

Security Note

BBM Protected

September 2014



Contents

Document revision history.....	4
About this guide.....	5
Using BBM Protected.....	6
System requirements.....	7
How BBM Protected protects messages.....	8
When BBM uses BBM Protected encryption.....	8
Default BBM encryption.....	8
BBM Protected standards and algorithms.....	8
BBM Protected key usage.....	10
Key exchange process.....	10
Key storage.....	15
BBM Protected messaging architecture.....	15
BBM Protected messaging for BlackBerry OS devices.....	15
BBM Protected messaging for BlackBerry 10 devices.....	17
BBM Protected messaging encryption.....	18
Data flow: Sending a BBM message to a device using BBM Protected.....	18
Data flow: Receiving a BBM message from a device using BBM Protected.....	19
IT policy rules that apply to BBM Protected.....	21
Provide feedback.....	22
Glossary.....	23
Legal notice.....	24

Document revision history

1

Date	Description
12 September 2014	<ul style="list-style-type: none">Updated various topics to indicate that BBM Protected now supports all activation types for BlackBerry 10 devices.

About this guide

2

BBM Protected is the first product in the eBBM Suite of products and services aimed at enterprise customers. BBM Protected uses advanced security features to allow BlackBerry device users in your organization to communicate securely with each other using BBM. This guide describes how BBM Protected provides a higher level of security for BBM messages that are sent between BBM Protected users.

This guide is intended for senior IT professionals responsible for evaluating the product and planning its deployment, as well as anyone who's interested in learning more about BBM Protected security features. After you read this guide, you should understand how BBM Protected adds further protection to messages.

Note: This guide doesn't describe the security features of the standard BBM app. For more information, visit blackberry.com/go/serverdocs to see the *BBM Security Note*.

Using BBM Protected

3

BBM can use BBM Protected to provide end-to-end encryption for BBM messages that are sent between BBM Protected users in your organization and other BBM Protected users, inside or outside of your organization. BBM Protected uses default BBM encryption when users in your organization send BBM messages to contacts who aren't using BBM Protected. The encryption that BBM uses for BBM chats depends on whether BBM Protected is turned on or turned off. BBM Protected is turned on or turned off using the "Use BBM Protected" IT policy rule.

The "Use BBM Protected" IT policy rule has the following values that you can choose:

- If you set this rule to "Yes", BBM uses BBM Protected to encrypt and decrypt messages exchanged with contacts that have the "Use BBM Protected" IT policy rule enabled, and it uses default BBM encryption for messages exchanged with other contacts.
- If you set this rule to "No", BBM always uses default BBM encryption.

By default, BBM doesn't use BBM Protected.

For more information about the BlackBerry Enterprise Service 10 IT policy rule for BBM Protected, visit <http://docs.blackberry.com/BES10> to read the *BlackBerry Device Service Policy Reference Spreadsheet*. For more information about the BlackBerry Enterprise Server 5 IT policy rule for BBM Protected, visit blackberry.com/go/kbhelp to read article KB35988.

System requirements

4

To use BBM Protected, you must meet the following requirements:

Device	Requirements
BlackBerry OS (version 6 to 7.1)	<ul style="list-style-type: none"> • Activated on BlackBerry Enterprise Server and the "Use BBM Protected" IT policy rule included in KB35988 imported into the BES5 • Running BlackBerry Messenger 8.5 or later • BBM Protected user license
BlackBerry 10 (version 10.2 and later)	<ul style="list-style-type: none"> • Any activation type • Activated on BlackBerry Enterprise Service 10 version 10.2.2 or later • Running BBM 10.3.30 or later • BBM Protected user license

For more information about importing the BES5 IT policy rule that applies to this feature, visit blackberry.com/go/kbhelp to read KB35988.

BBM Protected is available for BlackBerry devices. Your organization can purchase the required BBM Protected user licenses from BlackBerry or an authorized reseller. For more information, visit <http://www.blackberry.com/BBMProtected>.

Devices that aren't activated on BlackBerry Enterprise Server 5 or BlackBerry Enterprise Service 10 can't use BBM Protected.

How BBM Protected protects messages

BBM Protected uses established cryptographic methods to encrypt and digitally sign messages in order to establish secure communications between BBM Protected users. Users can seamlessly send messages to their friends and family with default BBM encryption at the same time that they send messages to their work contacts with BBM Protected encryption.

When BBM uses BBM Protected encryption

The encryption that BBM uses for a BBM chat depends on whether BBM Protected is on or off.

If BBM Protected is on, BBM uses:

- BBM Protected end-to-end encryption for messages that users exchange with BBM contacts that also have BBM Protected turned on
- Default BBM encryption for messages that users exchange with BBM contacts that don't have BBM Protected turned on
- Default BBM encryption for messages that users exchange with BBM contacts that aren't activated on a BlackBerry Enterprise Server 5 or BlackBerry Enterprise Service 10

If BBM Protected is off, BBM uses default BBM encryption for messages.

Default BBM encryption

When BBM Protected is off or not available on a device, BBM uses default BBM encryption, which relies on TLS. Default BBM encryption uses a combination of authentication and encryption to protect messages. For more information about default BBM encryption, visit blackberry.com/go/serverdocs to see the *BBM Security Note*.

BBM Protected standards and algorithms

BBM Protected uses FIPS 140-2 validated cryptographic libraries to ensure that it satisfies the security requirements for protecting unclassified information as defined by the Federal Information Processing Standards.

BBM Protected uses ECC because it offers significant advantages over the most widely used alternative, RSA. BlackBerry uses the ECC implementation that is offered by Certicom, which is a wholly owned subsidiary of BlackBerry. Certicom has been developing standards-based cryptography for over 25 years. Certicom is the acknowledged worldwide leader in ECC, offering

the most security per bit of any known public key scheme. For example, a 160-bit ECC key and a 1024-bit RSA key offer a similar level of security. A 512-bit ECC key provides the same level of security as a 15,360-bit RSA key.

BBM Protected standards

BBM Protected uses the following standards for signing, encrypting, and hashing, which meet or exceed the NIST Suite B cryptographic guidelines:

- Digital signature standard FIPS 186-4: provides a means of guaranteeing the authenticity and non-repudiation of messages
- AES symmetric encryption standard FIPS 197: uses agreed symmetric keys to guarantee the confidentiality of messages
- HMAC standard FIPS 198-1: based on SHA2-256 and uses agreed symmetric keys to guarantee the integrity of messages
- Cryptographic key generation standard NIST SP 800-133: generates the cryptographic keys that are needed to employ algorithms that provide confidentiality and integrity protection for messages
- Secure Hash standard FIPS 180-4: provides preimage and collision resistant hash functions that are required for secure HMACs, digital signatures, key derivation, and key exchange

BBM Protected algorithms and functions

To protect the connection between BBM users during a BBM chat, BBM Protected users exchange public signing and encryption keys using an out-of-band shared secret and EC-SPEKE. These keys are then used to encrypt and digitally sign BBM messages between the devices. BBM Protected uses the following algorithms that are based on NIST standards with 256-bit equivalent security:

- EC-SPEKE: securely exchanges a symmetric key by protecting the exchange with a password
- KDF: securely derives message keys from shared secrets
- One-Pass DH: using one user's private key and another user's public key, derives a new shared secret between the users

The algorithms and associated key strengths that BBM Protected implements are:

- AES-256 for symmetric encryption
- ECDSA with NIST curve P-521 for signing
- One-Pass ECDH with NIST curve P-521 for symmetric key agreement
- SHA2-512 for hashing and key derivation
- SHA2-256-128 HMAC for message authentication codes

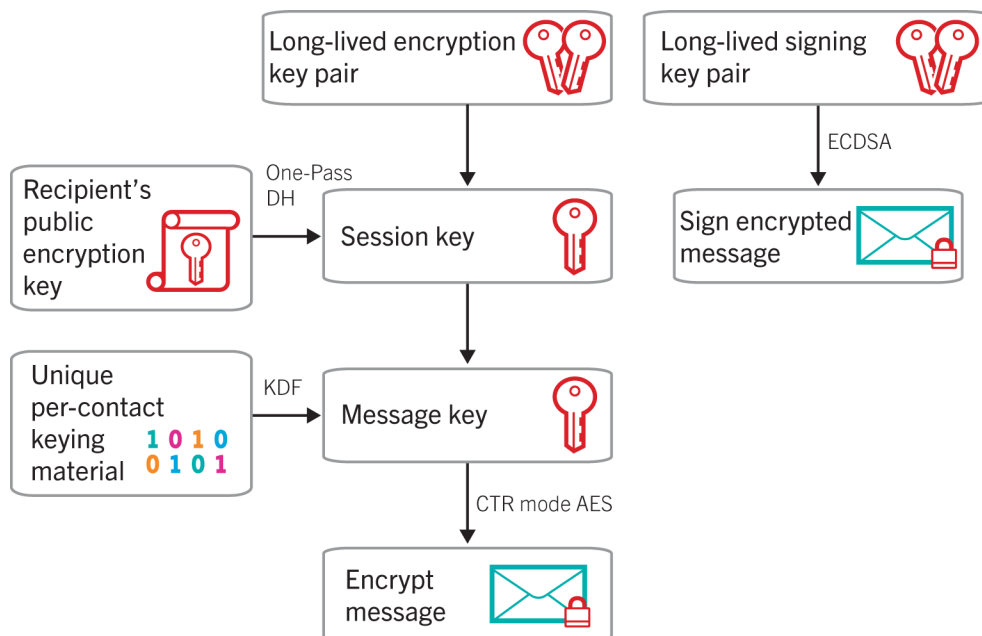
BBM Protected key usage

Each device that uses BBM Protected has two long-lived public and private key pairs that are static for the device and the user: an encryption key pair and a signing key pair.

When a BBM Protected user starts a BBM chat with another BBM Protected user, BBM creates a pairwise key between the users that is used as a session key. The session key is used to encrypt all messages in a BBM chat. The pairwise key is derived from the BBM chat initiator's private encryption key and the recipient's public encryption key, using One-Pass ECDH.

Each session key is combined with unencrypted, but signed, keying material in the message to produce a message encryption key. The message encryption key is derived from the keying material and the session key, using the KDF.

Each BBM Protected message is signed using ECDSA with the signing key pair.



Key exchange process

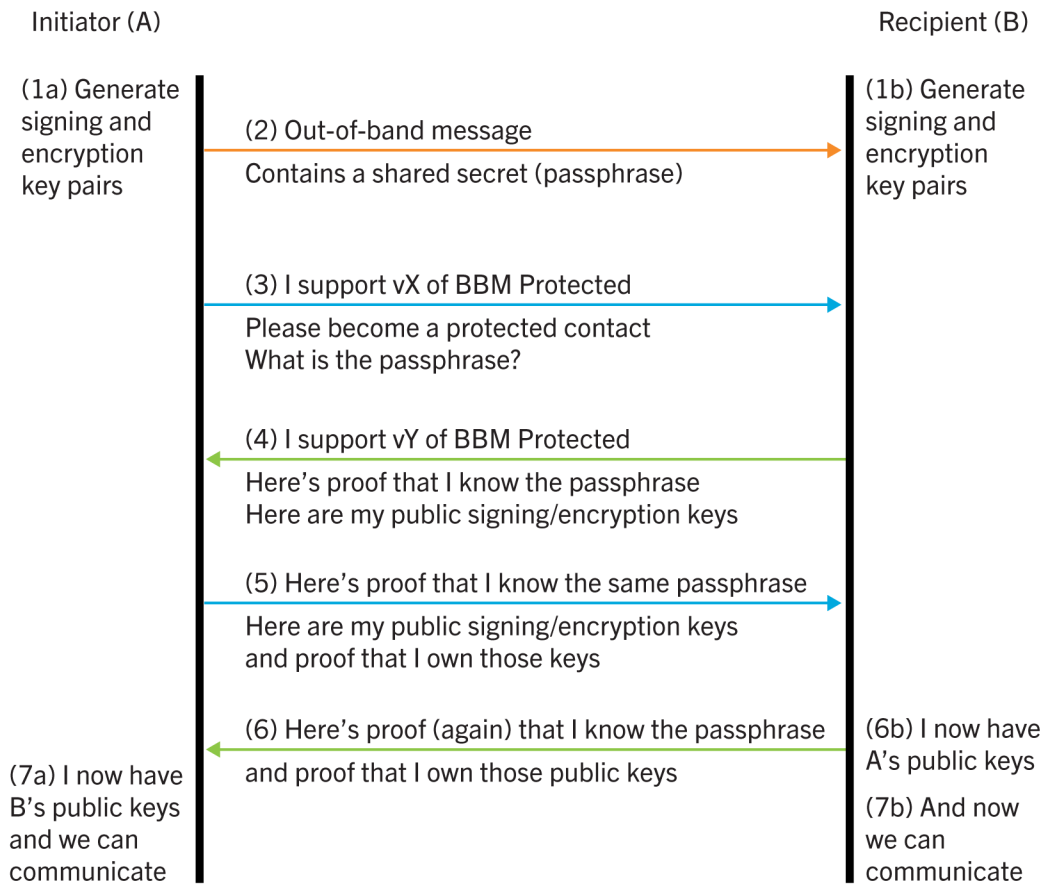
For two BBM users to become BBM Protected contacts, two conditions must be met. The users:

- Must be BBM contacts
- Must go through the key exchange process

In order to exchange keys, BBM Protected users must also exchange a shared secret using an out-of-band mechanism that isn't readable by BlackBerry, such as SMS text message, email, phone call, or in person. The shared secret can be a user-defined passphrase or, if using an SMS text message or email, an autogenerated passphrase.

An attacker would have to compromise the shared secret exchange, which is made more difficult because the attacker doesn't know when or how the secret will be shared. Because the secret is shared out-of-band, an attacker would need to intercept both the connection through the BlackBerry Infrastructure and the out-of-band channel that the BBM Protected users use to exchange the shared secret to compromise the key exchange. Therefore no one, including BlackBerry, can read or modify protected traffic without the ability to intercept the out-of-band channel in real time.

Data flow: BBM Protected key exchange process



The BBM Protected key exchange uses the following steps:

- Each device performs the following actions:
 - Generates a long-lived encryption key pair
 - Generates a long-lived signing key pair
- The initiator chooses a passphrase and sends it out-of-band to the recipient using an SMS text message, email, phone call, or in person.
- The initiator sends the first BBM message, which is an invitation that contains the initiator's contact information and the highest version (vX) of BBM Protected that they support.
- The recipient responds to the invitation and provides:

- The highest version (vY) of BBM Protected that the recipient supports
 - Proof that they know the passphrase
 - The recipient's long-lived public encryption and signing keys
5. The initiator responds to the acceptance and provides:
- Proof that the initiator knows the passphrase
 - The initiator's long-lived public encryption and signing keys
 - Proof that the initiator has the private keys that correspond to the public keys that they claim to own
6. The recipient responds with proof the recipient owns the private keys.
7. After the initiator verifies the final message from the recipient, each party knows the other's public keys and that they belong to someone who knows both the associated private keys and the passphrase. (Assuming that only the recipient and the initiator know the passphrase, they can confirm that the public keys belong to each other.)

Parameters that the BBM Protected key exchange uses

The description of the BBM Protected key exchange uses the following labels:

Parameter	Description
A, B	The two key exchange participants. A is the initiator, B is the recipient.
X_A, X_B	Versions of X belonging to A and B.
PIN_{AB}	BlackBerry PIN value for A and B.
$Version_{AB}$	The highest supported protocol version by each party.
S_{AB}	Public portion of EC-SPEKE exchange values.
S'_{AB}	Private portion of EC-SPEKE exchange values.
$K_{sign_{AB}}$	Public portion of signing key.
$K'_{sign_{AB}}$	Private portion of signing key.
$K_{enc_{AB}}$	Public portion of encryption key.
$K'_{enc_{AB}}$	Private portion of encryption key.
K_{enc}	Symmetric encryption key protecting the confidentiality of the key exchange.
K_{mac}	Symmetric key protecting the integrity of the key exchange.
nonce	Initialization Vector nonce associated with encryption using K_{enc} .
ENCMAC { K_{enc}, K_{mac}, IV } (data)	Symmetric encryption with K_{enc} followed by the addition of a MAC of the ciphertext with K_{mac} .
DECMAC { K_{enc}, K_{mac}, IV } (data)	The inverse of ENCMAC. Verification of the MAC with K_{mac} , followed by decryption of the authenticated ciphertext using K_{enc} .
KDF (aux, secret)	A standard KDF function.

Parameter	Description
EC-SPEKE-GEN (secret)	Generates a non-deterministic key pair based on a shared secret.
EC-DH (private, public)	Generates a raw shared secret with ECDH.
EC-GEN ()	Generates a new random Elliptic Curve key pair.
K_{proof}	A symmetric key used for proving possession of the private key.
EC-SIGN {secret} (data)	A public key signature on a hash using ECDSA.
MAC {secret} (data)	Calculates a MAC keyed with secret on data.
T3, T4	Message authentication tags for messages #3 and #4.
SS_{AB}	The EC-SPEKE shared secret value between A and B.
F	The prefix value used for cryptographic separation between usages of the same key between different BBM applications, protocol versions, and sessions.
S	Shared secrets, shared out-of-band.
	Indicates concatenation.
(X, Y)	Indicates separation of concatenated values.

Data flow: Detailed BBM Protected key exchange process

- Each device generates a long-lived encryption key pair and a signing key pair.

- The initiator's device generates:

```
(KsignA, K'signA) = EC-GEN ()
(KencA, K'encA) = EC-GEN ()
```

- The recipient's device generates:

```
(KsignB, K'signB) = EC-GEN ()
(KencB, K'encB) = EC-GEN ()
```

- The initiator chooses or autogenerates a secret password and sends this out-of-band to the recipient using an SMS text message, email, phone call, or in person.
- The initiator sends the first BBM message, which is an invitation that contains the initiator's contact information and the highest version of BBM Protected that they support.

```
Version = 0
p = KDF ("EC-SPEKE Password", F || S), forget S, where sizeof(p) = 256 bits
(SA, S'A) = EC-SPEKE-GEN (p), forget p
invite_id = 64-bit nonce
```

The initiator's invitation message (Message #1) is: (Version_A, invite_id, PIN_A, S_A)

4. The recipient responds to the invitation and provides the highest version of BBM Protected that the recipient supports, proof that they know the secret password, and the recipient's long-lived public encryption and signing keys.

```
Version = 0
p = KDF ("EC-SPEKE Password", F || S), forget S, where sizeof(p) = 256 bits
(SB, S'B) = EC-SPEKE-GEN (p), forget p
Version = MIN (VersionA, VersionB)
SSAB = EC-DH (S'B, SA)
(Kenc, Kmac, nonce) = KDF ("BBM Protected Key Exchange", F || SSAB)
Message #2 payload = P2 = (invite_id, KsignB, KencB)
Message #2 payload signature = S2 = EC-SIGN {K'signB} (F || versionB || P2 || SA || SB)
Message #2 encrypted payload = E2 = ENCMAC {Kenc, Kmac, nonce} (P2 || S2)
```

The recipient's response message (Message #2) is: (Version_B, S_B, E2)

5. The initiator responds to the acceptance and provides proof that they know the secret password, the initiator's long-lived public encryption and signing keys, and proof that the initiator's private keys correspond to the public keys that the initiator claims to own.

```
Version = MIN (VersionA, VersionB)
Increment password_attempts.
If (password_attempts > 5) then abort.
SSAB = EC-DH (S'A, SB)
(Kenc, Kmac, nonce) = KDF ("BBM Protected Key Exchange", F || SSAB)
(P2, S2) = DECMAC {Kenc, Kmac, nonce} (E2)
(KsignB, KencB) = P2
Verify signature S2.
KencAB = EC-DH (K'encA, KencB)
Kproof = KDF ("K_proof", F || KencAB), where sizeof(Kproof) = 256 bits
Message #3 Auth Tag = T3 = MAC {Kproof} (F || KsignB || KencB)
Message #3 payload = P3 = (KsignA, KencA, T3)
Message #3 payload signature = S3 = EC-SIGN {K'signA} (F || P3 || SB || SA || KsignB || KencB)
Message #3 encrypted payload = E3 = ENCMAC {Kenc, Kmac, nonce} (P3 || S3)
```

The initiator's response message (Message #3) is: E3

6. The recipient responds with proof that they own the recipient's private keys.

```
(P3, S3) = DECMAC {Kenc, Kmac, nonce} (E3)
(KsignA, KencA, T3') = P3
Verify signature S3.
KencAB = EC-DH (K'encB, KencA)
Kproof' = KDF ("K_proof", F || KencAB), where sizeof (Kproof) = 256 bits
T3 = MAC {Kproof'} (F || KsignB || KencB)
Check T3 == T3'
Message #4 Auth Tag = T4 = MAC {Kproof'} (F || KsignA || KencA)
E4 = ENCMAC {Kenc, Kmac, nonce} (T4)
```

The initiator's response message (Message #4) is: E4

7. After the initiator verifies the final message from the recipient, each party knows the other's public keys and that they belong to someone who knows both the associated private keys and the secret password.

```
T4' = DECMAC {Kenc, Kmac, nonce} (Message #4)
Check T4' against MAC {Kproof} (F || KsignA || KencA)
```

After the key exchange is completed, the security of messages no longer depends on the secrecy of the passphrase or the ephemeral key pairs. The public keys for encryption and signing are stored for each contact and the contact is confirmed as the owner of the private keys.

Key storage

On BlackBerry 10 devices, BBM stores the user's key pairs that are used by BBM Protected using the certificate manager.

On BlackBerry OS devices, BBM stores the user's key pairs that are used by BBM Protected using the device's keystore.

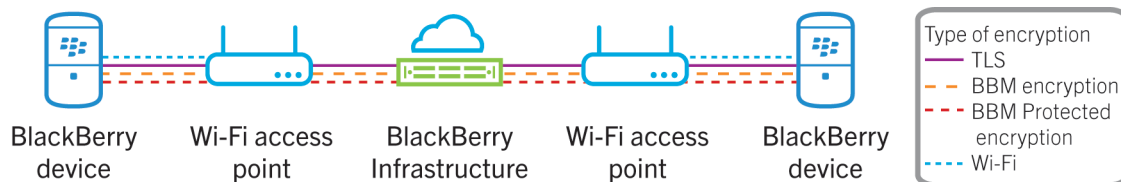
Private keys on devices are stored in a state that ensures that they can't be retrieved.

BBM Protected messaging architecture

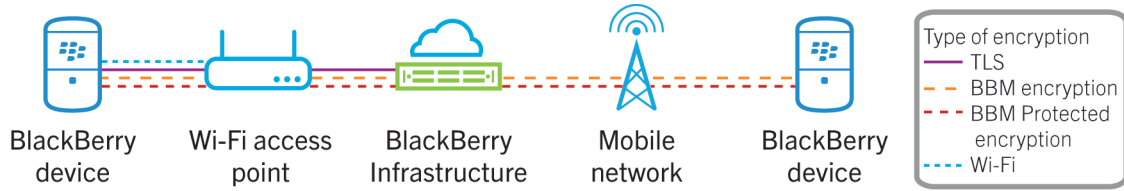
The following diagrams show how BBM Protected protects BBM messages in transit.

BBM Protected messaging for BlackBerry OS devices

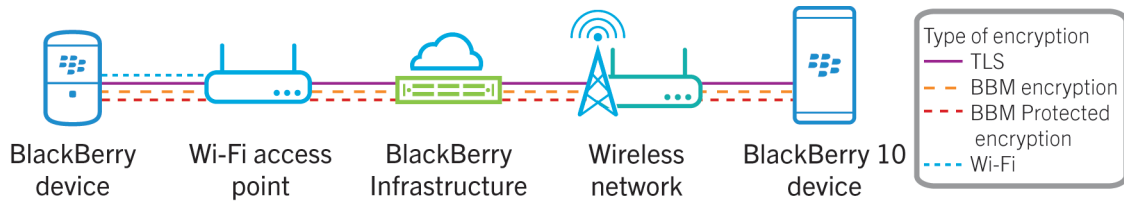
BBM between a BlackBerry OS device on a Wi-Fi network and a BlackBerry OS device on a Wi-Fi network



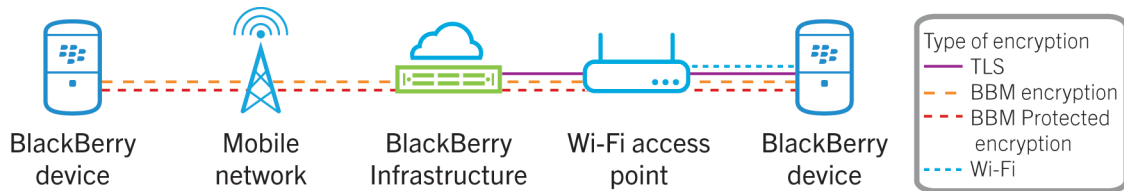
BBM between a BlackBerry OS device on a Wi-Fi network and a BlackBerry OS device on a mobile network



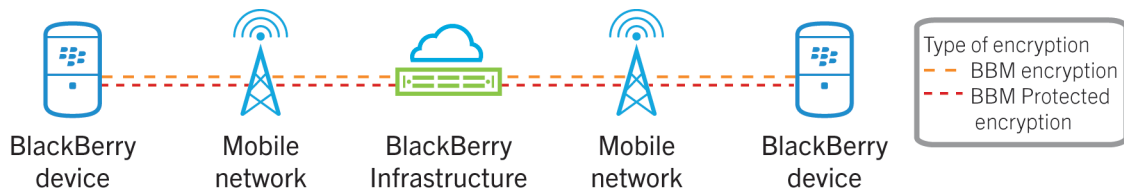
BBM between a BlackBerry OS device on a Wi-Fi network and a BlackBerry 10 device on any wireless network



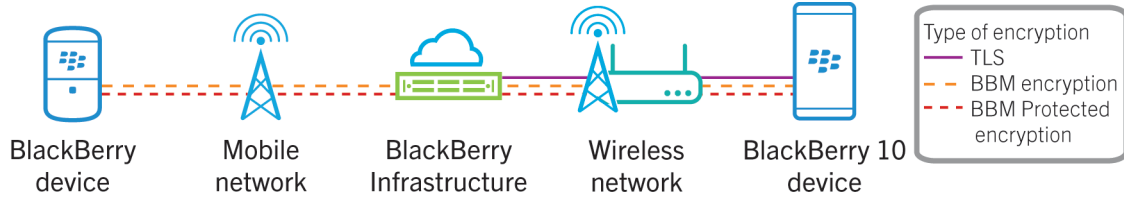
BBM between a BlackBerry OS device on a mobile network and a BlackBerry OS device on a Wi-Fi network



BBM between a BlackBerry OS device on a mobile network and a BlackBerry OS device on a mobile network

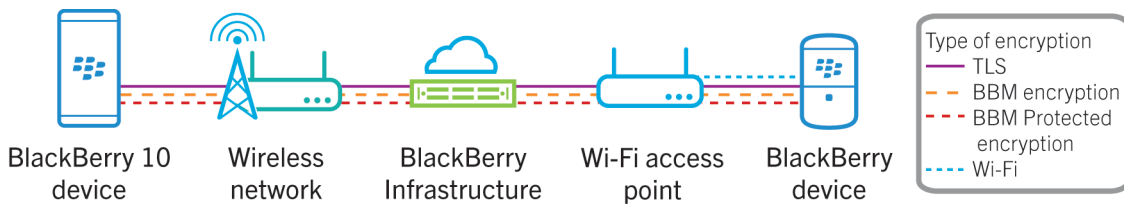


BBM between a BlackBerry OS device on a mobile network and a BlackBerry 10 device on any wireless network

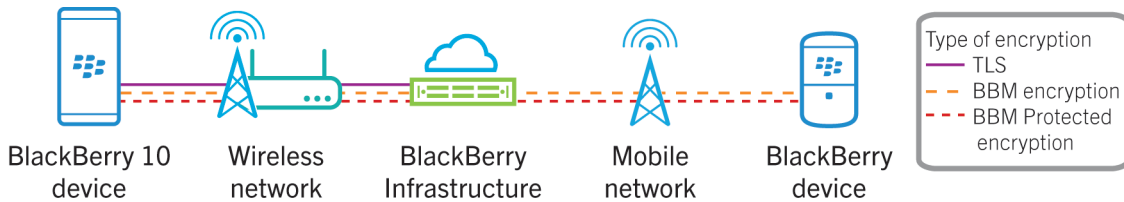


BBM Protected messaging for BlackBerry 10 devices

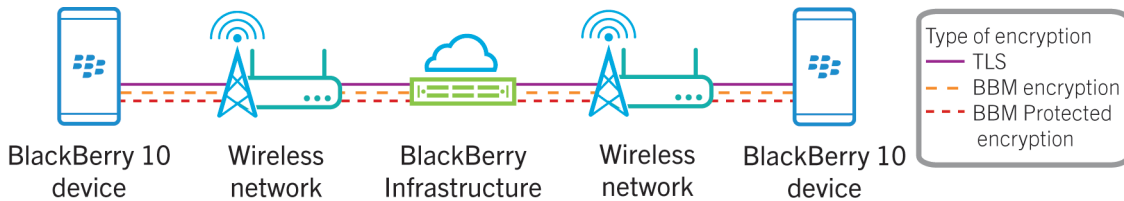
BBM between a BlackBerry 10 device on any wireless network and a BlackBerry OS device on a Wi-Fi network



BBM between a BlackBerry 10 device on any wireless network and a BlackBerry OS device on a mobile network



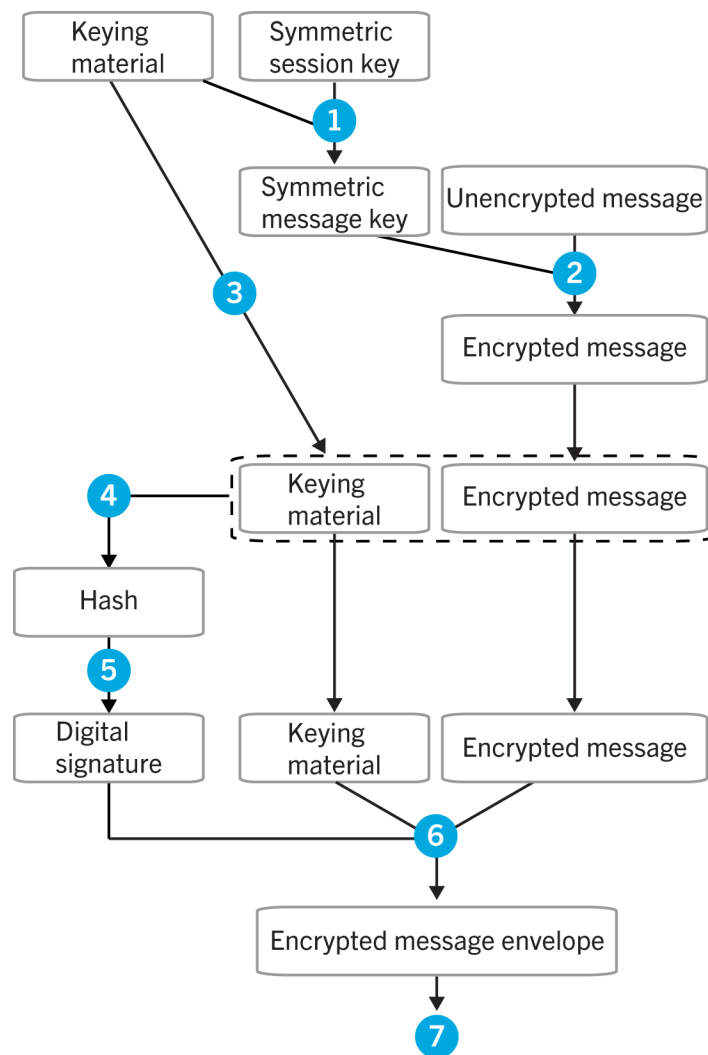
BBM between a BlackBerry 10 device on any wireless network and a BlackBerry 10 device on any wireless network



BBM Protected messaging encryption

After two parties have completed the key exchange process, BBM Protected uses each party's long-lived signing key pair to digitally sign the messages and the encryption key pair to encrypt or decrypt messages. The session key is the symmetric key shared by all conversation participants.

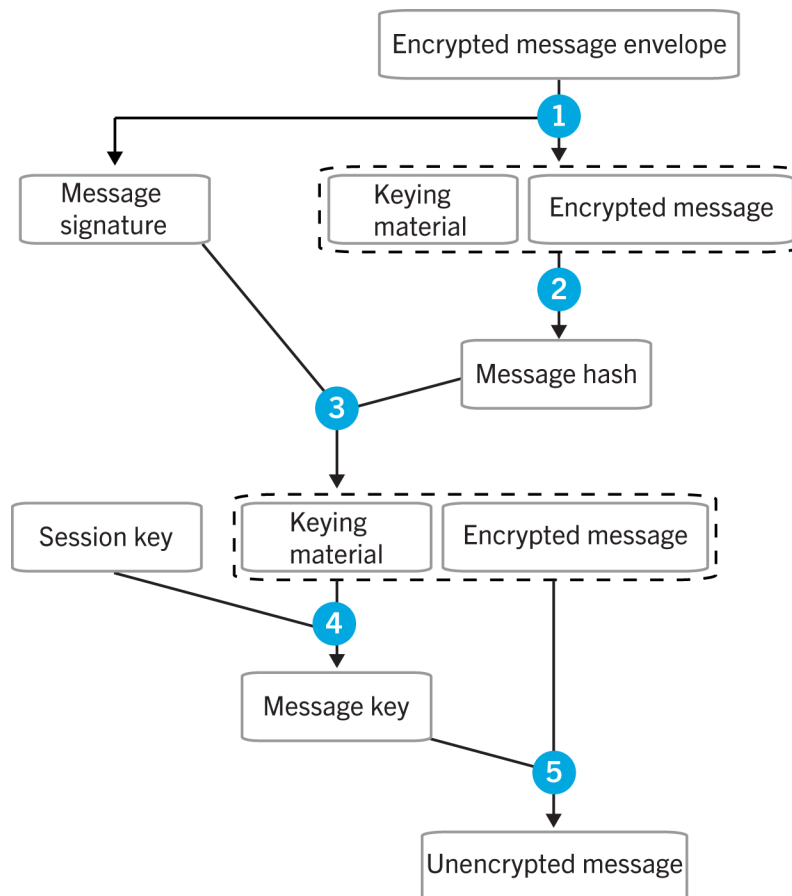
Data flow: Sending a BBM message to a device using BBM Protected



When a BBM Protected user sends a message to another BBM Protected user, the device performs the following actions:

1. Establishes a 256-bit AES message key from the session key and unique keying material.
2. Encrypts the message with the symmetric key using AES in CTR mode.
3. Includes the keying material to recreate the message key in the unencrypted portion of the message.
4. Hashes the whole message using SHA-512.
5. Signs the hash with the sender's private signing key (ECC-521) using ECDSA.
6. Wraps the parts in a message envelope.
7. Passes the message to the transport layer.

Data flow: Receiving a BBM message from a device using BBM Protected



When a BBM Protected user receives a message from another BBM Protected user, the device performs the following actions:

1. Parses the envelope containing the encrypted message.
2. Hashes the encrypted message using SHA2-512.

3. Verifies the message signature using the sender's public key and the encrypted message hash; a pass indicates that the message is authentic.
4. Derives the message key from the session key and the unencrypted keying material.
5. Decrypts the message using AES in CTR mode.

IT policy rules that apply to BBM Protected

The following IT policy rules apply to BBM Protected.

Table 1: BlackBerry Enterprise Server 5 IT policy rule for BBM Protected

IT policy group	IT policy rule
BlackBerry Messenger	<ul style="list-style-type: none"> Use BBM Protected

For more information about the BES5 IT policy rule for BBM Protected, visit blackberry.com/go/kbhelp to read article KB35988.

Table 2: BlackBerry Enterprise Service 10 IT policy rule for BBM Protected

IT policy group	Activation type	IT policy rule
Security	<ul style="list-style-type: none"> All activation types 	<ul style="list-style-type: none"> Use BBM Protected

For more information about the BlackBerry Enterprise Service 10 IT policy rule for BBM Protected, visit <http://docs.blackberry.com/BES10> to read the *BlackBerry Device Service Policy Reference Spreadsheet*.

Provide feedback

To provide feedback on this content, visit www.blackberry.com/docsfeedback.

Glossary

AES	Advanced Encryption Standard
CTR	Counter
DH	Diffie-Hellman
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EC-SPEKE	Elliptic Curve – Simple Password Exponential Key Exchange
FIPS	Federal Information Processing Standards
HMAC	keyed-hash message authentication code
KDF	key derivation function
MAC	message authentication code
NIST	National Institute of Standards and Technology
SHA	Secure Hash Algorithm
SMS	Short Message Service
TLS	Transport Layer Security

Legal notice

©2014 BlackBerry. All rights reserved. BlackBerry® and related trademarks, names, and logos are the property of BlackBerry Limited and are registered and/or used in the U.S. and countries around the world.

Certicom is a trademark of Certicom Corp. Wi-Fi is a trademark of the Wi-Fi Alliance. All other trademarks are the property of their respective owners.

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

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

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

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, IN NO EVENT SHALL BLACKBERRY BE LIABLE FOR ANY TYPE OF DAMAGES RELATED TO THIS DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN INCLUDING WITHOUT LIMITATION ANY OF THE FOLLOWING DAMAGES: DIRECT, CONSEQUENTIAL, EXEMPLARY, INCIDENTAL, INDIRECT, SPECIAL, PUNITIVE, OR AGGRAVATED DAMAGES, DAMAGES FOR LOSS OF PROFITS

OR REVENUES, FAILURE TO REALIZE ANY EXPECTED SAVINGS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, LOSS OF BUSINESS OPPORTUNITY, OR CORRUPTION OR LOSS OF DATA, FAILURES TO TRANSMIT OR RECEIVE ANY DATA, PROBLEMS ASSOCIATED WITH ANY APPLICATIONS USED IN CONJUNCTION WITH BLACKBERRY PRODUCTS OR SERVICES, DOWNTIME COSTS, LOSS OF THE USE OF BLACKBERRY PRODUCTS OR SERVICES OR ANY PORTION THEREOF OR OF ANY AIRTIME SERVICES, COST OF SUBSTITUTE GOODS, COSTS OF COVER, FACILITIES OR SERVICES, COST OF CAPITAL, OR OTHER SIMILAR PECUNIARY LOSSES, WHETHER OR NOT SUCH DAMAGES WERE FORESEEN OR UNFORESEEN, AND EVEN IF BLACKBERRY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

THE LIMITATIONS, EXCLUSIONS, AND DISCLAIMERS HEREIN SHALL APPLY: (A) IRRESPECTIVE OF THE NATURE OF THE CAUSE OF ACTION, DEMAND, OR ACTION BY YOU INCLUDING BUT NOT LIMITED TO BREACH OF CONTRACT, NEGLIGENCE, TORT, STRICT LIABILITY OR ANY OTHER LEGAL THEORY AND SHALL SURVIVE A FUNDAMENTAL BREACH OR BREACHES OR THE FAILURE OF THE ESSENTIAL PURPOSE OF THIS AGREEMENT OR OF ANY REMEDY CONTAINED HEREIN; AND (B) TO BLACKBERRY AND ITS AFFILIATED COMPANIES, THEIR SUCCESSORS, ASSIGNS, AGENTS, SUPPLIERS (INCLUDING AIRTIME SERVICE PROVIDERS), AUTHORIZED BLACKBERRY DISTRIBUTORS (ALSO INCLUDING AIRTIME SERVICE PROVIDERS) AND THEIR RESPECTIVE DIRECTORS, EMPLOYEES, AND INDEPENDENT CONTRACTORS.

IN ADDITION TO THE LIMITATIONS AND EXCLUSIONS SET OUT ABOVE, IN NO EVENT SHALL ANY DIRECTOR, EMPLOYEE, AGENT, DISTRIBUTOR, SUPPLIER, INDEPENDENT CONTRACTOR OF BLACKBERRY OR ANY AFFILIATES OF BLACKBERRY HAVE ANY LIABILITY ARISING FROM OR RELATED TO THE DOCUMENTATION.

Prior to subscribing for, installing, or using any Third Party Products and Services, it is your responsibility to ensure that your airtime service provider has agreed to support all of their features. Some airtime service providers might not offer Internet browsing functionality with a subscription to the BlackBerry® Internet Service. Check with your service provider for availability, roaming arrangements, service plans and features. Installation or use of Third Party Products and Services with BlackBerry's products and services may require one or more patent, trademark, copyright, or other licenses in order to avoid infringement or violation of third party rights. You are solely responsible for determining whether to use Third Party Products and Services and if any third party licenses are required to do so. If required you are responsible for acquiring them. You should not install or use Third Party Products and Services until all necessary licenses have been acquired. Any Third Party Products and Services that are provided with BlackBerry's products and services are provided as a convenience to you and are provided "AS IS" with no express or implied conditions, endorsements, guarantees, representations, or warranties of any kind by BlackBerry and BlackBerry assumes no liability whatsoever, in relation thereto. Your use of Third Party Products and Services shall be governed by and subject to you agreeing to the terms of separate licenses and other agreements applicable thereto with third parties, except to the extent expressly covered by a license or other agreement with BlackBerry.

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

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

BlackBerry Limited

2200 University Avenue East
Waterloo, Ontario
Canada N2K 0A7

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

Published in Canada