Common Criteria Configuration Guide

BlackBerry SecuSUITE 4.0
CACI SteelBox 4.0

Version 1.5

Contents

1. Acronyms

Term	Definition
CCTL	Common Criteria Testing Laboratory
CLI	Command Line Interface (Local console and SSH access)
CRL	Certificate revocation list
CSR	Certificate signing request
ECC	Elliptic curve cryptography
NDCPP	Network devices collaborative protection profile
RSA	Rivest-Shamir-Adleman cryptosystem
RTP	Real-time transport protocol
SCA	Secure client authentication
SGLVN	SecuGATE LVN
SSH	Secure shell
TOE	Target of evaluation
TSF	Target of evaluation security function

2. References

Ref.	Document
[A]	SecuGATE Common Criteria User Guide version 1.0
[B]	Protection Profile for Application Software Version 1.3
[C]	Extended Package for Voice and Video over IP (VVoIP) Version 1.0
[D]	SecuSUITE Client Security Target Version 0.8

3. Document history

Version	Date	Status	Author	Comments
0.9	06-Dec-2019	Draft	BlackBerry	For Gossamer review
1.0	19-Dec-2019	Final	BlackBerry	Including updates based on observations from Gossamer Security Solutions
1.1	27-Jan-2020	Final	BlackBerry	Including updates based on review comments from the evaluator.
1.2	30-Jan-2020	Final	BlackBerry	Added clarification for breakout calls
1.3	30-Jan-2020	Final	BlackBerry	Final version
1.4	13-Jan-2021	Draft	BlackBerry	Added SteelBox client related information
1.5	26-Jan-2021	Final	BlackBerry	Security Target Reference Updated

4. Variants of the TOE

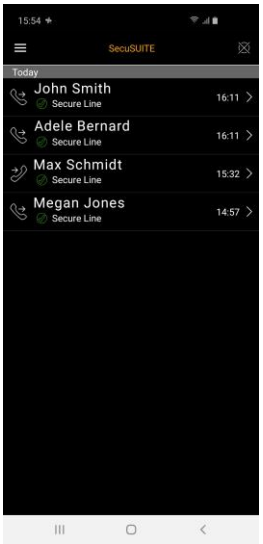
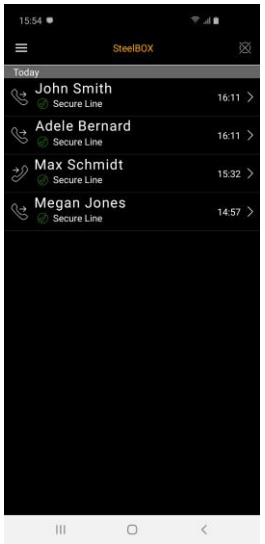
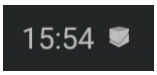
The TOE is represented either by an instance of the BlackBerry SecuSUITE 4.0 application or the rebranded CACI Steelbox 4.0 client. Both representations are identical from functional perspective and only differ in the look and feel and from App Store publishing perspective (separate product and publisher).

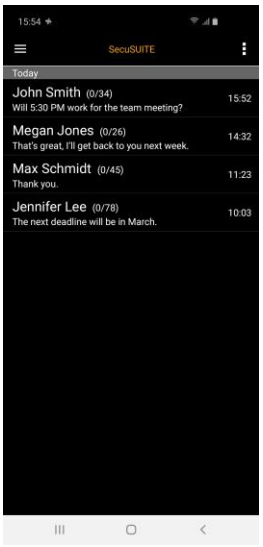
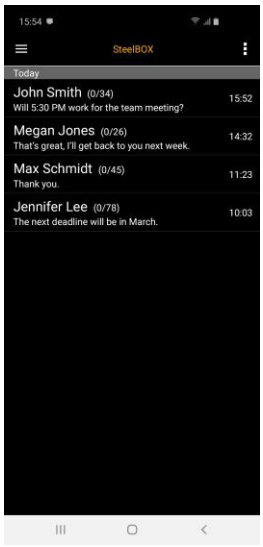
Compared to the BlackBerry SecuSUITE client, the SteelBox variant has:

- Updated Product Name shown in headlines and notifications (where applicable)
- Application package names used for App Store publishing
- Own start-up splash screen and EULA text
- Own Status icon (used in status bar and notification center)

All configuration guidance provide in this CC documentation refers to the SecuSUITE and CACI SteelBox clients even if only "SecuSUITE" is mentioned in one of the following chapters.

Examples of the graphical deltas between the two representations of the TOE:

UI Screen	SecuSUITE Client	SteelBox Client	Comment
Splash Screen			Different splash screens shown during start-up
Call Log			Product name in header Please note also the different icons in the top status bar: SteelBox:  SecuVOICE: 

UI Screen	SecuSUITE Client	SteelBox Client	Comment
Message View			Different product name in header
Call Screen			Call Screen is identical for SecuSUITE and SteelBox (except for the icons shown in the status bar)

For the reminder of the document the screen shots shown are taken from the SecuSUITE variant of the TOE.

5. General Common Criteria Configuration

The TOE is configured during the client enrollment process performed between the TOE and the BlackBerry SecuGATE 4.0 backend automatically.

Key generation schemes (FCS_CKM.1(1))

Cryptographic keys used for the generation of client TLS certificates are created based on the client configuration submitted by the BlackBerry SecuGATE server (ESC) during initial client enrollment. The configuration is defaulted in SecuGATE Server to the usage of NIST p-384 curve and cannot be changed. The client still supports curve p-256 for backwards compatibility for the transition from SecuGATE 3.x to SecuGATE 4.0.

The key generation scheme used during TLS related key establishment is selected by the SecuGATE and defaulted to NIST p-384 and cannot be changed. Please see paragraph 7.7.2 and 7.7.3 of [A].

Key establishment scheme (FCS_CKM.2)

The TOE supports only ECDHE as key establishment scheme.

TLS configuration (FCS_TLSC_EXT.1.1)

By default, the TOE supports only TLS 1.2 and offers two cipher suites (TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 and TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) for the trusted connections to the ESC. The cipher suite is selected by the SecuGATE server during TLS handshake and currently defaulted to TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 and cannot be changed in the SecuGATE.

Hashing

The TOE uses SHA-1 for the SRTP cipher suite, SHA-256 for SIP Digest Authentication via TLS and SHA-384 for the TLS cipher suites. The applied hashing functions cannot be configured by the security administrator.

X.509 Certificates for mutual authentication (FCS_TLSC_EXT.2 and FIA_X509_EXT.2.1)

The TOE is provisioned with X.509 certificates to be used for mutual TLS authentication during the initial client registration process executed between the TOE and the SecuGATE server. The initial registration process is described in chapter Activating the SecuSUITE app.

Used cryptographic engine

The TOE uses a build-in OpenSSL cryptographic engine and utilizes NIST approved algorithms. The version and type of the cryptographic engine cannot be changed by the security administrator or SecuSUITE user.

6. Security Functionality covered by the Common Criteria Evaluation

The security functionality that has been covered by the common criteria evaluation relates to the claims outlined in the SecuSUITE Security Target document [D]. These claims cover, for instance, TLS trusted channels, including x.509 authentication, certificate validation and signature checking.

Additionally, to those claims, the SecuSUITE client implements end-to-end protection of the SRTP session key exchanged between the caller parties. This scheme is on top of the standard SDES/SRTP scheme demanded by the VVoIP Extended Profile [C] and, as a result, **not covered** by the common criteria evaluation of the SecuSUITE client.

The related key generation and certificate validation schemes applied for the end-to-end protection utilize the same implementation as the related schemes used for the TLS protected trusted channels. However, the end-to-end protection of the SRTP session key has not been explicitly tested by the CCTL during the evaluation.

Breakout and Secure Landing Calls

Besides the peer to peer calls between SecuSUITE clients registered to the same infrastructure, the TOE together with the SecuGATE server allows forwarding of secure calls to a PBX within a secure network.

For that the SecuGATE administrator can configure call forwarding to endpoints reached through a PBX (another SIP server connected to local/internal landline phones and potentially connected to outside phone lines). If so configured, a SecuSUITE client can then place calls to additional endpoints beyond the SecuGATE through the configured PBX; however, because the call signaling and call data travels beyond the SecuGATE itself, its security ultimately lies beyond the SecuSUITE client and SecuGATE SIP server's control.

The SecuSUITE client differentiates between calls deemed secure (called "Secure Landing") and calls that are considered unprotected as they're routed potentially unencrypted to external numbers over untrusted networks (called "Breakout").

The ability of the SecuGATE SIP server to route calls to additional endpoints through a PBX lies beyond the scope of this ASPP13/PKGTLS11/VVoIPASEP10 evaluation and is not covered by the common criteria evaluation of the SecuSUITE client

7. Setting up secure voice communication with SecuSUITE

With SecuSUITE®, you can make high-security calls on your Android™ or iOS® device, no matter which network you're connected to. Your calls are encrypted end-to-end and protected against eavesdropping.

Important: SecuSUITE is based on a BlackBerry SecuGATE voice infrastructure that your organization must provide. Any user of the app must be registered to the SecuGATE server to activate SecuSUITE. This must be set up by your administrator.

If you download SecuSUITE yourself, you can easily perform the activation (Installing and activating the SecuSUITE app). After successful activation, you can use the app for end-to-end encrypted voice communication.

To use SecuSUITE, you'll need an internet connection (Wi-Fi or mobile data).

8. Installing and activating the SecuSUITE app

Before you can use the SecuSUITE app, your administrator must create an account for you. When your account is created, your administrator provides you with the activation code and the URL of the server (Authentication Server), which you need to register the app on your smartphone.

8.1. Supported devices and firmware

The evaluated configuration covers following devices and firmware

Brand	App Version	Devices	Firmware
Apple®	4.0	**iPhone®** 8, 8 Plus, X, Xs, Xs Max, XR	iOS® 12
Android™	4.0	**Samsung® Galaxy** S9, S9+, S10, S10+, Note9, Note10	Android™ 8.0 and 8.1

8.2. Overview: Steps to set up the SecuSUITE app

To set up the SecuSUITE app, you'll need to perform the following actions:

1. Download and install the app.
2. Enter the activation code and SCA server URL.
3. If you don't have a screen lock until now, you'll be prompted to set one (e.g. fingerprint, pattern, or password).

8.2.1. Installing the SecuSUITE app

When your administrator creates your SecuSUITE account, they will provide you with your activation code and the SCA server URL.

1. Open the app store for your device and search for 'SecuSUITE'.
2. Download the app.
3. Tap 'Install'.
4. After the installation completes, tap on 'Open'.
5. You are prompted to give SecuSUITE several permissions: contacts, microphone, manage phone calls, manage storage, and notifications.

Note: In iOS, you will not see all requests immediately, since iOS will ask for permissions as necessary, e.g. for microphone only when making a call.

9. Activating the SecuSUITE app

After you install the SecuSUITE app, you must activate it. You'll need the activation code and the address of the SCA server which is part of your organization's infrastructure. Both are provided to you by your SecuSUITE administrator. To simplify this process, a QR code is included into the activation email sent to you by your administrator. The QR code appears under step number 3 of the activation email, and it will look similar to this:

After successful activation, you can make end-to-end encrypted phone calls and send secure text messages to other SecuSUITE users.

Note: The app will be secured by a mandatory screen lock. The activation process is easier if you set the screen lock before you start it (Setting a device screen lock).

1. Open the SecuSUITE app. You'll see the activation screen.
2. Accept the permissions from the app when prompted.
3. At the activation prompt, you can activate by using a QR code or by manually typing the activation code and the server URL in the activation email. (Note: If you select the QR option, you may be required to accept a permission prompt, tap 'ALLOW').

   To use the QR code, tap the QR-code icon and aim your smartphone within the provided area to capture the QR code image (Below is a **sample** QR code, please make sure that you scan the one provided on your activation email). Without the QR code, simply type in the activation code and SCA server URL that is provided on the email.

   Note: The TOE uses the URL entered by the user or derived from the QR code information as a reference identifier for the TLS certificate validation.
4. You'll see the activation processing.
5. The 'SecuSUITE Client Addendum' is displayed. Please read it carefully. At the bottom tap the box next to 'I agree to the terms …' ⇨ 'I Agree'.
6. If your device wasn't secured with a screen lock until now, you are prompted to set this before proceeding (Setting a device screen lock).
7. After the completed activation, SecuSUITE opens. If your administrator configured the need for an additional layer of security, you are prompted to define a PIN for the app. This can be replaced by your fingerprint, if you consent the next notification with your fingerprint.
8. The next step depends on the setting in the server.
   - Your phone contacts are loaded as contacts in the app. None of them are marked with a padlock yet.
   - All active SecuSUITE contacts from your organization are displayed as contacts in your app. All contacts are marked with a grey and open padlock.

9.1.1. Setting a device screen lock

Android™

1. Open system 'Settings' ⇨ 'Lock Screen and Security' ⇨ 'Phone Security' ⇨ 'Screen Lock Type'
2. Select one or more types of locks: Pattern, PIN, Password, or Fingerprint.
3. Define the screen lock.

iOS®

1. Open system 'Settings' ⇨ 'Touch ID and Passcode'
2. Select one or more types of locks: Pattern, PIN, Password, or Fingerprint.
3. Define the screen lock.

Note: Your system administrator may enable an additional layer of protection to the SecuSUITE app, in addition to the device-wide locking mechanism that you selected above. This can be chosen the first time you activate the app, and it can either be a PIN or, as an alternative, a fingerprint prompt.

9.1.2. SecuSUITE app can be configured to need an additional layer of security

If more restriction is desired for the protection of the SecuSUITE app, a separate PIN request can be activated by your administrator.

During the activation process, you will need to select an additional PIN, exclusive to the SecuSUITE app. Additionally, you can also associate your fingerprint, as an alternative to the PIN. Every time access to the app is requested, either the PIN or the fingerprint must be used.

10. Secure Calls

SecuSUITE does not interact with the phone app of your device. You can make regular phone calls as usual.

Your phone number for SecuSUITE is set by your administrator. This is not necessarily the number from the SIM card, but in most cases it makes sense to also use this for SecuSUITE, so that other SecuSUITE participants can reach you with the same number. Because this number is also transferred during a call, your name is already assigned to it if the call recipient saved you as a contact.

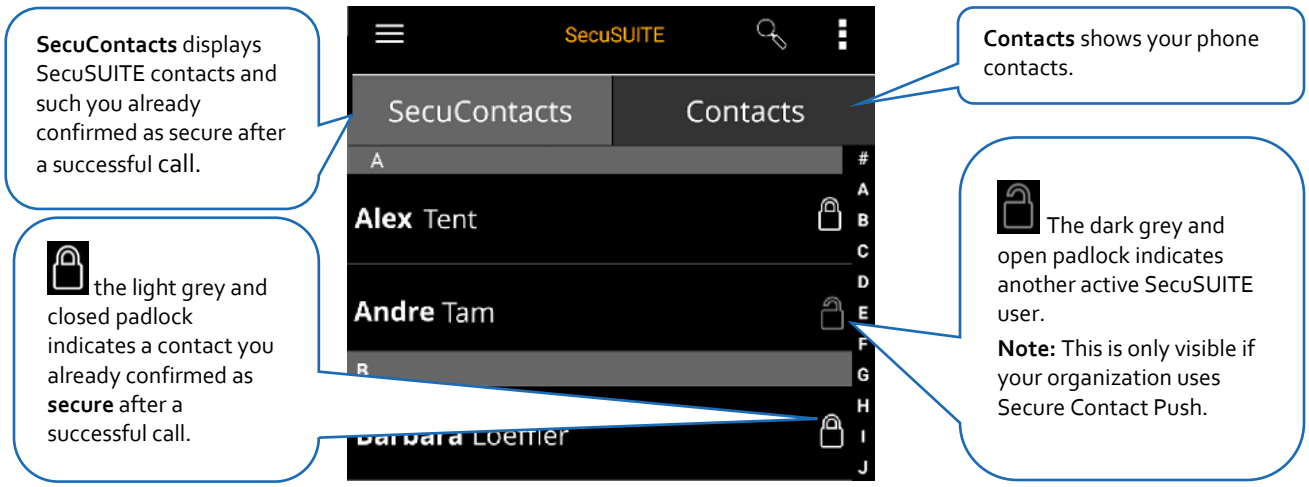
Note: To check the phone number assigned to your SecuSUITE account, look in the SecuSUITE menu ⇨ 'Settings' ⇨ 'Account' ⇨ 'Account Number'.

Secure calls require a stable data connection. Either Wi-Fi or mobile data will work. If SecuSUITE isn't connected, a red bar is shown with 'No server connection' and a disconnect icon is shown in the notification tray. When SecuSUITE is connected, the logo will display clearly in the notification tray. You can try to reconnect by switching between Wi-Fi and mobile data

10.1. Your contacts in the app

When you open the SecuSUITE app, the 'contacts' screen is shown. The contacts in there are split in two tabs:

- **SecuContacts**: This displays all contacts you have saved as **secure** and **SecuSUITE-contacts**, i.e. contacts from other SecuSUITE users.
  Note: The display of the SecuSUITE contacts depends on the activation of Secure Contacts Push (SCP) in your organization
- **Contacts**: This shows the contacts from your native phone app.



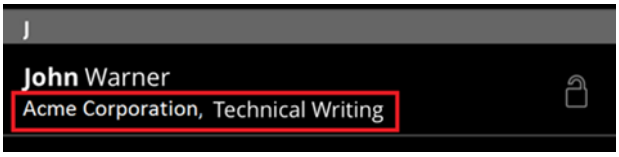
Note: If you do not see the split tabs, drag the screen slowly down until they appear.

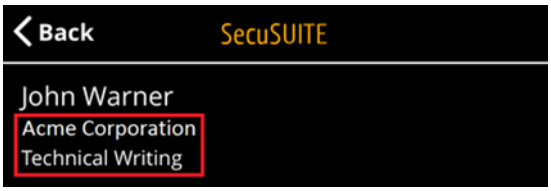
10.1.1. Display of company and department information

Within your SecuSUITE contacts in the SecuSUITE app, you can now see additional information about your contacts. Aside from the name, the contacts screen also shows **company** and **department information**. To view this information, it is necessary that a User Administrator added the information in the SecuSUITE backend. You as a user of the SecuSUITE app cannot add information regarding company and department to your SecuSUITE contacts.

Once added, this is how the information looks in your SecuSUITE app:

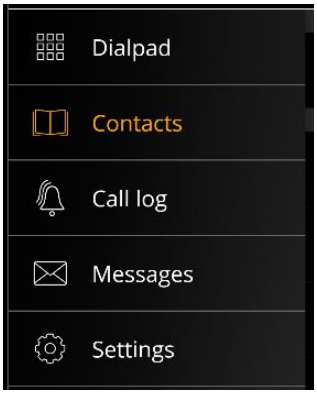
This is how it looks in the **contact's overview:** And this how it looks in the **contact's details:**





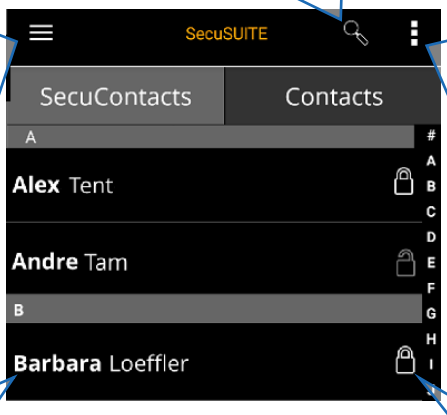
10.2. Home screen and call options

Tap the menu to access the dial pad, call log, and settings.



Search for contacts by name.

The **iOS** client has a permanently visible search field above the contact's tab.



This context menu offers two features:

- Sort your contacts by first or by last name.
- Update the contacts in the active contact's tab.

On iOS®: the context menu is displayed in the bottom right-hand corner:

Tap on a contact to open the details. Then you can select to make a call or send a message.

The closed padlock icon shows that this is a secure contact, which you confirmed after a successful secure call.

10.3. Making a SecuSUITE call

Secure calls can be made to **another user** of SecuSUITE in your organization. There are additional types of secure calls, e.g. to landline numbers inside the protected network of your organization (**Error! Reference source not found.**).

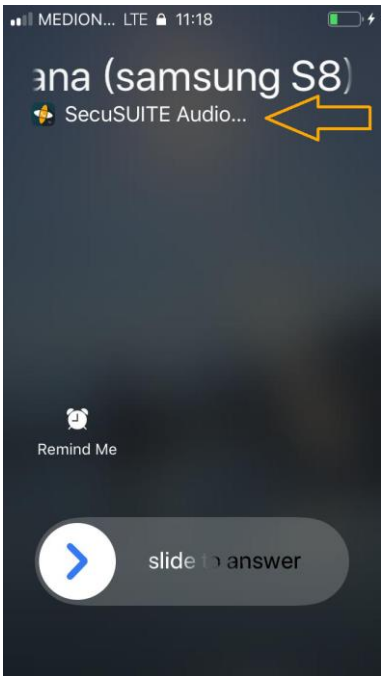
As soon as the recipient accepts your call, a secure connection is established. You can verify the status of encryption by watching the circle around the lock icon on the screen (Icons for call status).

10.3.1. Call Integration on iPhones

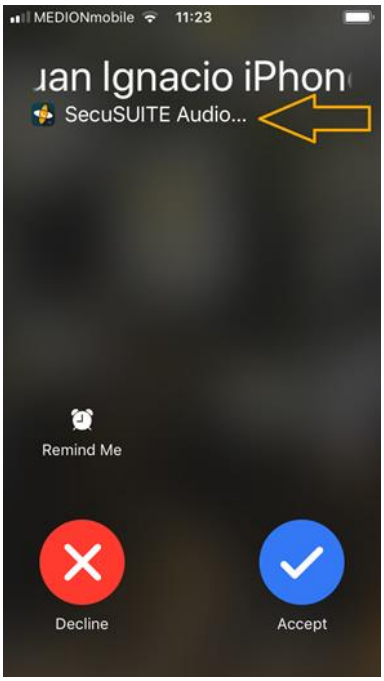
For iOS devices only, SecuSUITE uses CallKit Support. SecuSUITE calls will show on the screen like an ordinary iOS call, and can be handled like a normal call.

Incoming call with SecuSUITE:

on locked screen



on unlocked screen



Ongoing call with SecuSUITE:

10.3.2. Icons for call status

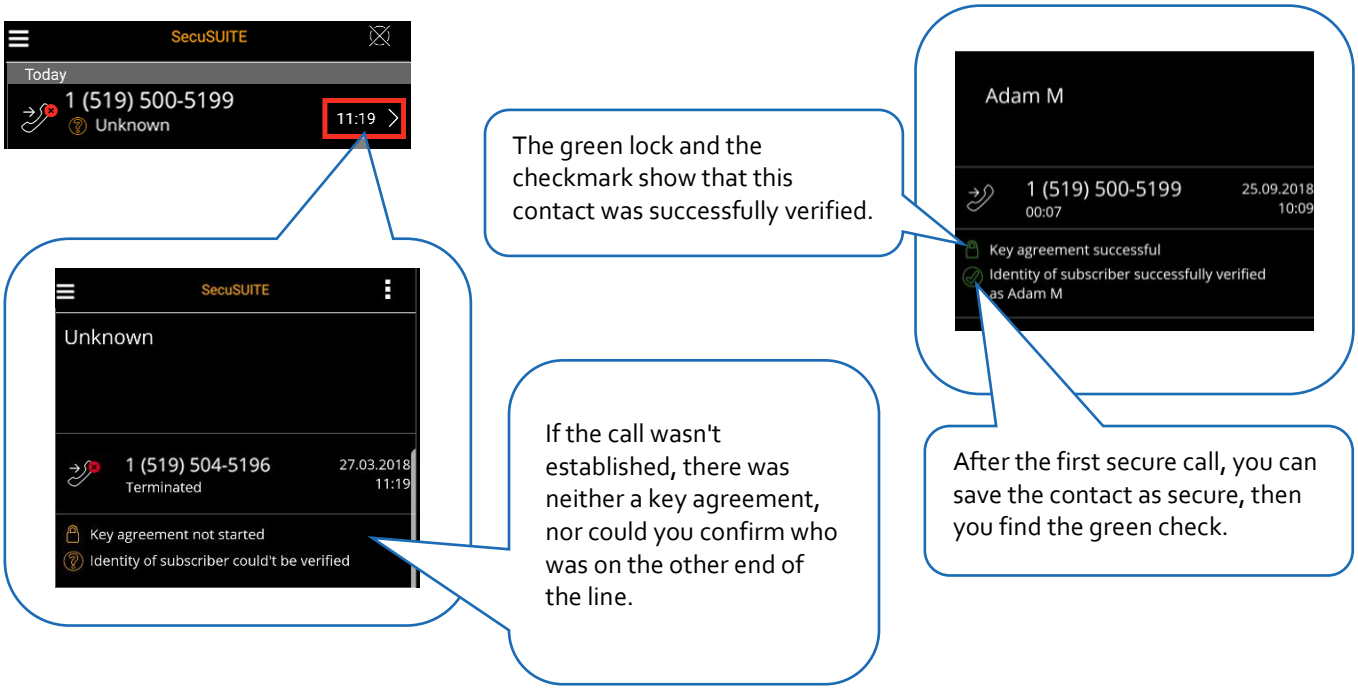
	Incoming/Outgoing call ringing	Key-agreement	Secure call
	Call is ringing.	Call accepted. A secure connection is being established.	A secure connection (mobile to mobile or secure work line) is now established. You can start talking.
Android™ & iOS®			

Note: You'll see the same symbols whether you are making or receiving a call. You can start speaking as soon as the lock icon is closed.

10.3.3. Information about call participants (examples)

Important information about the other participant is transmitted even in a call attempt. It is displayed on the call screen and later in the call log.

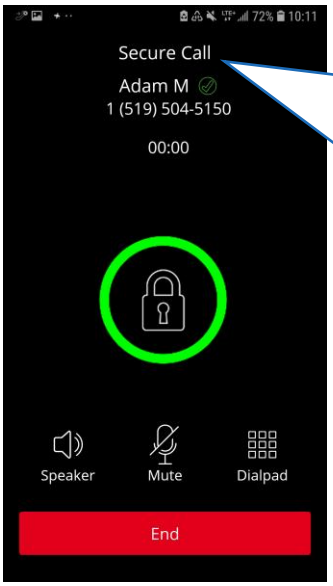
In the call log, you'll see all available details when you tap on the icon (Android™: > iOS®: ⓘ) next to a name:



10.3.4. Authentication

During call setup, authentication features including call number are securely transferred and can be trusted. However, the name of your contact must be confirmed (and/or created) separately (Saving a secure contact).

SecuSUITE shows the status of authentication through different icons:



The icon next to the name shows the authentication status:

This contact was not yet confirmed as secure contact.

This contact is a secure contact.

This contact is a secure work line contact.
(G = Gateway)

10.4. Accepting secure calls with SecuSUITE

10.4.1. SecuSUITE background operation

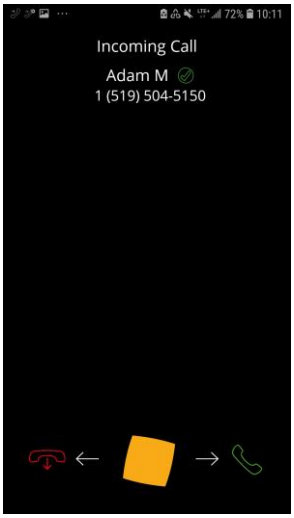
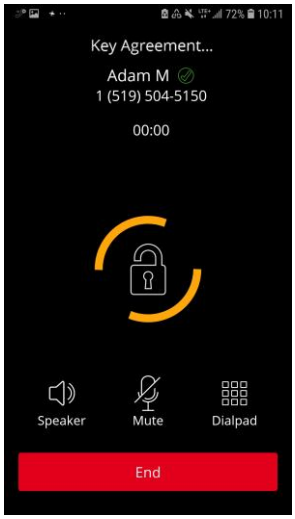
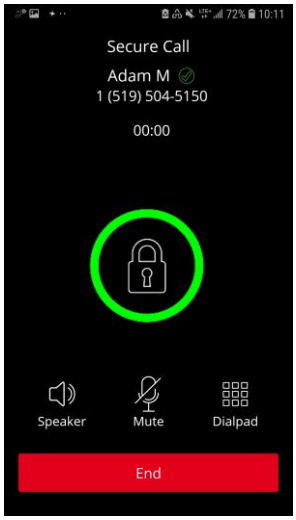
To ensure your device receives secure calls via SecuSUITE, the app runs in the background, even when locked. To do this, SecuSUITE needs an active data connection.

On Android™, a notification indicates that SecuSUITE is connected:

SecuSUITE is disconnected	**SecuSUITE is connected**
	

Note: After rebooting your device, SecuSUITE will prompt you to enter your device password to verify your identity.

10.4.2. Receiving calls

Slide the middle icon to the right to accept the call. If your device is locked, you'll be asked to unlock it first.	Wait while the key agreement is performed.	The call is active. You can now start talking.
		

After the first secure call with a number, the app asks you to save this contact as secure contact (Saving a secure contact).

Note: On iPhones a secure call that you receive with a locked screen looks like an ordinary iPhone call except for the banner 'SecuSUITE Audio'.

10.4.3. Receiving concurrent calls

SecuSUITE and the phone app of your device are not connected. Concurrent call attempts lead to the following scenarios:

- **While you are in a call using the native phone app, someone calls you with SecuSUITE:** The caller hears the sound for an occupied line, and their call attempt is aborted. In the status bar of your device, you'll see the icon for a missed call from SecuSUITE.

  Note: If you don't want to see missed calls from SecuSUITE in the status bar, turn it off in the SecuSUITE settings (Settings).

- **You are in a secure call with SecuSUITE while someone calls you with SecuSUITE:** The caller hears the sound for an occupied line, and their call attempt is aborted. In the status bar of your device, you'll see the icon for a missed call from SecuSUITE.

- **You are in a secure call with SecuSUITE while somebody calls you with the phone app:** The call with the phone app shows on the display of your device. Accepting it will abort the SecuSUITE call. Decline the native call if you want to continue your SecuSUITE call.

10.4.4. Placing SecuSUITE calls in the background

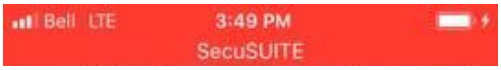
You can put an active SecuSUITE call in the background if you tap 'home' or 'recent apps'. You can continue to use your phone while the call is active.

To bring the call back to the foreground, tap on the overlay.

The different overlays for Android and iOS appear on the right.

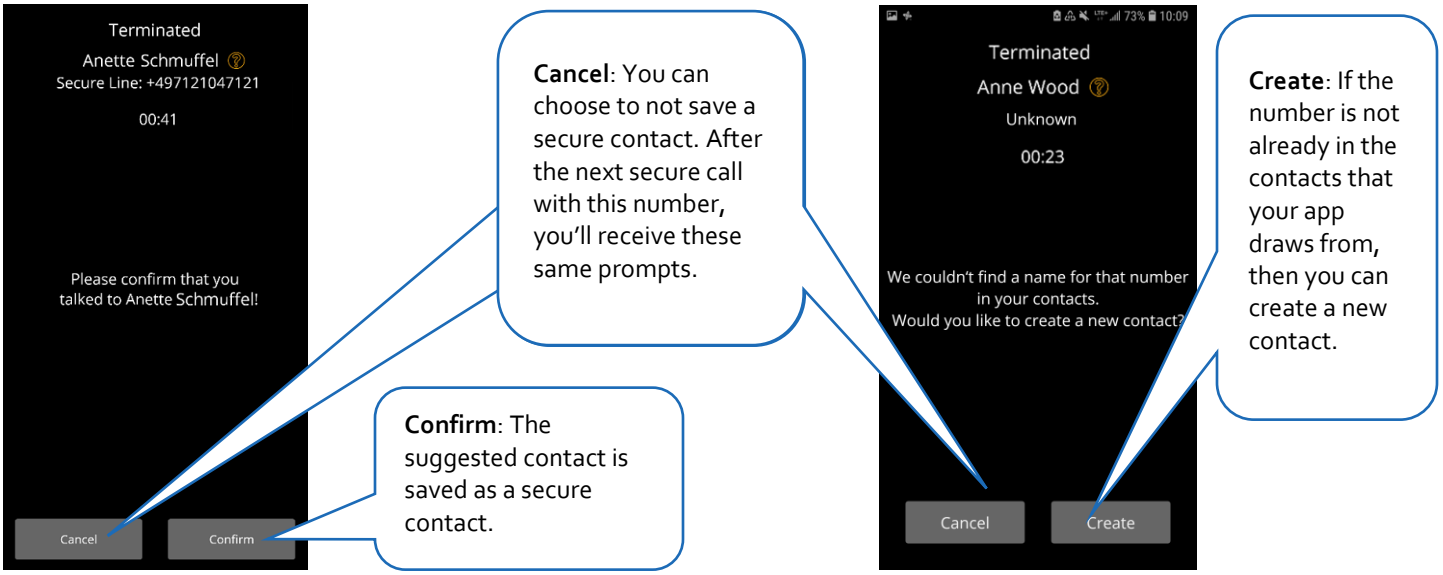
Android™

iOS®



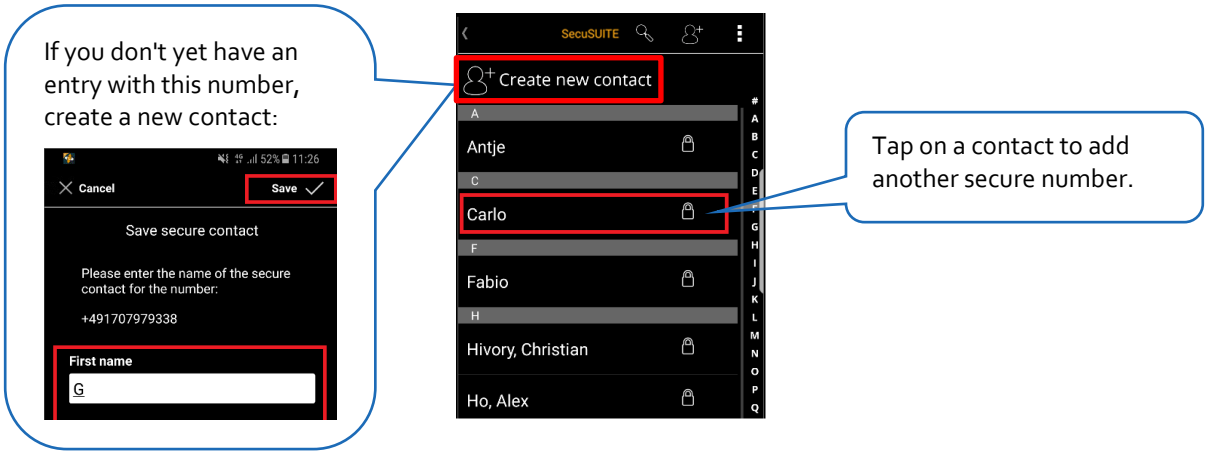
10.5. Saving a secure contact

If it did not happen automatically after a secure call, you can save contacts as **secure** manually after you have had a secure call with them. If they are not known in your contacts yet, you can either create a new contact or add a number to an existing contact.



10.5.1. Create a new contact

- **Cancel**: You can always decline saving a secure contact. After the next secure call with this number, you'll see the same prompt.
- **Create**:



Note: You can save several numbers to one contact entry. Select a contact name to assign the new number. The old number will remain associated with this contact.

11. Managing secure contacts

The handling of contacts by SecuSUITE depends on a setting in the server called **Secure Contacts Push**. This decides which categories of possibly secure contacts you will find on your phone:

- **all active SecuSUITE contacts** from your tenant inside the organization
- all contacts you confirmed after a successful SecuSUITE call as **secure contacts** (Saving a secure contact).

Additionally, you will find your phone contacts also displayed in your SecuSUITE contacts inside the 'Contacts' tab.

11.1. Understanding contacts in the SecuSUITE app

If you see contacts **marked with a grey and open padlock** in the 'SecuContact' tab, the push of SecuSUITE contacts to your app is enabled. You see all active SecuSUITE users from your tenant in the organization in your 'SecuContact' list.

It is not possible to change the data of one of those contacts because they are managed by the administrator at the SecuSUITE server. Changes made in the backend are synchronized daily, but you can update them manually by tapping on the 'context menu' dots (on iOS these are found on the right bottom corner, these pictures here show Android) and 'Update contacts'.

After the first secure call with another contact, you are asked to confirm the person you spoke with. Once you confirm that this is a 'secure' contact, they are marked with a **white and closed padlock** next to the name.

11.1.1. VIP users and contacts

VIP users are persons who don't want their contact data spread. When marked as VIP by the admin, their contact details will not be transferred to other users of their tenant. However, it is possible to call them securely, once you know their phone number, and save them as secure after a successful SecuSUITE call.

Note: When you are a **VIP** user, just be aware that, although you see all contacts from your tenant in your contact screen, they will not see you there. If you want to make secure calls with someone, it's easiest to start the first call. After the first successful call, the other user can save your contact as secure and is, from that moment on, able to call you in the future.

Exception: VIP users can see other VIP users of their tenant in the contact list.

11.2. Understanding contacts in the SecuSUITE app imported from phone contacts

The SecuSUITE app receives contacts from your native phone app and displays them in the **Contacts** tab of the contacts screen. When you update your native phone contacts, these changes are shared with SecuSUITE in the next contacts update, which occurs daily or can be triggered by yourself. You cannot edit contacts that come from within the SecuSUITE app.

If a contact from your phone if reachable via SecuSUITE, a secure call is started from the app. After the first secure call, you can save a contact as a 'Secure' contact (

Saving a secure contact). These are then shown in the SecuSUITE contacts list in the tab 'SecuContacts' and are marked with a closed padlock.

11.2.1. Editing or deleting contacts

All contacts in the app but those you created yourself can neither be edited or deleted. SecuSUITE contacts are managed in the backend, changes will be updated in your app. Phone contacts have to be edited or deleted in the phone app, changes here will also be updated in the SecuSUITE app.

12. Call settings

12.1. Switching Bluetooth on or off

SecuSUITE **cannot secure** the connection to a via Bluetooth connected headset or a hands-free speaking system. The data transfer via Bluetooth is vulnerable to tapping, and this is the reason that it is **by default deactivated**.

If you are aware of the security risk, but still want to use Bluetooth for SecuSUITE, you can switch it on:

1. Tap on 'Settings' in the SecuSUITE menu ⇨ 'Security'.
2. To enable or disable Bluetooth for SecuSUITE, tap on the switch 'Allow Bluetooth'.
3. If you are about to allow Bluetooth, a notification warns you of the risk ⇨ 'OK'.

Important: Even secure SecuSUITE calls via Bluetooth are not suited for RESTRICTED content! You must tell this to your associate **at the beginning of the call**!

12.2. Account information

In 'Account' you'll find all the details of your current account in SecuSUITE.

Under certain conditions, your administrator will ask you to re-activate your account. First, you'll have to delete your account by tapping on 'Remove'.

Note: Removing the account will **not** remove your secure contacts and call log.

13. Secure Messaging

You can exchange end-2end protected secure text messages with other users of SecuSUITE.

13.1.1. Send a secure text message

1. Tap a contact in SecuSUITE.
2. Tap 'Send Message'.
3. Type your text in the field 'New Message'.
4. Tap 'Send'.

You can also select the item 'Messages' in the menu. There, you'll find an overview of your conversations. You can tap on a thread to add a new message.

14. Settings

14.1.1. Notifications (Android™)

You can decide which SecuSUITE notifications you want to get by default, you'll be notified about missed calls and messages.

1. In the SecuSUITE app menu, tap 'Settings'.
2. Tap 'General'.
3. To see notifications about missed calls switch 'Missed calls' to active.
4. To see notifications about secure messages switch 'Secure messages' to active.

14.1.2. Notifications (iOS®)

To enable or disable notifications, navigate to your phone's 'settings' ⇨ 'SecuSUITE'. From there, you can control whether you want SecuSUITE to notify you with sounds, and whether message alerts will appear on your lock screen.

Important: If you disable notification on iOS, the user will **not be noticed of any incoming calls**. This setting will disable **all** notifications.

15. SecuSUITE Client Updates

BlackBerry provides timely security updates for the TOE in case vulnerabilities have been discovered. Reported vulnerabilities and defects are investigated and rated based on the potential thread and then scheduled for an upcoming bug fix or roadmap release. The time between disclosure of a vulnerability and the availability of a security update is minimum 10 days (due to the app store publishing process) and BlackBerry aims for a maximum of 50 days. In case of low-risk security issues updates may be provided later as part of a regular release.

BlackBerry is accepting reports about potential vulnerabilities of the SecuSUITE client via the HTTPS protected BlackBerry contact form: https://www.blackberry.com/us/en/forms/enterprise/contact-us.

Update of 3rd party libraries

For all included 3rd party libraries, BlackBerry checks regularly for release updates that would address vulnerabilities that have been discovered and published for that component (e.g. via https://nvd.nist.gov).

Depending on the classification of the vulnerabilities and impact to the SecuSUITE product, BlackBerry provides updated client releases that include those fixes in a timely manner.

As soon as the fix release is available for the 3rd party component, BlackBerry plans the integration of the updated component release for one of the upcoming SecuSUITE client releases. The time between the public availability of a 3rd party component vulnerability fix and the availability of the SecuSUITE client update is minimum 10 days (due to the app store publishing process) and BlackBerry aims for a maximum of 50 days. In case of low-risk security issues updates may be provided later as part of a regular release.

15.1. Client Software Version

To validate the current version of the SecuSUITE application, please go to **Settings > About SecuSUITE.** Alternatively, the version number can be validated also in the platform application manager

Android™:

Settings > Apps > SecuSUITE (version information at the bottom of the page)

iOS®:

Settings > General > iPhone Storage > SecuSUITE (version information is shown next to the app icon)

15.2. Client update via App Stores

Once available, the client updates are offered via the public application stores. To validate the current version of the SecuSUITE application, please go to **Settings > About SecuSUITE.**

Update of the Android™ client:

1. Open Google Play Store Application
2. Go to 'My Applications'
3. In case an update is available, the SecuSUITE application is listed under "Updates pending" section
4. Tap on "Update" to initiate the download and installation of the new release.
5. The Play Store application shows the progress of the download and installation
6. Once the installation is complete, the user should validate the release number within the SecuSUITE client in **Settings > About SecuSUITE**

Note: The OS platform automatically validates the application signature that is included in the installation package. In case the signature does not match the certificate of the installed application, the client update process is terminated by the OS, and the user is notified.

Update of the iOS® client

1. Open App Store Application
2. Tap on "Updates" tab
3. In case an update is available, the SecuSUITE application is listed under "Updates pending" section
4. Tap on "Update" to initiate the download and installation of the new release.
5. The App Store application shows the progress of the download and installation
6. Once the installation is complete, the user can validate the release number within the SecuSUITE client in **Settings > About SecuSUITE**

Note: The iOS platform automatically validates the application signature before the update is installed. In case the signature does not match the certificate of the installed application, the client update process is terminated by the OS, and the user is notified.

16. SecuSUITE FAQ

What if I can't hear call audio?

You may not be able to hear call audio if your Wi-Fi network has not opened the required ports. You can attempt your call over mobile data, and if the issue persists, contact your network administrator.

What's my phone number?

The telephone number assigned to your account is not necessarily the same as the phone number of your SIM card, as the administrator is free to define another phone number. Usually, both phone numbers are the same. To find out which phone number is assigned to your SecuSUITE account, look in the SecuSUITE menu 'Settings' ⇨ 'Account' ⇨ 'Account Number'.

So that you can receive secure calls from the inside of your organization's protected call environment, your administrator defines a callback number for you. This is not visible in SecuSUITE Settings.

What prefixes do I need to dial?

An international prefix is only necessary for international numbers. Numbers which are dialed without a prefix are automatically completed with your national prefix.

To make secure calls into the protected PBX of your organization, you can use specially defined short numbers. Your administrator will provide you with these numbers.

What does each sound notification mean?

Action/Situation	Sound Notification
Call establishment	deep triple tone
Call ringing	single long, ringing tone
Key agreement	Repeated, short double tone
Connection established	single high tone
Call end	descending double tone
Your callee is already in a phone call	busy tone
Phone or app of the callee is either not active or outside of network	'The person you have called is temporarily unavailable.'
PIN entry needed	"Please unlock"

Why can't I see the contact of an important person in my tenant?

Maybe this person was marked as 'VIP' by the administrator. In this case, their contact data is not shared automatically. If you have their number (or they call you first), you can save it as secure after the first communication and find it in your contacts from then on.

17. Legal Notice

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 Limited

2200 University Avenue East

Waterloo, Ontario

Canada N2K 0A7

BlackBerry UK Limited

200 Bath Road

Slough, Berkshire SL1 3XE

United Kingdom