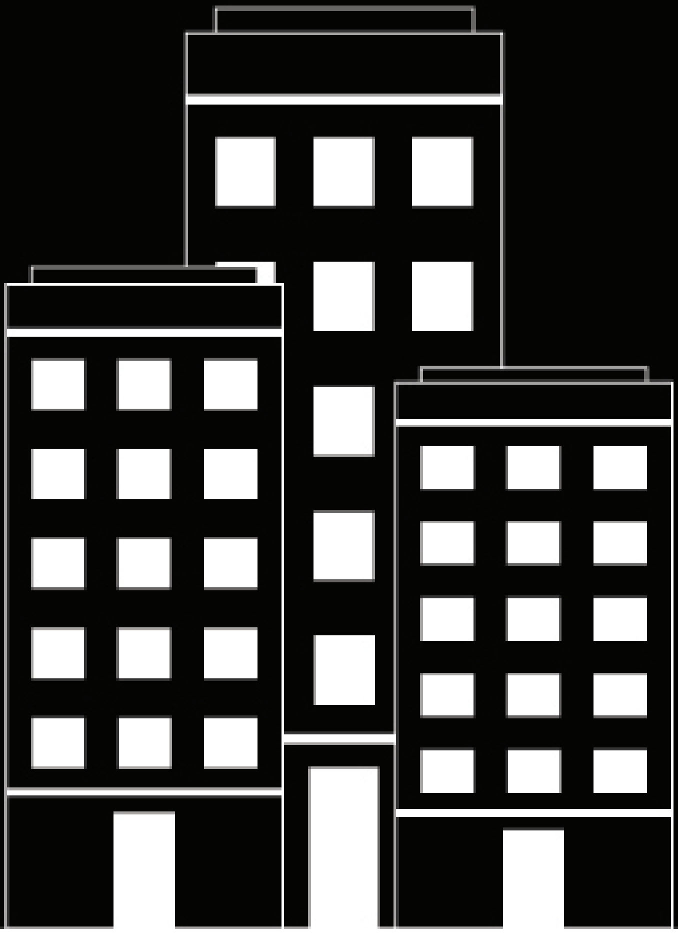


BBM Enterprise

Security Note

1.10

Contents

About this guide

BBM Enterprise uses advanced security features to allow iOS, Android, Windows, and macOS device users in your organization to communicate securely with each other. This guide describes how BBM Enterprise provides a higher level of security for messages, voice calls, and video calls between BBM Enterprise 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 Enterprise or BBM Enterprise security features.

Note: On January 4, 2022, BlackBerry discontinued support for the BlackBerry 7.1 and BlackBerry 10 OSs. This guide might include references to BBM Enterprise features or functionality on these platforms. The references are no longer valid. For more information about the end of life for these platforms, see the BlackBerry 10 and BlackBerry OS Services FAQ.

System requirements

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

Device	Requirements
iOS version 12.0 or later	• BBM Enterprise enabled in the BlackBerry UEM management console • BBM Enterprise for iOS 1.9 or later • BBM Enterprise user license
Android version 7 or later	• BBM Enterprise enabled in the BlackBerry UEM management console • BBM Enterprise for Android 1.9 or later • BBM Enterprise user license
Windows version 10 and later	• BBM Enterprise enabled in the BlackBerry UEM management console • BBM Enterprise for Windows version 1.9 or later • BBM Enterprise user license
macOS version 10.12 and later	• BBM Enterprise enabled in the BlackBerry UEM management console • BBM Enterprise for macOS version 1.9 or later • BBM Enterprise user license

Using BBM Enterprise

BBM Enterprise provides end-to-end encryption for messages, voice calls, and video calls that are sent between BBM Enterprise users in your organization and other BBM Enterprise users, inside or outside of your organization.

How BBM Enterprise protects messages

BBM Enterprise uses established cryptographic methods to encrypt and digitally sign messages in order to establish secure communications between BBM Enterprise users.

BBM Enterprise standards and algorithms

BBM Enterprise 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 Enterprise 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 Enterprise standards

BBM Enterprise 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 Enterprise algorithms and functions

To protect the connection between BBM Enterprise users during a chat, BBM Enterprise users exchange public signing and encryption keys using an in-band or out-of-band shared secret and EC-SPEKE. For details, see Key exchange process. These keys are then used to encrypt and digitally sign messages between the devices. BBM Enterprise 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 Enterprise 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 Enterprise voice and video calling uses SRTP media streaming and implements the following algorithms and associated key strengths:

- AES-256 in GCM mode for symmetric encryption
- 112-bit salting keys
- BBM Enterprise messaging for symmetric key transfer
- SHA1 80-bit tag for message authentication and integrity

BBM Enterprise key usage

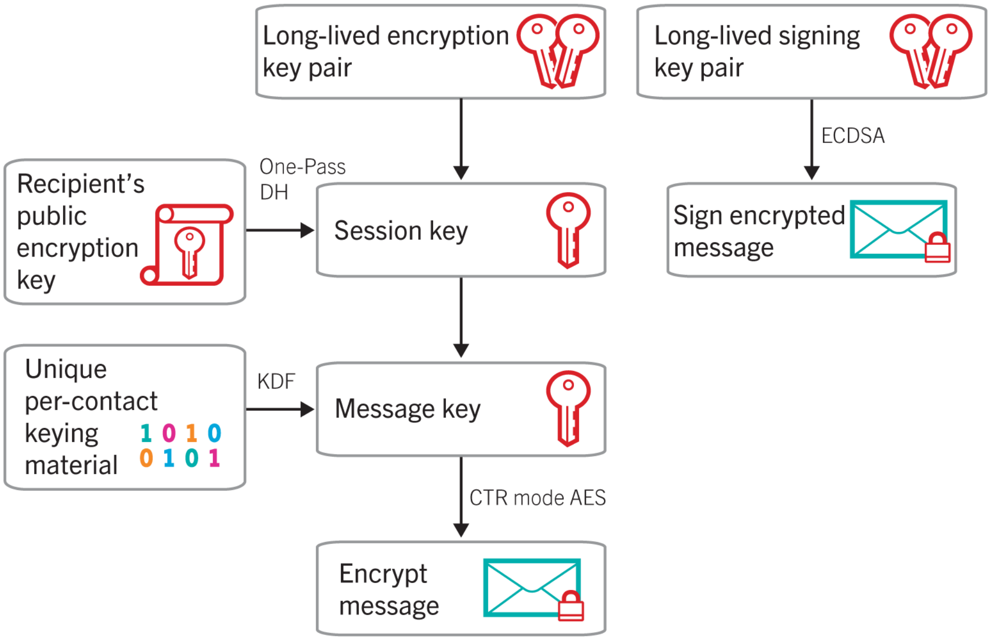
BBM Enterprise uses two types of cryptographic keys: *identity keys* and *chat keys*. Each user has two long-lived public and private key pairs know as their identity keys. One of the key pairs in this set is used to sign messages from the user, and one is used to create secure peer-to-peer encryption contexts between two users. The public identity keys must be shared with other users, while the private identity keys must only be held by the clients of the user that owns them.

When a BBM Enterprise user wants to start communicating with another BBM Enterprise user, the two users must first exchange their public identity keys. Before exchanging keys, BBM Enterprise first performs an EC-SPEKE exchange with the other user, who must prove their identity by providing a passphrase generated by the initiator. This EC-SPEKE exchange establishes a trusted ephemeral cryptographic context within which the users' identity keys are then exchanged. For more information, see Key exchange process.

When a BBM Enterprise user starts a chat with another BBM Enterprise user, BBM Enterprise creates a new random *chat key* that is used to protect the metadata and messages of that chat. Chat messages are encrypted using a per-message key generated by combining the chat key with a message counter, nonce, and other information using ANSI-X9.63-KDF. All participant endpoints within a chat must share the chat key, and it must be protected from users and clients that do not belong to the chat. BBM Enterprise shares the chat key with another user by sending a protected *identity message*.

Identity messages are messages exchanged between two users outside of a chat (for instance, an invitation to join a chat from one user to another). Identity messages are encrypted using a per-message key generated by both the sender and recipient: the remote identity's public encryption key and the local identity's private encryption key are used to generate a ECDH secp521r1 528-bit shared secret. This shared secret is combined with the message counter and nonce to make a secret that is used to derive a key using ANSI-X9.63-KDF.

Each BBM Enterprise identity and chat message is signed using ECDSA with the sender's signing key pair and verified by the receiver.


Long-lived encryption key pair
Long-lived signing key pair
ECDSA
Recipient's public encryption key
One-Pass DH
Session key
Sign encrypted message
Unique per-contact keying material
1 0 1 0
0 1 0 1
KDF
Message key
CTR mode AES
Encrypt message

Key exchange process

The BBM Enterprise key exchange process is protected by an EC-SPEKE passphrase. Protecting the exchange of public identity keys with a passphrase is a unique property of BBM Enterprise. The main purpose of this approach is provide a strong cryptographic promise between the initiator and the recipient of a key exchange so that BBM Enterprise users can be sure that they have the true, trusted keys for other users. With trusted identity keys, users can trust that only intended recipients can join chats and receive messages.

To exchange keys, BBM Enterprise users must also exchange a shared secret, using one of the following options:

- **Automatic passphrase exchange**: Auto passphrase is a default feature of BBM Enterprise that allows users to exchange the required passphrase using an in-band mechanism instead of an out-of-band mechanism. The passphrase that users exchange is generated automatically. The passphrase is shared in-band, using a BBM Enterprise message and requires no user interaction to set it up. The sender's BBM Enterprise app automatically generates a passphrase and sends it to the recipient to use as the passphrase. With auto passphrase, BBM Enterprise seamlessly initiates key exchanges when first communicating with other users.
- **Manual passphrase exchange**: With a manual passphrase exchange, the user who initiates the process sends a shared secret using an out-of-band mechanism, such as in person or using SMS or email. The shared secret can be a user-defined passphrase or it can be an auto-generated passphrase suggested by BBM Enterprise.

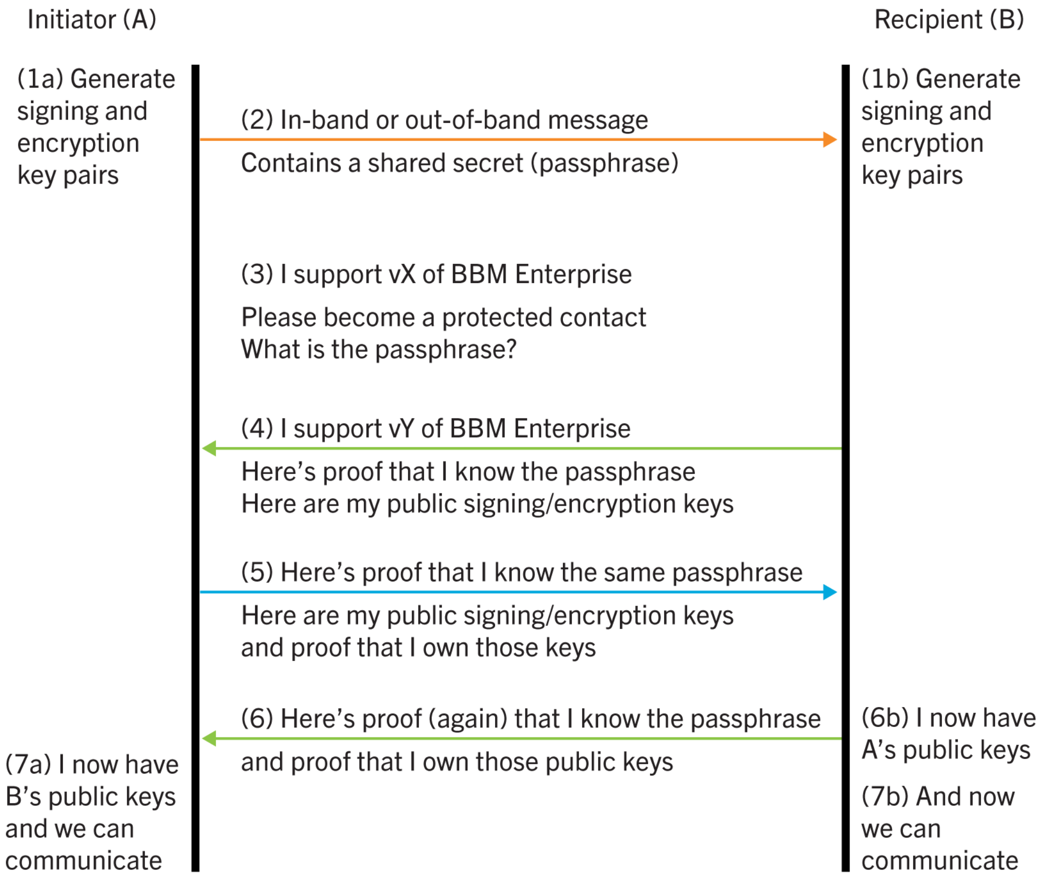
  An attacker would have to compromise the shared secret exchange, which is made more difficult because the attacker doesn't know when or how the secret will be shared. Because the secret is shared out-of-band, in order to compromise the key exchange, an attacker would need to intercept both the connection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

  To enable this option for all users, turn on an IT policy in the BBM Enterprise user management console. Additionally, users with BBM Enterprise version 1.8 can, at any time, use the "Share Passphrase" option in a 1:1 chat to start a manual passphrase key exchange with the chat participant, irrespective of the IT policy settings.

- **Manual key verification**: Starting in BBM Enterprise version 1.8, a manual key verification security measure is available to BBM Enterprise users at all times. When the user manually verifies the fingerprint or scans the

QR code directly from the other user's client in-person or by another secure means, BBM Enterprise marks the user's copy of the keys as manually verified. Users can examine the manual key verification state of all other users, and users receive notifications when new keys are exchanged. When keys are exchanged using a manual passphrase exchange, BBM Enterprise will automatically mark the keys as manually verified. Under an auto passphrase exchange policy, users can manually verify each other's keys by a QR code scan or visual comparison of their key fingerprint.

Data flow: BBM Enterprise key exchange process


Initiator (A)
Recipient (B)
(1a) Generate signing and encryption key pairs
(1b) Generate signing and encryption key pairs
(2) In-band or out-of-band message
Contains a shared secret (passphrase)
(3) I support vX of BBM Enterprise
Please become a protected contact
What is the passphrase?
(4) I support vY of BBM Enterprise
Here's proof that I know the passphrase
Here are my public signing/encryption keys
(5) Here's proof that I know the same passphrase
Here are my public signing/encryption keys
and proof that I own those keys
(6) Here's proof (again) that I know the passphrase
and proof that I own those public keys
(6b) I now have A's public keys
(7a) I now have B's public keys and we can communicate
(7b) And now we can communicate

The BBM Enterprise key exchange uses the following steps:

1. Each device performs the following actions:
    - Generates a long-lived encryption key pair
    - Generates a long-lived signing key pair
2. The shared secret passphrase is exchanged using an automatic or manual passphrase exchange method.
3. The initiator sends the first BBM Enterprise message, which is an invitation that contains the initiator's contact information and the highest version (vX) of BBM Enterprise that they support.
4. The recipient responds to the invitation and provides:
    - The highest version (vY) of BBM Enterprise 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.)
8. If an in-band shared secret is exchanged, once initial keys have been exchanged between two BBM Enterprise contacts, subsequent key exchanges will result in notification to a user when their remote contact has exchanged keys again.

Parameters that the BBM Enterprise key exchange uses

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

Parameter	Description
A, B	The two key exchange participants (A initiator, B 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
$Ksign_{AB}$	Public portion of signing key
$K'sign_{AB}$	Private portion of signing key
$Kenc_{AB}$	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
EC-SPEKE-GEN (secret)	Generates a non-deterministic key pair based on a shared secret

Parameter	Description
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 in-band out-of-band (for details, see Key exchange process)
||	Indicates concatenation
(X, Y)	Indicates separation of concatenated values

Data flow: Detailed BBM Enterprise key exchange process

1. Each device generates a long-lived encryption key pair and a signing key pair.
   a. The initiator's device generates:

   ```
   (Ksign_A, K'sign_A) = EC-GEN ()
   (Kenc_A, K'enc_A) = EC-GEN ()
   ```

   b. The recipient's device generates:

   ```
   (Ksign_B, K'sign_B) = EC-GEN ()
   (Kenc_B, K'enc_B) = EC-GEN ()
   ```

2. The initiator chooses or autogenerates a secret password. This shared password is sent automatically in-band or is sent manually out-of-band to the recipient using an SMS text message, email, phone call, or in person. For details, see Key exchange process.
3. The initiator sends the first BBM message, which is an invitation that contains the initiator's contact information and the highest version of BBM Enterprise that they support.

   ```
   Version = 0
   p = KDF ("EC-SPEKE Password", F || S), forget S, where sizeof(p) = 256 bits
   (S_A, 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 Enterprise 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
($S_B$, $S'_B$) = EC-SPEKE-GEN (p), forget p
Version = MIN (Version$_A$, Version$_B$)
$SS_{AB}$ = EC-DH ($S'_B$, $S_A$)
($K_{enc}$, $K_{mac}$, nonce) = KDF ("BBM Enterprise Key Exchange", F || $SS_{AB}$)
Message #2 payload = P2 = (invite_id, Ksign$_B$, Kenc$_B$)
Message #2 payload signature = S2 = EC-SIGN {K'sign$_B$} (F || version$_B$ || P2 || $S_A$
 || $S_B$)
Message #2 encrypted payload = E2 = ENCMAC {$K_{enc}$, $K_{mac}$, 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.
$SS_{AB}$ = EC-DH (S'_A, S_B)
($K_{enc}$, $K_{mac}$, nonce) = KDF ("BBM Enterprise Key Exchange", F || $SS_{AB}$)
(P2, S2) = DECMAC {$K_{enc}$, $K_{mac}$, nonce} (E2)
(Ksign_B,Kenc_B) = P2
Verify signature S2.
Kenc$_{AB}$ = EC-DH (K'enc$_A$, Kenc$_B$)
$K_{proof}$ = KDF ("K_proof", F || Kenc$_{AB}$), where sizeof($K_{proof}$) = 256 bits
Message #3 Auth Tag = T3 = MAC {$K_{proof}$} (F || Ksign$_B$|| Kenc$_B$)
Message #3 payload = P3 = (Ksign$_A$, Kenc$_A$, T3)
Message #3 payload signature = S3 = EC-SIGN {K'sign$_A$} (F || P3 || $S_B$ || $S_A$ ||
 Ksign$_B$ || Kenc$_B$)
Message #3 encrypted payload = E3 = ENCMAC {$K_{enc}$, $K_{mac}$, 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 {$K_{enc}$, $K_{mac}$, nonce} (E3)
(Ksign$_A$, Kenc$_A$, T3') = P3
Verify signature S3.
Kenc$_{AB}$ = EC-DH (K'enc_B, Kenc$_A$)
Kproof' = KDF ("K_proof", F || Kenc$_{AB}$), where sizeof ($K_{proof}$) = 256 bits
T3 = MAC {$K_{proof}$'} (F || Ksign$_B$ || Kenc$_B$)
Check T3 == T3'
Message #4 Auth Tag = T4 = MAC {$K_{proof}$'}(F || Ksign$_A$ || Kenc$_A$)
E4 = ENCMAC {$K_{enc}$, $K_{mac}$, 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 {$K_{enc}$, $K_{mac}$, nonce} (Message #4)
Check T4' against MAC {$K_{proof}$} (F || Ksign$_A$ || Kenc$_A$)
```

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

Keys obtained from the steps described in the Data flow: BBM Enterprise key exchange process topic are stored locally on the device, in the BBM Enterprise application database. The database's content is encrypted. For more information, see the BBM Enterprise application encryption for data at rest topic.

BBM Enterprise application encryption for data at rest

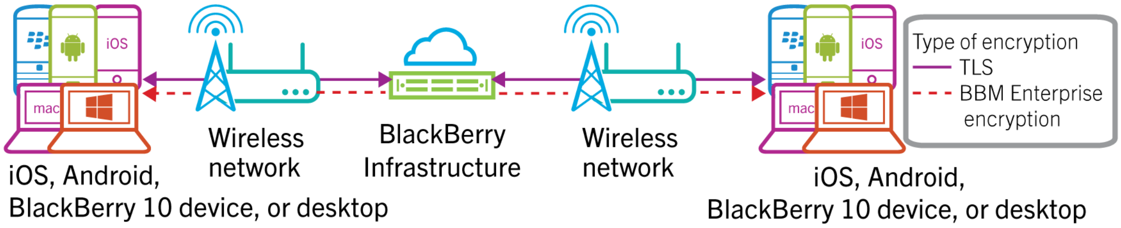
The BBM Enterprise application database is encrypted. BBM Enterprise uses an SQLCipher database, initialized with a passphrase, to store the BBM Enterprise content. BBM Enterprise generates a block of random data (48 bytes) to use as the passphrase. The passphrase is random, unique to each BBM Enterprise app, and used each time the BBM Enterprise app starts on a device. BBM Enterprise encrypts the passphrase and stores it in the platform's specific keystore. For BlackBerry 10, BBM Enterprise encrypts the passphrase and stores it using the platform's certificate manager. For Windows, BBM Enterprise encrypts the passphrase with DPAPI and stores the results locally.

BBM Enterprise messaging architecture

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

BBM Enterprise messaging for iOS, Android or BlackBerry 10 devices, and Windows or macOS desktops

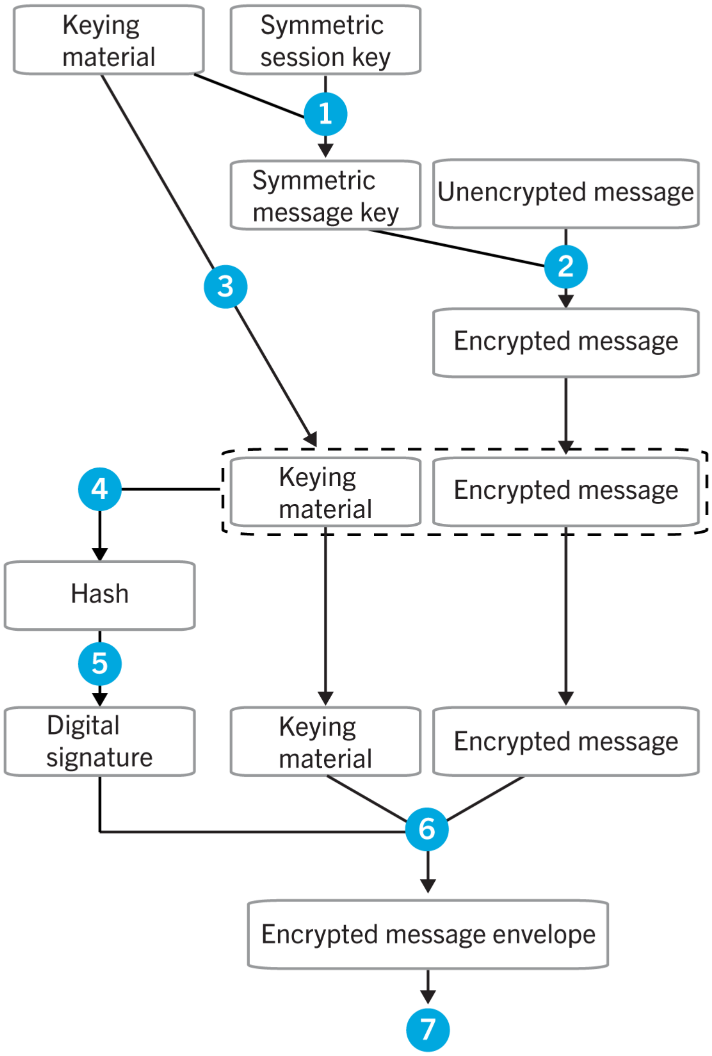
BBM Enterprise between a BlackBerry OS device on any wireless or wired network and an iOS, Android or BlackBerry 10 device, and Windows or macOS desktop, on any wireless or wired network



BBM Enterprise messaging encryption

After two parties have completed the key exchange process, BBM Enterprise 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.

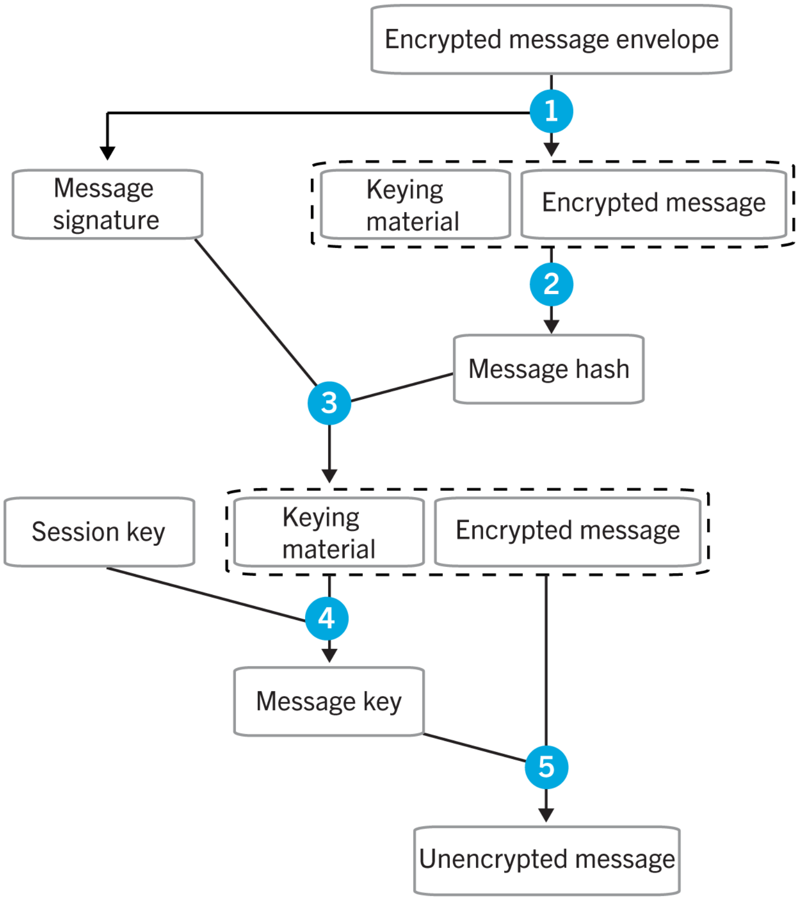
Data flow: Sending a BBM Enterprise message to a device using BBM Enterprise



When a BBM Enterprise user sends a message to another BBM Enterprise 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 Enterprise message from a device using BBM Enterprise



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

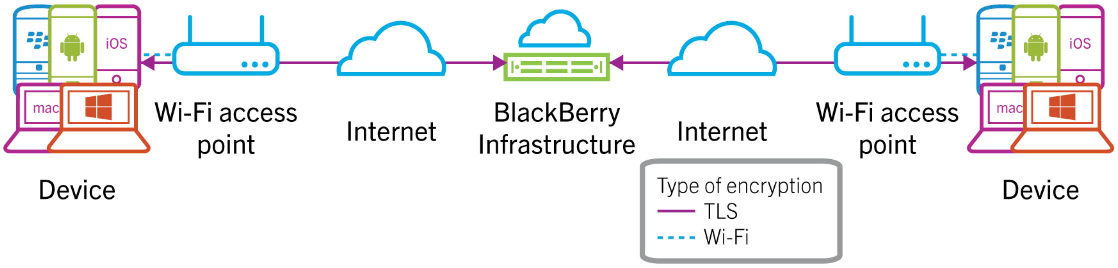
1. Parses the envelope containing the encrypted message
2. Hashes the encrypted message using SHA2-512
3. Verifies the message signature using the sender's public key and the encrypted message hash; a pass indicates that the message is authentic
4. Derives the message key from the session key and the unencrypted keying material
5. Decrypts the message using AES in CTR mode

BBM Enterprise voice and video architecture

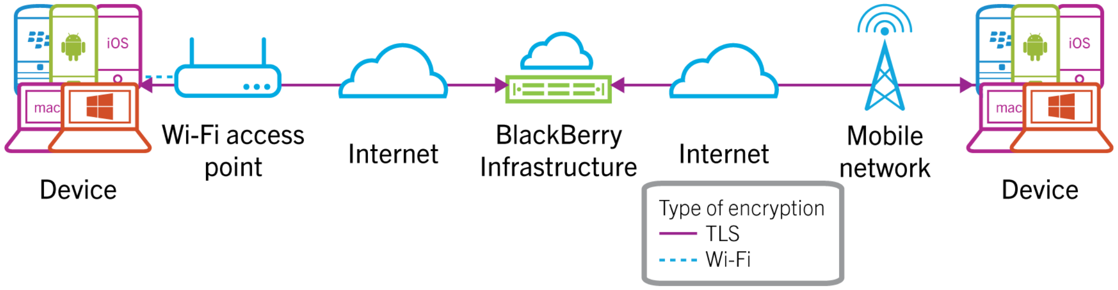
The following diagrams show the architecture and encryption for the setup and data transfer of BBM Enterprise voice and video calls on devices.

BBM Enterprise voice and video call setup

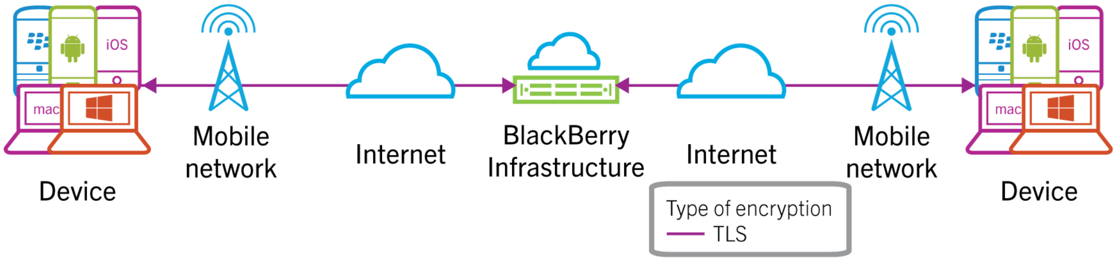
BBM Enterprise voice or video call between a device on a Wi-Fi network and a device on a Wi-Fi network



BBM Enterprise voice or video call between a device on a Wi-Fi network and a device on a mobile network



BBM Enterprise voice or video call between a device on a mobile network and a device on a mobile network

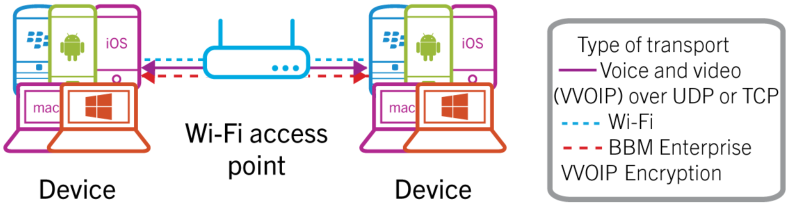


BBM Enterprise voice and video call data transfer

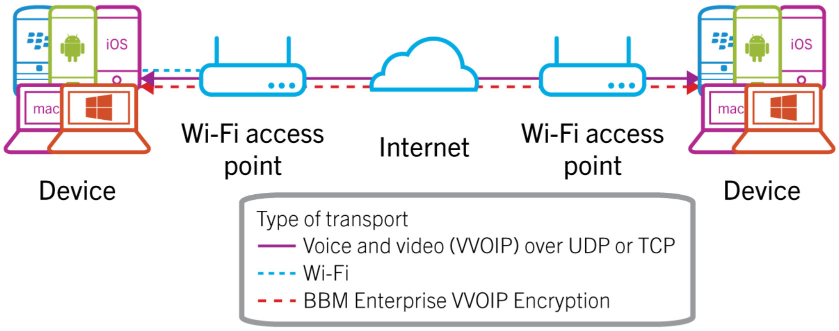
BBM Enterprise voice and video is designed to use the most direct and efficient path for data transfer between the two users in the call. In some cases, when a direct path is not possible, the encrypted voice or video call will be connected through the BlackBerry Infrastructure.

Note: BlackBerry OS devices are not capable of conducting secure BBM Enterprise voice and video calls.

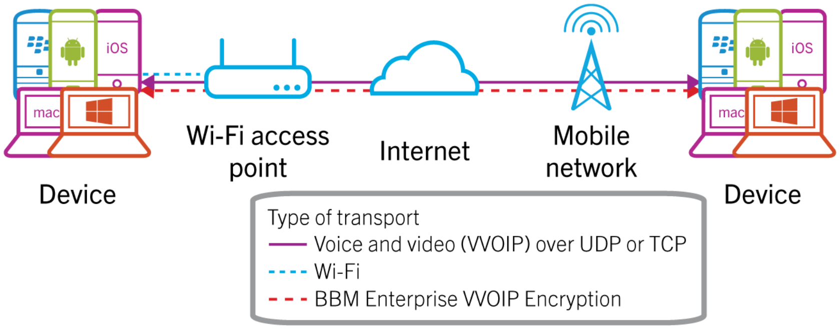
BBM Enterprise voice or video call between devices on the same Wi-Fi network


iOS
mac
Device
Wi-Fi access point
iOS
mac
Device
Type of transport
Voice and video (VVOIP) over UDP or TCP
Wi-Fi
BBM Enterprise VVOIP Encryption

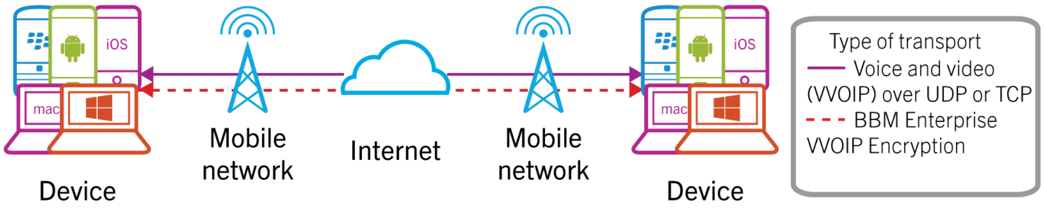
BBM Enterprise voice or video call between a device on a Wi-Fi network and a device on a different Wi-Fi network



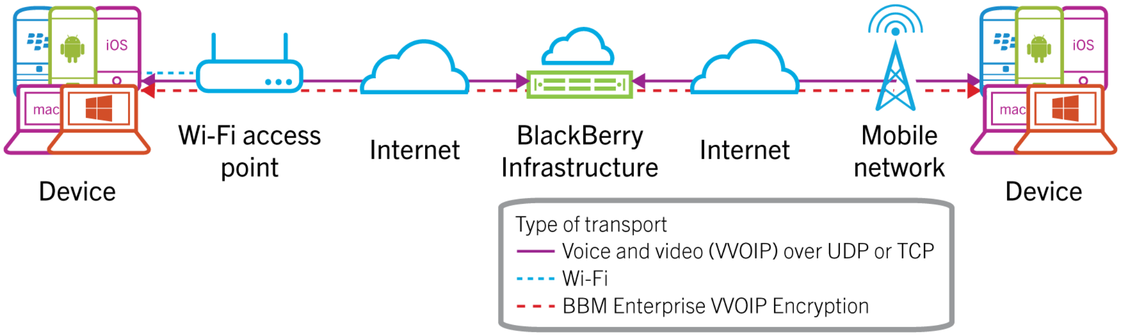
BBM Enterprise voice or BBM Video between a device on a Wi-Fi network and a device on a mobile network



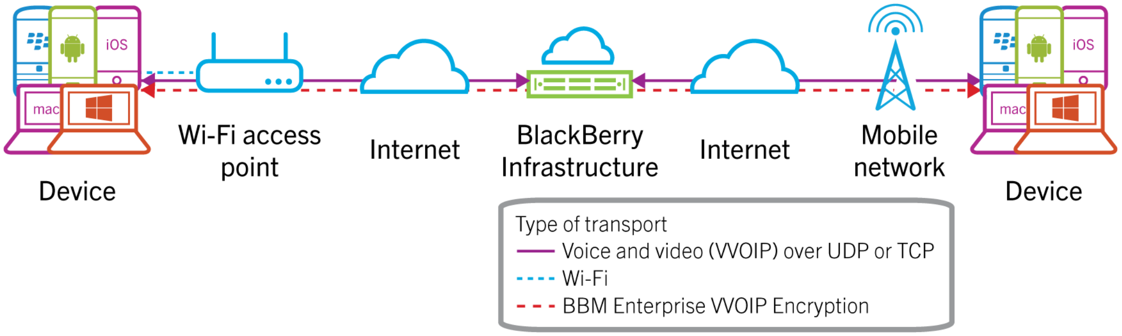
BBM Enterprise voice or BBM Video between a device on a mobile network and a device on a mobile network



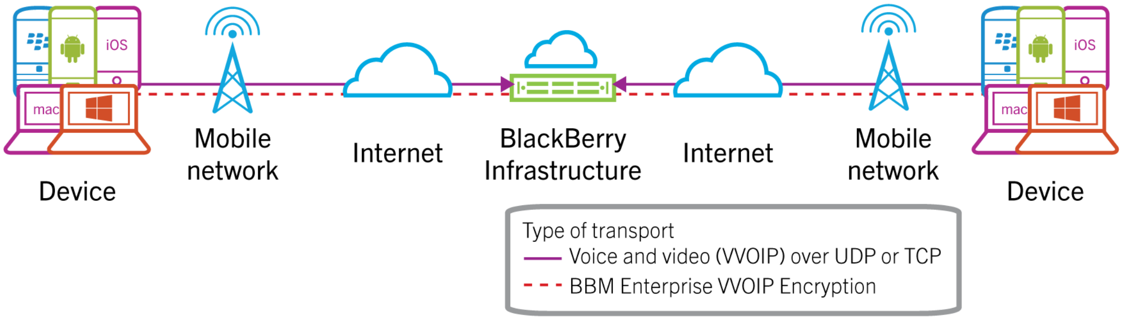
BBM Enterprise video or voice between a device on a Wi-Fi network and a device on a Wi-Fi network through the BlackBerry Infrastructure


iOS
mac
Device
Wi-Fi access point
Internet
BlackBerry Infrastructure
Internet
Mobile network
iOS
mac
Device
Type of transport
Voice and video (VVOIP) over UDP or TCP
Wi-Fi
BBM Enterprise VVOIP Encryption

BBM Enterprise video or voice between a device on a Wi-Fi network and a device on a mobile network through the BlackBerry Infrastructure


iOS
mac
Device
Wi-Fi access point
Internet
BlackBerry Infrastructure
Internet
Mobile network
iOS
mac
Device
Type of transport
Voice and video (VVOIP) over UDP or TCP
Wi-Fi
BBM Enterprise VVOIP Encryption

BBM Enterprise video or voice between a device on a mobile network and a device on a mobile network through the BlackBerry Infrastructure


iOS
mac
Device
Mobile network
Internet
BlackBerry Infrastructure
Internet
Mobile network
iOS
mac
Device
Type of transport
Voice and video (VVOIP) over UDP or TCP
BBM Enterprise VVOIP Encryption

BBM Enterprise voice and video encryption

After two users have completed the key exchange process, BBM Enterprise 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.

When a user in your organization makes a BBM Enterprise voice or video call, BBM Enterprise uses a new, random AES-256 key for each participant in the call, and for each media stream in the call. The symmetric keys are encrypted and signed before they are sent to the other participant in the BBM Enterprise voice or video call.

BBM Enterprise voice, video, and screen-sharing media encryption follows the SDES standard for key management and the SRTP standard for secure media streams establishment.

When a BBM Enterprise voice or video user is in an encrypted voice or video call, the 🔒 icon appears on the user's call screen. When a BBM Enterprise voice or video user is not in an encrypted voice or video call, the 🔓 icon appears on the user's call screen.

BBM Enterprise Conferencing

Conference access management

BBM Enterprise Conferencing is a cloud-based service hosted by BlackBerry.

A BBM Enterprise user, activated using BlackBerry UEM, can create and participate in BBM Enterprise multi-party calls provided their organization has purchased valid licenses and enabled users for the BBM Enterprise Conferencing feature.

The licenses will be available for review in the Licensing section of UEM, while the BBM Enterprise profile provides control of the ability to host conferences. For more information, see the BBM Enterprise Administration Guide for BlackBerry UEM.

Participants can join BBM Enterprise multi-party conferences either via a BBM Enterprise chat or a conference link, in cases where browser-based call participation is allowed by the organization.

The following additional controls are automatically provided by the BBM Enterprise Conferencing solution:

- UEM administrators can restrict conferences to be accessible only from BBM Enterprise chats, thereby preventing browser-based access using the following UEM policy in a given BBM Enterprise policy profile: Disable sharing of conference URL.
- Administrators can remove participants from a given conference at any time.
- Participants cannot join a conference after the conference invitation has expired.
- Participants are forced to leave a conference as soon as or shortly after the host leaves the conference.

Participants' identity assertion

The identity of participants joining a conference from a BBM Enterprise chat message will be validated based on their BBM Enterprise identity created during BBM Enterprise activation in UEM, using the following information from the BBM Enterprise Cloud Directory: First name, Last name, and Organization name, if available.

Because the identity of participants joining from a browser cannot be reliably validated by BBM Enterprise, those users will be asked to provide (type) their name before they the conference. The name will be displayed in the list of participants and will have a small open padlock icon beside their name to indicate that their identity cannot be confirmed by BBM Enterprise.

Hosting and joining a conference

A valid BBM Enterprise user joining from the BBM Enterprise app will have their identity asserted by the BBM Enterprise server before the app is granted further access to host and join a BBM Enterprise conference call. The permission to have access for hosting and joining the call is time-bound and cannot be re-used once expired.

Given a valid hosting and joining permission, the BBM Enterprise Conferencing server will mediate an allocation and establishment of a secure, encrypted conferencing session for a given participant. In this case, the BBM Enterprise Conferencing server is a trusted proxy between a user's BBM Enterprise app and the BBM Enterprise media server.

Securing a conference's real-time media

The BBM Enterprise Conferencing solution is built upon industry standard WebRTC technology and SFU (Selective Forwarding Unit) model of media server. Not only does this model allow efficient processing, but it also offers greater security of a call because each video and audio stream is individually encrypted with unique, ephemeral, per-session encryption keys. This method of media conferencing achieves a high security standard and differentiates it from other similar solutions.

Specifically, the BBM Enterprise Conferencing real-time media negotiation and encryption utilizes an industry standard protocol such as DTLS-SRTP with additional enhancements to provide identity assurance.

Identity assertion during real-time media session establishment

To provide mutual identity assurance between a participant and media server and to prevent MITM (man-in-the-middle) attacks, the BBM Enterprise Conferencing server is used as a trusted proxy for the exchange of DTLS fingerprints of both parties, generated during DTLS channel establishment as per RFC5763.

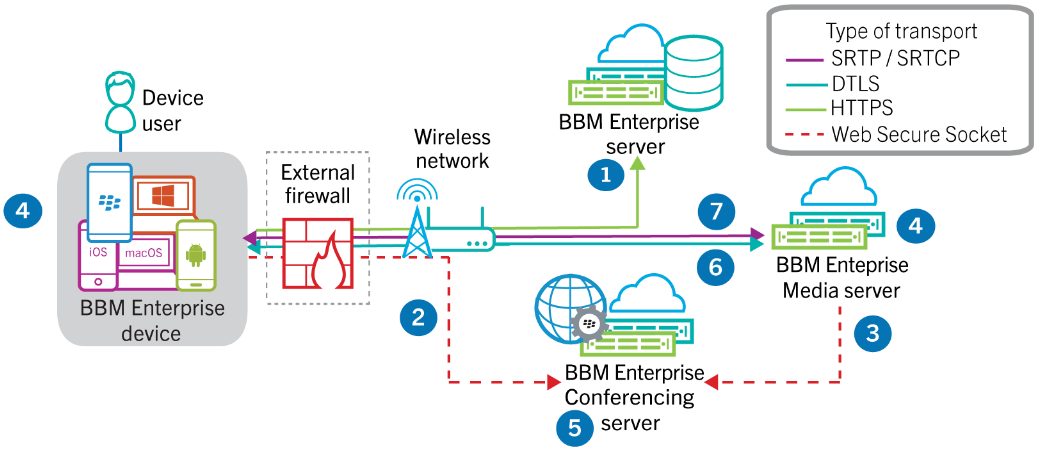
Real-time encryption

AES-128 in CM mode with HMAC-SHA1-80 (BBM Enterprise app, Google Chrome, Safari, Chromium based Microsoft Edge and other Chromium based browsers) or AES-128 in GCM mode with HMAC-SHA1-80 (Mozilla Firefox).

Real-time media stream encryption

As per the SRTP specification, each uplink and downlink video stream is encoded using unique keys exchanged between a given participant and the media server. The solution allows up to four downlink video streams per conference session, for efficiency and bandwidth preservation. Downlink audio from multiple participants is mixed into one stream for efficiency and optimization purposes.

Data flow: Creating a BBM Enterprise conference



1. A BBM Enterprise that wants to host or join a conference is authorized with a secure, short-lived permission grant issued by the BBM Enterprise server, following validation of the user against their organization's policies.

2. The BBM Enterprise user connects to the BBM Enterprise Conferencing server and is authenticated using the issued permission grant.
3. The BBM Enterprise Conferencing server initiates a conference hosting/joining flow with the BBM Enterprise media server over a secure, authenticated connection within the BlackBerry Infrastructure.
4. The BBM Enterprise app and media server generate a self-signed certificate for establishing the DTLS connection in accordance with RFC5763 of DTLS-SRTP.
5. The BBM Enterprise app and media server exchange DTLS fingerprints via an SDP payload using a WSS (Web Secure Sockets) connection to the BBM Enterprise Conferencing server. Exchanging DTLS fingerprints over a trusted proxy provides assurance that the eventual DTLS connection between BBM Enterprise app and the media server has not been subject to MITM attack.
6. The BBM Enterprise app and the media server negotiate SRTP encryption keys for real-time communication over the established DTLS connection in accordance with RFC5764 specification of DTLS-SRTP and RFC3711 of SRTP.

   a. Encryption: AES-128 CTR/CM or AES-128 in GCM as per RFC3711.
   b. Message Authentication and Integrity: HMAC-SHA1-80 as per RFC3711.
   c. KDF: DTLS PRF and SRTP AES-CM KDF as per RFC5
7. Encrypted real-time media flows directly between the BBM Enterprise app and the media server.>

BBM Enterprise features

BBM Enterprise offers extra features that allow you to change the way that BBM Enterprise works by default.

You must use the Enterprise Identity administrator console to turn on these features for users. For more information, visit the following links:

- Windows
- macOS
- Android
- iOS

Glossary

AES	Advanced Encryption Standard
BES12	BlackBerry Enterprise Service 12
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

Patents, as applicable, identified at: www.blackberry.com/patents.

This documentation including all documentation incorporated by reference herein such as documentation provided or made available on the BlackBerry website 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, MERCHANTABLE 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.

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

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

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

BlackBerry UK Limited
Ground Floor, The Pearce Building, West Street,
Maidenhead, Berkshire SL6 1RL
United Kingdom

Published in Canada