determine the secret private key held by the BlackBerry Enterprise Server. To do this, the attacker must solve the discrete log problem, which is computationally infeasible.

Impersonating a BlackBerry Enterprise Server

For an attacker to impersonate the BlackBerry Enterprise Server, the attacker must send messages to the handheld so that the handheld believes it is communicating with the BlackBerry Enterprise Server. The first message the attacker sends is a function of the activation password. Note that the attacker can only guess the activation password. The handheld will then construct its master encryption key based on the message sent by the attacker and a secret private key chosen by the handheld. The only way the attacker can compute the same master encryption key is to determine the secret private key held by the handheld. To do this, the attacker must solve the discrete log problem, which is computationally infeasible.

Offline dictionary attack

A dictionary attack occurs when the attacker attempts all possible passwords and determines which password is the correct password. An offline dictionary attack means that the attacker can use as many computational resources as he can muster. In theory, nothing limits the speed that the attacker can use to force the password.

SPEKE prevents an offline dictionary attack.

Online dictionary attack

An online dictionary attack is a dictionary attack, but the attacker must rely on the handheld or the BlackBerry Enterprise Server to determine if a password is the correct password.

The BlackBerry Enterprise Server only supports five attempts. Hence, the attacker has at most five guesses before the activation password is rendered invalid on the BlackBerry Enterprise Server.

Small subgroup attack

A small subgroup attack occurs when the attacker limits the key establishment protocol to generate master encryption keys from a small subset of keys only.

To identify this type of attack, both the handheld and the BlackBerry Enterprise Server check their inputs.

Security benefits of the BlackBerry key rollover protocol

The key rollover protocol is designed to prevent the following attacks.

See "Appendix B" on page 13 for more information.

Man-in-the-middle attack

The MQV protocol prevents a man-in-the-middle attack. That is, as long as the long-term private keys remain secret, this type of attack is computationally infeasible.

Perfect forward secrecy

The MQV protocol provides perfect forward secrecy. Each run of the MQV protocol uses a unique and random ephemeral key pair to create the new master encryption key. Then, the key pair is discarded. Even if both the static and ephemeral private keys from a particular protocol run are compromised, the master encryption keys from other protocol runs remain secure.

Masquerade attack

A masquerade attack occurs when an attacker with possession of the victim's long term private key impersonates any third party to the victim.

The MQV protocol prevents a masquerade attack.⁴

⁴ NIST Special Publication 800-56: Recommendation on Key Establishment Schemes, Draft 2.0.
<http://csrc.nist.gov/CryptoToolkit/tkkeymgmt.html>, January 2003.

Appendix A: BlackBerry initial key establishment protocol

The handheld and the BlackBerry Enterprise Server share the following cryptosystem parameters:

$E(F_q)$: the NIST-approved 521 bit random elliptic curve over F_q . This curve has a cofactor of one.

F_q : a finite field of prime order q .

P : a point of E that generates a subgroup of $E(F_q)$ of prime order r .

xR : represents elliptic curve scalar multiplication, where x is the scalar and R is a point on $E(F_q)$.

s : s is a small password chosen by the system administrator.

S : s is converted to a point on $E(F_q)$.

$\bar{R} = (\bar{x} \bmod 2^{\lfloor \frac{f}{2} \rfloor}) + 2^{\lfloor \frac{f}{2} \rfloor}$, where \bar{x} is the integer representation of the x coordinate of the elliptic curve point R and f is the bit length of r (ie. $f = \lfloor \log_2 r \rfloor + 1$).

All math operations are done in the group $E(F_q)$.

Auxiliary data contains the following values: PIN, network type, handheld capabilities, rekey algorithm, transaction ID, handheld supported algorithms, key sequence hint, service UID, selected algorithm, and full key ID.

Initialization

Handheld	BlackBerry Enterprise Server
Pick long-term key pair: Pick random $a, 1 < a < F-1$ Calculate $A = aP$	Pick long-term key pair: Pick random $b, 1 < b < F-1$ Calculate $B = bP$
Securely store: a (device long-term private key), A (handheld long-term public key)	Securely store: b (service long-term private key), B (service long-term public key)

Activation

The activation phase generates the key using SPEKE and DH.

Handheld		BlackBerry Enterprise Server
Handheld is given a short-term shared secret s .		BlackBerry Enterprise Server is given a short-term shared secret s .
Convert s to a point on $E(F_q)$. Denote the point as S .		Convert s to a point on $E(F_q)$. Denote the point as S .
Pick short-term authentication key pair: Pick random $x, 1 < x < F-1$ Calculate $X = xS$		

Handheld		BlackBerry Enterprise Server
Send X, A to BES.	X, A , auxiliary data _D →	Pick short-term authentication key pair: Pick random $y, 1 < y < F-1$ Calculate $Y = yS$ Calculate master secret: $k_1 = yX$ $k_2 = bA$ If $k_1 = 0, 1, -1$ then set $k_1 =$ random. If $k_2 = 0, 1, -1$ then set $k_2 =$ random. $(k k_{conf}) = \text{SHA-512}(k_1 k_2)$ Calculate the BlackBerry Enterprise Server key confirmation value: $h_B = \text{HMAC-256}_{k_{conf}}$ (auxiliary data _D auxiliary data _B A B X Y "B")
	Y, B, h_B , auxiliary data _B ←	Send Y, B, h_B to handheld
Calculate master key: $k_1 = xY$ $k_2 = aB$ If $k_1 = 0, 1, -1$, then set $k_1 =$ random. If $k_2 = 0, 1, -1$ then set $k_2 =$ random. $(k k_{conf}) = \text{SHA-512}(k_1 k_2)$ Check the BlackBerry Enterprise Server key confirmation value: If $h_B \neq \text{HMAC-256}_{k_{conf}}$ (auxiliary data _D auxiliary data _B A B X Y "B"), then abort. Calculate handheld's key confirmation value: $h_A = \text{HMAC-256}_{k_{conf}}$ (auxiliary data _D auxiliary data _B A B		

Handheld		BlackBerry Enterprise Server
$ X Y "A")$		
Send h_A to BlackBerry Enterprise Server	$h_A \rightarrow$	
		<p>If $h_A \neq \text{HMAC-256}_{k_{conf}} (\text{auxiliary data}_D \text{auxiliary data}_B A B X Y "A")$, then abort.</p> <p>If the handheld makes more than 10 failed attempts, then deny that handheld service.</p>
<p>Zero: s, x, k_1, k_2, k_{conf}</p> <p>Securely store: B (service long-term public key), k (shared master key)</p>		<p>Zero: s, y, k_1, k_2, k_{conf}</p> <p>Securely store: A (handheld long-term public key), k (shared master key)</p>

Notes on attacks:

For an eavesdropping attack to succeed, the attacker must determine $K1 = xyS$ given only xS and yS and $k2 = abP$ given only aP and bP . However, this calculation is equivalent to solving the DH problem.

For a man-in-the-middle attack to succeed, the attacker must know the activation password. Thus, the activation password must be given securely to the authorized user.

If an attacker tries to impersonate a handheld because the attacker does not know the secret s , the attacker must send $X = xP$, instead of xS to the BlackBerry Enterprise Server. The BlackBerry Enterprise Server will calculate $k_1 = yX = yxP$. To calculate the same key, the attacker needs to determine y from Y . This problem is considered to be computationally infeasible.

For an offline attack, assume the attacker sends $X = xP$ instead of xS to the BlackBerry Enterprise Server. The BlackBerry Enterprise Server will reply with $Y = xS$ and calculate $k_{1\text{ BES}} = yX = yxP$. Meanwhile, the attacker will calculate $k_{1\text{ attacker}} = xY = yxS = yxzP$, for some z such that $S = zP$. Using the key confirmation value h_B , the attacker needs to find a value w such that $wk_{1\text{ attacker}} = wxY = wyxzP = xyP = k_{1\text{ BES}}$. Notice however, that $w = z^{-1} \pmod r$. Therefore, finding w amounts to finding z , which corresponds to solving the discrete logarithm problem for S . This problem is considered to be computationally infeasible.

For an online attack, during each run, the handheld attempts a different password, and checks if it has made the correct choice against h_B . This is averted by limiting the handheld to 10 attempts at determining the correct secret s .

A small subgroup attack is one in which an attacker forces the key agreement to originate from a small set of values. For example if the attacker chooses X to be the point at infinity, then k_1 would be the point at infinity irrespective of what the BlackBerry Enterprise Server chooses for Y . Therefore, by checking that X is not at the point of infinity, one or minus one this threat is averted.

Appendix B: BlackBerry key rollover protocol

The handheld and the BlackBerry Enterprise Server share the following cryptosystem parameters:

$E(F_q)$: the NIST approved 521 bit random elliptic curve over F_q . This curve has a cofactor of one.

F_q : a finite field of prime order q .

P : a point of E that generates a subgroup of $E(F_q)$ of prime order r .

xR : represents elliptic curve scalar multiplication, where x is the scalar and R is a point on $E(F_q)$.

$\bar{R} = (\bar{x} \bmod 2^{\lceil \frac{f}{2} \rceil}) + 2^{\lceil \frac{f}{2} \rceil}$, where \bar{x} is the integer representation of the x coordinate of the elliptic curve point R , and f is the bit length of r (ie. $f = \lfloor \log_2 r \rfloor + 1$).

All MQV math operations are done in Z_r .

Auxiliary data contains the following values: rekey algorithm, shared secret key ID, transaction ID, handheld supported algorithms, key sequence hint, service UID, selected algorithm, and full key ID.

Handheld		BlackBerry Enterprise Server
	← GenerateKeyRequest	Optional step: BlackBerry Enterprise Server decides it is time to cut a new master key.
Handheld decides it is time to cut a new master key.		
Pick short-term key pair: Pick random $x, 1 < x < r-1$ Calculate $X = xP$		
Send X to BlackBerry Enterprise Server	X , auxiliary data _D →	
		Pick short-term key pair: Pick random $y, 1 < y < r-1$ Calculate: $Y = yP$ $s_B = (y + \bar{Y}b) \bmod r$ $Z = s_B(X + \bar{X}A)$ If Z is the point of infinity, then choose a new y and recalculate the above equations. Calculate: $(k k_{cont}) = SHA-512(xz)$

		<p>where x_Z is the x-coordinate of Z.</p> <p>Calculate:</p> $h_B = \text{HMAC-256}_{k_{conf}} (\text{auxiliary data}_D \text{auxiliary data}_B A B X Y \text{"B"})$
	$Y, h_B, \text{auxiliary data}_B \leftarrow$	Send Y, h_B to device
<p>Calculate:</p> $s_A = (x + \bar{X}a) \bmod r$ $Z = s_A(Y + \bar{Y}B)$ <p>If Z is the point of infinity, then set it to a random point of $E(F_q)$.</p> <p>Calculate:</p> $(k k_{conf}) = \text{SHA-512}(x_Z), \text{ where } x_Z \text{ is the } x\text{-coordinate of } Z.$ <p>Calculate:</p> $h_A = \text{HMAC-256}_{k_{conf}} (\text{auxiliary data}_D \text{auxiliary data}_B A B X Y \text{"A"})$		<p>In the meantime, if a received message cannot be decrypted with a current master key, or with a previous master key (if available), then try the pending master key.</p>
<p>Check the BlackBerry Enterprise Server key confirmation value:</p> <p>If $h_B \neq \text{HMAC}_{k_{conf}} (\text{auxiliary data}_D \text{auxiliary data}_B A B X Y \text{"B"})$, then abort.</p> <p>Set current master key to k</p>		
Send h_A to BES	$h_A \rightarrow$	
		<p>If $h_A \neq \text{HMAC-256}_{k_{conf}} (\text{auxiliary data}_D \text{auxiliary data}_B A B X Y \text{"A"})$, then abort.</p> <p>Set current master key to k.</p>
Zero: x, s_A, k_{conf}		<p>Zero: y, s_B, k_{conf}</p> <p>Securely store: k (shared master)</p>

Securely store: k (shared master key)		key)

Part number: SWD_X_BES(EN)-041.000

*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 handheld 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.

© 2004 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, BlackBerry and 'Always On, Always Connected' are registered with the U.S. Patent and Trademark Office and may be pending or registered in other countries.

All other brands, product names, company names, trademarks and service marks 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.