Qualcomm Technologies International, Ltd.

BR/EDR and Bluetooth Low Energy Technology Secure Connections

User Guide

80-CF168-1 Rev. AA

October 27, 2017

Qualcomm Technologies International, Ltd. (formerly known as Cambridge Silicon Radio Limited) is a company registered in England and Wales with a registered office at: Churchill House, Cambridge Business Park, Cowley Road, Cambridge, CB4 0WZ, United Kingdom.
Registered Number: 3665875 | VAT number: GB787433096

Revision history

Revision	Date	Description
1	SEP 2016	Initial release. Alternative document number CS-00345503-UG.
2	APR 2017	Updated for ADK 4.2 and added to the Content Management System.
AA	OCT 2017	Document Reference Number updated to use Agile number. No technical change.

Contents

Tables

Figures

1 Secure Connections - overview

The Secure Connections (SCs) feature is included in ADK 4.1 and later versions.

It is enabled at boot time, during initialization. If Secure Connections is supported then QTIL recommend that the application initializes with Secure Connections.

If the host and controller of both devices in a point-to-point connection support Secure Connections is always used. If either the host or controller of one device does not support Secure Connections, a non-SC link is used.

Secure Connections Only Mode is also a device property enabled at initialization. Secure Connections Only Mode cannot be disabled without warm-resetting or power-cycling the device. An attempt to reinitialize the Connection library at run time does not disable Secure Connections Only Mode. Secure Connections Only Mode is a single setting that applies to both Bluetooth low energy technology SC and BR/EDR SC.

A Secure Connection has higher security than previously enabled by P192 Secure Simple Pairing (SSP) or legacy Bluetooth security.

BR/EDR Secure Connections is a *Bluetooth Core Specification v4.1* feature that provides stronger authentication and encryption mechanisms to increase the security of a BR/EDR Bluetooth connection.

Bluetooth low energy technology Secure Connections is a *Bluetooth Core Specification v4.2* feature that provides stronger authentication and encryption mechanisms to increase the security of a Bluetooth low energy technology connections. The algorithms used are Federal Information Processing Standard (FIPS) approved algorithms.

NOTE *Bluetooth Core Specification v4.2* also included key generation using Secure Connections on either BR/EDR or Bluetooth low energy technology transport to derive keys that can be used for the other transport. This avoids pairing a second time when connecting using the other transport. Known as Cross Transport Key derivation, it is an optional feature and occurs if the connecting devices negotiate to use a Cross Transport Key.

Table 1-1 Table 1-1 Device support for SC

Transport	CSR8675 Flash	CSR8670 Flash
BR/EDR	Yes	No
Bluetooth low energy technology	Yes	Yes

Table 1-2 lists products that have been tested with the SC feature.

Table 1-2 Table 1-2 SC testing

Transport	Product			
	Headset	Speaker	Soundbar	Audio Dongle (source)
BR/EDR	Yes	Yes	Yes	Yes
Bluetooth low energy technology	Yes	Yes	Yes	No (1)

(1) The Source application in the ADK does not support Bluetooth low energy technology.

2 Pairing behavior with/without Secure Connections

The following BR/EDR/Bluetooth low energy technology pairing scenarios are possible depending on the SC support of the connecting devices.

Table 2-1 Pairing scenarios

Local and remote both support SC on Bluetooth low energy technology	Local and remote both support SC on BR/EDR	Pairing Procedure	Notes on security provided
Yes	Yes	When pairing occurs on a transport the keys for the other transport may be derived, as part of the process. This is optional.	Same Key strength and MITM protection on both transports. The encryption used is AES-CCM
No	Yes	If pairing is initiated on BR/EDR or Bluetooth low energy technology transport, pairing occurs individually on each transport as and when necessary.	The encryption on BR/EDR link is AES-CCM.
Yes	No	Optionally devices may generate BR/EDR keys of identical strength and the same MITM protection as the Bluetooth low energy technology keys as part of the Bluetooth low energy technology pairing procedure. The Link Key bit in the initiator and responder Key Distribution/Generation field of Bluetooth low energy technology Pairing Request/Response sets how the link key is generated. If both devices set the Link key bit to `1`, the procedure for calculating the BR/EDR link key from the Secure Connections Long Term Key (LTK) is used.	Encryption on BR/EDR link is E0 (not AES-CCM).
No	No	Pairing occurs on each transport as and when necessary.	

2.1 BR/EDR/Bluetooth low energy technology pairing scenarios

This section further describes the pairing scenarios.

BR/EDR (SC), Bluetooth low energy technology (SC) supported on both devices

If both the local and remote devices support Secure Connections over BR/EDR and Bluetooth low energy technology transports, and pairing is initiated on a transport then Cross Transport pairing will trigger key generation for the other transport. That is, either BR/EDR or Bluetooth low energy technology SC transport.

BR/EDR (SC) on both devices, Bluetooth low energy technology (SC) on one device

If either the remote or local device does not support Bluetooth low energy technology SC but both support BR/EDR SC and pairing is initiated on BR/EDR transport, then, pairing occurs individually for each transport as and when triggered by the application.

BR/EDR, Bluetooth low energy technology (SC)

If both the local and remote devices support Secure Connections over the Bluetooth low energy technology transport but not over the BR/EDR transport, then the devices may optionally generate BR/EDR keys of identical strength and the same MITM protection as the Bluetooth low energy technology keys as part of the Bluetooth low energy technology pairing procedure.

The encryption on BR/EDR link is not AES-CCM but is E0. The Link Key bit in the initiator and responder Key Distribution/Generation field of Bluetooth low energy technology Pairing Request/ Response sets how the link key for BR/EDR is generated. If both devices set the Link key bit to `1`, the procedure for calculating the BR/EDR link key from the Long Term Key (LTK) is used.

BR/EDR, Bluetooth low energy technology

Pairing occurs individually for each transport as and when triggered by the application.

3 Secure connection pairing

3.1 BR/EDR SC initialization and pairing

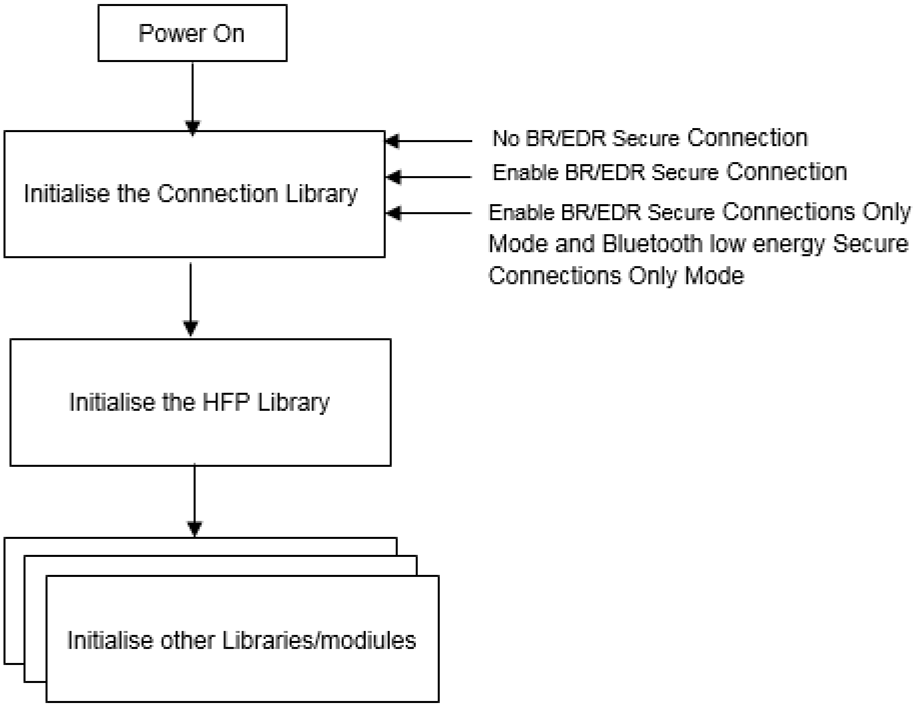

Power On
Initialise the Connection Library
No BR/EDR Secure Connection
Enable BR/EDR Secure Connection
Enable BR/EDR Secure Connections Only Mode and Bluetooth low energy Secure Connections Only Mode
Initialise the HFP Library
Initialise other Libraries/modiules

Figure 3-1 Secure Connections initialization during device bootup

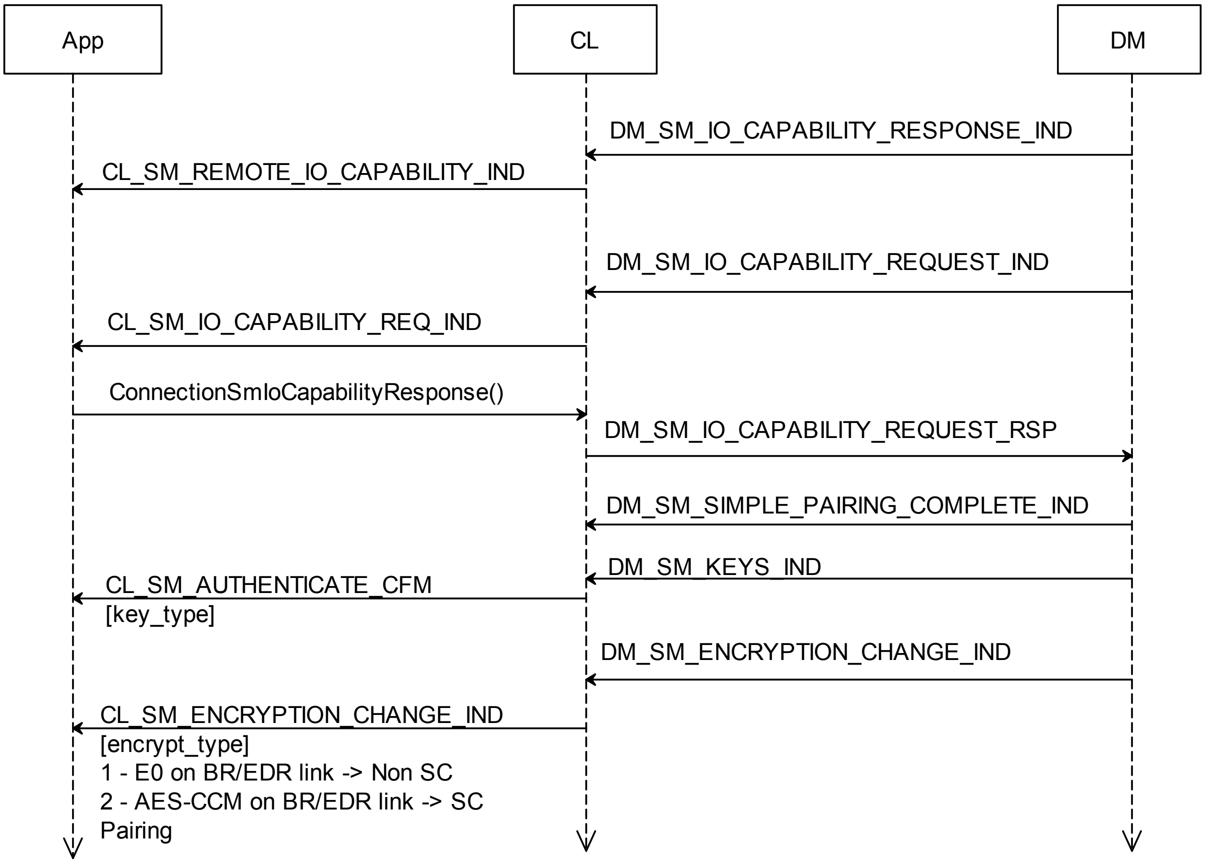

App
CL
DM
DM_SM_IO_CAPABILITY_RESPONSE_IND
CL_SM_REMOTE_IO_CAPABILITY_IND
DM_SM_IO_CAPABILITY_REQUEST_IND
CL_SM_IO_CAPABILITY_REQ_IND
ConnectionSmIoCapabilityResponse()
DM_SM_IO_CAPABILITY_REQUEST_RSP
DM_SM_SIMPLE_PAIRING_COMPLETE_IND
DM_SM_KEYS_IND
CL_SM_AUTHENTICATE_CFM [key_type]
DM_SM_ENCRYPTION_CHANGE_IND
CL_SM_ENCRYPTION_CHANGE_IND
[encrypt_type]
1 - E0 on BR/EDR link -> Non SC
2 - AES-CCM on BR/EDR link -> SC Pairing

Figure 3-2 BR/EDR Secure Connections pairing

The `key_type` information received in the BR/EDR authentication confirmation message is not sufficient to tell whether BR/EDR encryption was secure. For example, the `key_type` could be p256, but AES_CCM encryption, which is required for a Secure Connection, is not enabled on the link. This can happen when the BR/EDR controller does not support Secure Connections and Bluetooth low energy technology SC pairing was initiated first, deriving the link key use to form a BR/EDR transport.

BlueStack indicates the type of encryption algorithm it enabled on the transport link as part of `CL_SM_ENCRYPTION_CHANGE_IND` message sent after the link is encrypted. If BR/EDR SC is supported by both local and remote device, the `encrypt_type` value is 2, that is, AES-CCM encryption is enabled.

If either device does not support BR/EDR SC, then the `encrypt_type` value is 1.That is, E0 encryption is enabled which is non-SC.

If both the devices support BR/EDR SC, and if BR/EDR pairing is initiated first, then it will always be SC pairing and the `encrypt_type` that is used is AES-CCM on the BR/EDR link.

3.2 Bluetooth low energy technology SC pairing

Figure 3-3 shows the message sequence during a SC pairing over Bluetooth low energy technology transport.

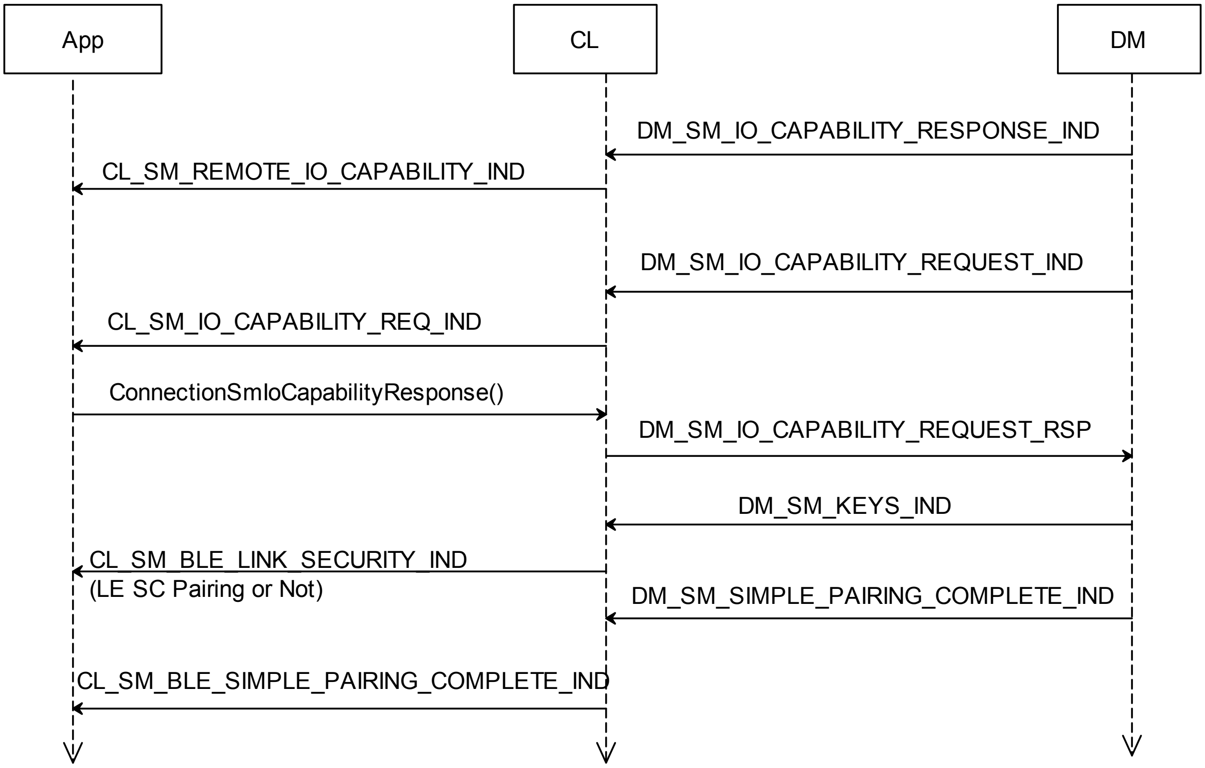

App
CL
DM
DM_SM_IO_CAPABILITY_RESPONSE_IND
CL_SM_REMOTE_IO_CAPABILITY_IND
DM_SM_IO_CAPABILITY_REQUEST_IND
CL_SM_IO_CAPABILITY_REQ_IND
ConnectionSmIoCapabilityResponse()
DM_SM_IO_CAPABILITY_REQUEST_RSP
DM_SM_KEYS_IND
CL_SM_BLE_LINK_SECURITY_IND
(LE SC Pairing or Not)
DM_SM_SIMPLE_PAIRING_COMPLETE_IND
CL_SM_BLE_SIMPLE_PAIRING_COMPLETE_IND

Figure 3-3 Bluetooth low energy technology SC pairing

3.3 Cross transport pairing

If both the local and remote devices support Secure Connections over BR/EDR and Bluetooth low energy technology transports, devices may optionally generate keys of identical strength and the same MITM protection for both transports as part of a single pairing procedure.

If both the local and remote devices support Secure Connections over the Bluetooth low energy technology transport but not over the BR/EDR transport, then the devices may optionally generate the BR/EDR keys of identical strength and the same MITM protection as the Bluetooth low energy technology keys as part of the Bluetooth low energy technology pairing procedure.

Figure 3-4 shows cross transport pairing message sequence when Bluetooth low energy technology transport is used to generate a link key.

3.3.1 When Secure Connections pairing occurs first on Bluetooth low energy transport

Figure 3-4 shows cross transport pairing message sequence when Bluetooth low energy technology transport is used to generate a link key.

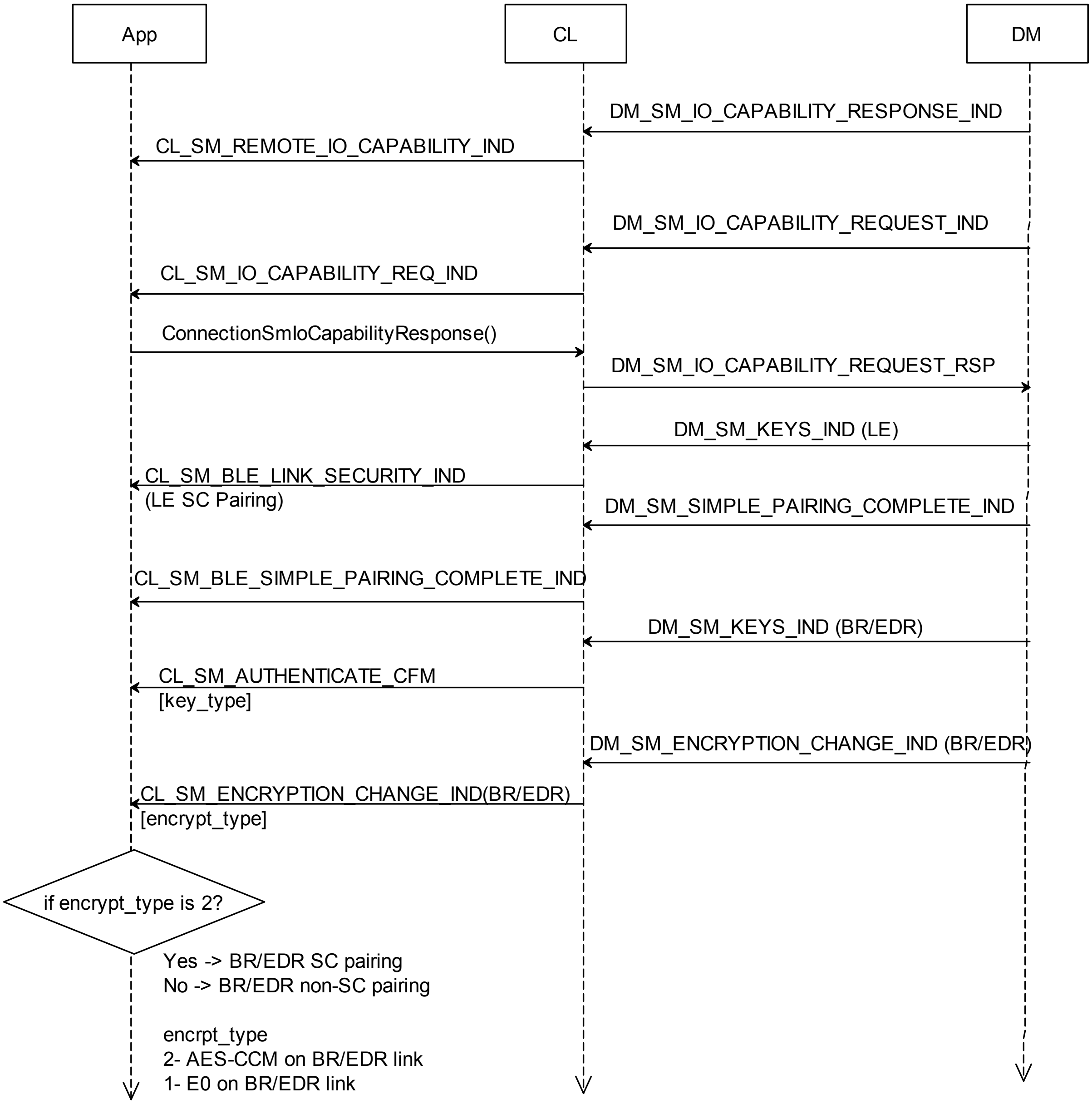

App
CL
DM
DM_SM_IO_CAPABILITY_RESPONSE_IND
CL_SM_REMOTE_IO_CAPABILITY_IND
DM_SM_IO_CAPABILITY_REQUEST_IND
CL_SM_IO_CAPABILITY_REQ_IND
ConnectionSmIoCapabilityResponse()
DM_SM_IO_CAPABILITY_REQUEST_RSP
DM_SM_KEYS_IND (LE)
CL_SM_BLE_LINK_SECURITY_IND
(LE SC Pairing)
DM_SM_SIMPLE_PAIRING_COMPLETE_IND
CL_SM_BLE_SIMPLE_PAIRING_COMPLETE_IND
DM_SM_KEYS_IND (BR/EDR)
CL_SM_AUTHENTICATE_CFM
[key_type]
DM_SM_ENCRYPTION_CHANGE_IND (BR/EDR)
CL_SM_ENCRYPTION_CHANGE_IND(BR/EDR)
[encrypt_type]
if encrypt_type is 2?
Yes -> BR/EDR SC pairing
No -> BR/EDR non-SC pairing
encrpt_type
2- AES-CCM on BR/EDR link
1- E0 on BR/EDR link

Figure 3-4 Cross transport pairing: Bluetooth low energy technology SC first

3.3.2 When Secure Connections pairing occurs first on BR/EDR transport

Figure 3-5 shows the cross transport pairing message sequence when BR/EDR transport is used to generate the link key.

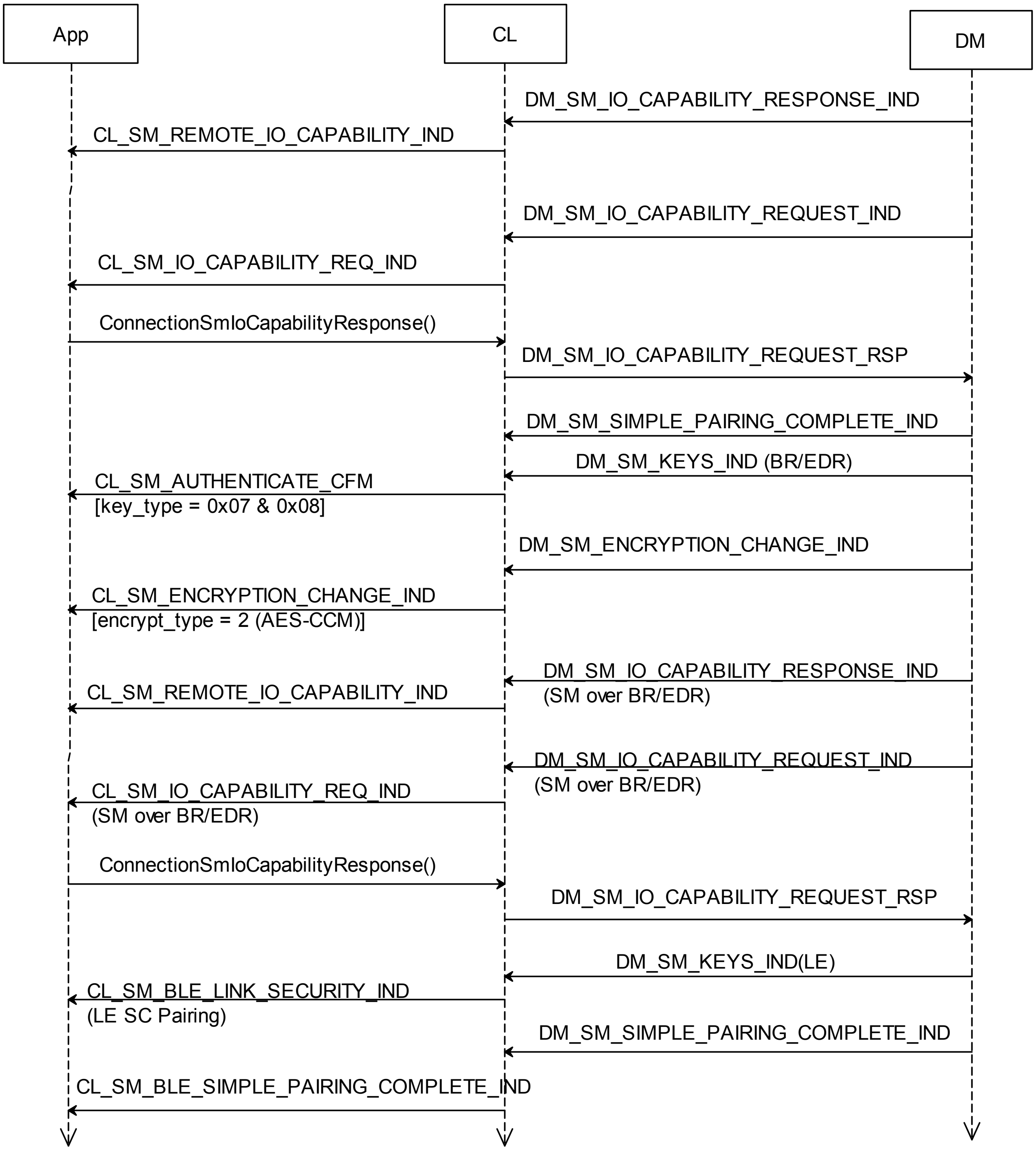

App
CL
DM
DM_SM_IO_CAPABILITY_RESPONSE_IND
CL_SM_REMOTE_IO_CAPABILITY_IND
DM_SM_IO_CAPABILITY_REQUEST_IND
CL_SM_IO_CAPABILITY_REQ_IND
ConnectionSmIoCapabilityResponse()
DM_SM_IO_CAPABILITY_REQUEST_RSP
DM_SM_SIMPLE_PAIRING_COMPLETE_IND
DM_SM_KEYS_IND (BR/EDR)
CL_SM_AUTHENTICATE_CFM
[key_type = 0x07 & 0x08]
DM_SM_ENCRYPTION_CHANGE_IND
CL_SM_ENCRYPTION_CHANGE_IND
[encrypt_type = 2 (AES-CCM)]
DM_SM_IO_CAPABILITY_RESPONSE_IND
(SM over BR/EDR)
CL_SM_REMOTE_IO_CAPABILITY_IND
DM_SM_IO_CAPABILITY_REQUEST_IND
(SM over BR/EDR)
CL_SM_IO_CAPABILITY_REQ_IND
(SM over BR/EDR)
ConnectionSmIoCapabilityResponse()
DM_SM_IO_CAPABILITY_REQUEST_RSP
DM_SM_KEYS_IND(LE)
CL_SM_BLE_LINK_SECURITY_IND
(LE SC Pairing)
DM_SM_SIMPLE_PAIRING_COMPLETE_IND
CL_SM_BLE_SIMPLE_PAIRING_COMPLETE_IND

Figure 3-5 Cross transport pairing: BR/EDR SC first

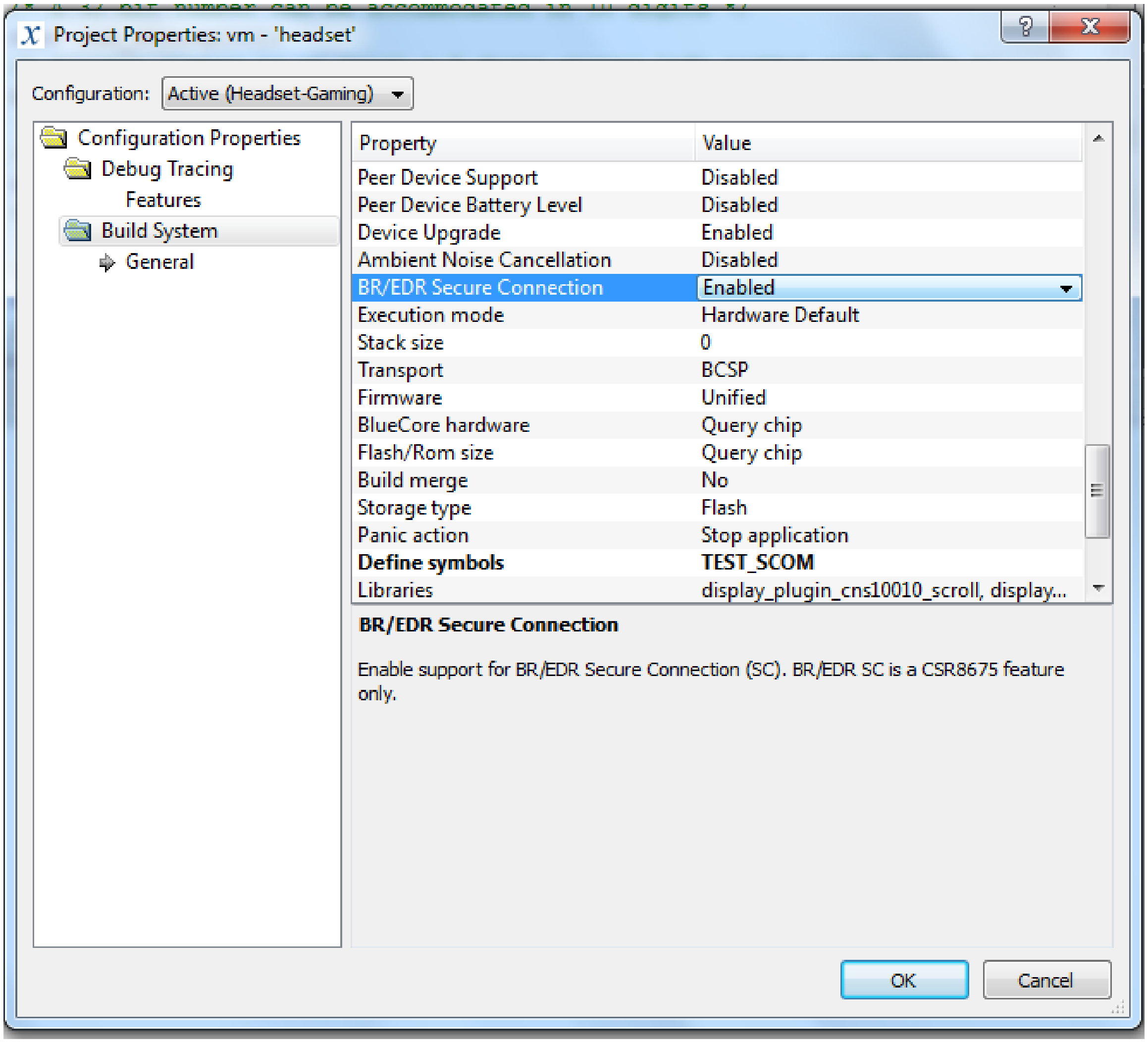
4 Enabling the SC feature in a sink application

To enable the BR/EDR SC feature in the sink application

1. Enable the BR/EDR SC in the **Project Properties**:
   a. Set the **BR/EDR Secure Connection** field in the **Project Properties > Built System** to **Enabled**, see Figure 4-1.
   b. Build the image and Flash it to the device.

NOTE (1) This feature is only applicable for CSR8675.

(2) The Bluetooth low energy technology SC feature is enabled by default for CSR8670 and CSR8765.



Configuration: Active (Headset-Gaming)

Property	Value
Peer Device Support	Disabled
Peer Device Battery Level	Disabled
Device Upgrade	Enabled
Ambient Noise Cancellation	Disabled
BR/EDR Secure Connection	Enabled
Execution mode	Hardware Default
Stack size	0
Transport	BCSP
Firmware	Unified
BlueCore hardware	Query chip
Flash/Rom size	Query chip
Build merge	No
Storage type	Flash
Panic action	Stop application
Define symbols	**TEST_SCOM**
Libraries	display_plugin_cns10010_scroll, display...

BR/EDR Secure Connection

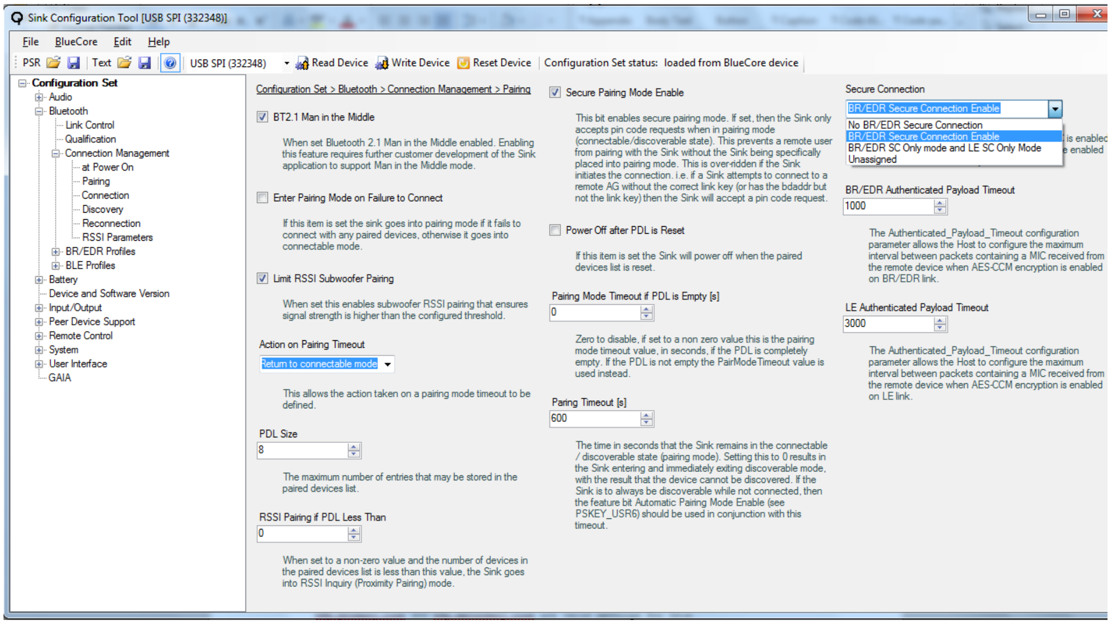
Enable support for BR/EDR Secure Connection (SC). BR/EDR SC is a CSR8675 feature only.

Figure 4-1 Enabling BR/EDR/Bluetooth low energy technology SC in a sink application

2. Configure the BR/EDR Secure Connection feature in the Sink Configuration Tool:

   a. Navigate to:
      Configuration Set>Bluetooth>Connection Manager>Pairing

   b. Select **BR/EDR Secure Connection Enable** from the **Secure Connection** dropdown, see Figure 4-2.



Configuration Set status: loaded from BlueCore device

Configuration Set > Bluetooth > Connection Management > Pairing

☑ BT2.1 Man in the Middle

When set Bluetooth 2.1 Man in the Middle enabled. Enabling this feature requires further customer development of the Sink application to support Man in the Middle mode.

☐ Enter Pairing Mode on Failure to Connect

If this item is set the sink goes into pairing mode if it fails to connect with any paired devices, otherwise it goes into connectable mode.

☑ Limit RSSI Subwoofer Pairing

When set this enables subwoofer RSSI pairing that ensures signal strength is higher than the configured threshold.

Action on Pairing Timeout: Return to connectable mode

This allows the action taken on a pairing mode timeout to be defined.

PDL Size: 8

The maximum number of entries that may be stored in the paired devices list.

RSSI Pairing if PDL Less Than: 0

When set to a non-zero value and the number of devices in the paired devices list is less than this value, the Sink goes into RSSI Inquiry (Proximity Pairing) mode.

☑ Secure Pairing Mode Enable

This bit enables secure pairing mode. If set, then the Sink only accepts pin code requests when in pairing mode (connectable/discoverable state). This prevents a remote user from pairing with the Sink without the Sink being specifically placed into pairing mode. This is over-ridden if the Sink initiates the connection. i.e. if a Sink attempts to connect to a remote AG without the correct link key (or has the bdaddr but not the link key) then the Sink will accept a pin code request.

☐ Power Off after PDL is Reset

If this item is set the Sink will power off when the paired devices list is reset.

Pairing Mode Timeout if PDL is Empty [s]: 0

Zero to disable, if set to a non zero value this is the pairing mode timeout value, in seconds, if the PDL is completely empty. If the PDL is not empty the PairModeTimeout value is used instead.

Paring Timeout [s]: 600

The time in seconds that the Sink remains in the connectable / discoverable state (pairing mode). Setting this to 0 results in the Sink entering and immediately exiting discoverable mode, with the result that the device cannot be discovered. If the Sink is to always be discoverable while not connected, then the feature bit Automatic Pairing Mode Enable (see PSKEY_USR6) should be used in conjunction with this timeout.

Secure Connection: BR/EDR Secure Connection Enable

BR/EDR Authenticated Payload Timeout: 1000

The Authenticated_Payload_Timeout configuration parameter allows the Host to configure the maximum interval between packets containing a MIC received from the remote device when AES-CCM encryption is enabled on BR/EDR link.

LE Authenticated Payload Timeout: 3000

The Authenticated_Payload_Timeout configuration parameter allows the Host to configure the maximum interval between packets containing a MIC received from the remote device when AES-CCM encryption is enabled on LE link.

Figure 4-2 Sink Configuration Tool

4.1 SC support in CSR8670

- Bluetooth low energy technology Secure Connections Only Mode is supported in CSR8670 and is enabled by default.
- CSR8670 does not support BR/EDR Secure Connection and so Bluetooth low energy technology Secure Connections Only Mode is not supported in CSR8670. Bluetooth low energy technology Secure Connections Only Mode is tied with BR/EDR Secure Connections Only Mode.
- If Secure Connections Only Mode is enabled on the CSR8670, it is not possible to create any BR/EDR links. QTIL recommends that Secure Connection Only Mode is not enabled with CSR8670.

4.2 SC support in CSR8675

- CSR8675 supports BR/EDR Secure Connection.
- Bluetooth low energy technology Secure Connections Only Mode is supported in CSR8675 and is enabled by default.
- BR/EDR Secure Connections Only Mode and Bluetooth low energy technology Secure Connections Only Mode is supported in CSR8675.

BR/EDR Secure Connections Only Mode and Bluetooth low energy technology Secure Connections Only Mode can be enabled together using the Sink Configuration Tool provided the BR/EDR Secure Connection feature is enabled at compile time and **BR/EDR Secure only Mode** and **Bluetooth low energy technology Secure only mode** is selected in the Sink Configuration Tool.

4.2.1 TEST_SCOM flag

A test flag `TEST_SCOM` is available to demonstrate the use of Secure Connections Only Mode with MITM support.

NOTE The `TEST_SCOM` flag can be defined in **Project Properties**.

To enable MITM support:

1. Navigate to the **Configuration Set>Bluetooth>Connection Manager>Pairing** tab in the Sink Configuration Tool and select the **BT2.1 Man in the Middle** option.
2. Navigate to the **Configuration Set>User Interface>Audio Prompts** tab in the Sink Configuration Tool and select the **Read out PIN Code using Audio Prompts** option.

Based on the Numeric Key heard the user needs to respond to accept or reject MITM pairing. It is left for the application developer to decide how to implement the procedure in the product, by which the user responds. The developer can map the Yes/No reponse to a button press or implement a spoken Yes/No response.

4.3 PS Keys and Sink Configuration Tool changes

Refer to the *ADK Audio Sink Application Configuration User Guide* for PS Keys and Sink Configuration Tool updates for Secure Connection.

4.3.1 System events for SC user notifications

The following system events have been added that allow user notifications to be configured. They allow LED or tone notifications indicating that the feature is in use to be configured.

- **EventSysHfpSecureLink**: Used to configure a tone pattern for the system event associated when an HFP SLC is established with SC.
- **EventSysSCOSecureLinkOpen:** Used to configure an LED pattern that is displayed when an eSCO link is connected in Secure Connections Only Mode.
- **EventSysSCOSecureLinkClose**: Used to cancel the LED pattern initiated by the **EventSysSCOSecureLinkOpen** event when the SC eSCO link is disconnected.
- **EventSysLESecureLink**: Used to configure an LED pattern that displays when the Bluetooth low energy technology link is SC and encrypted.

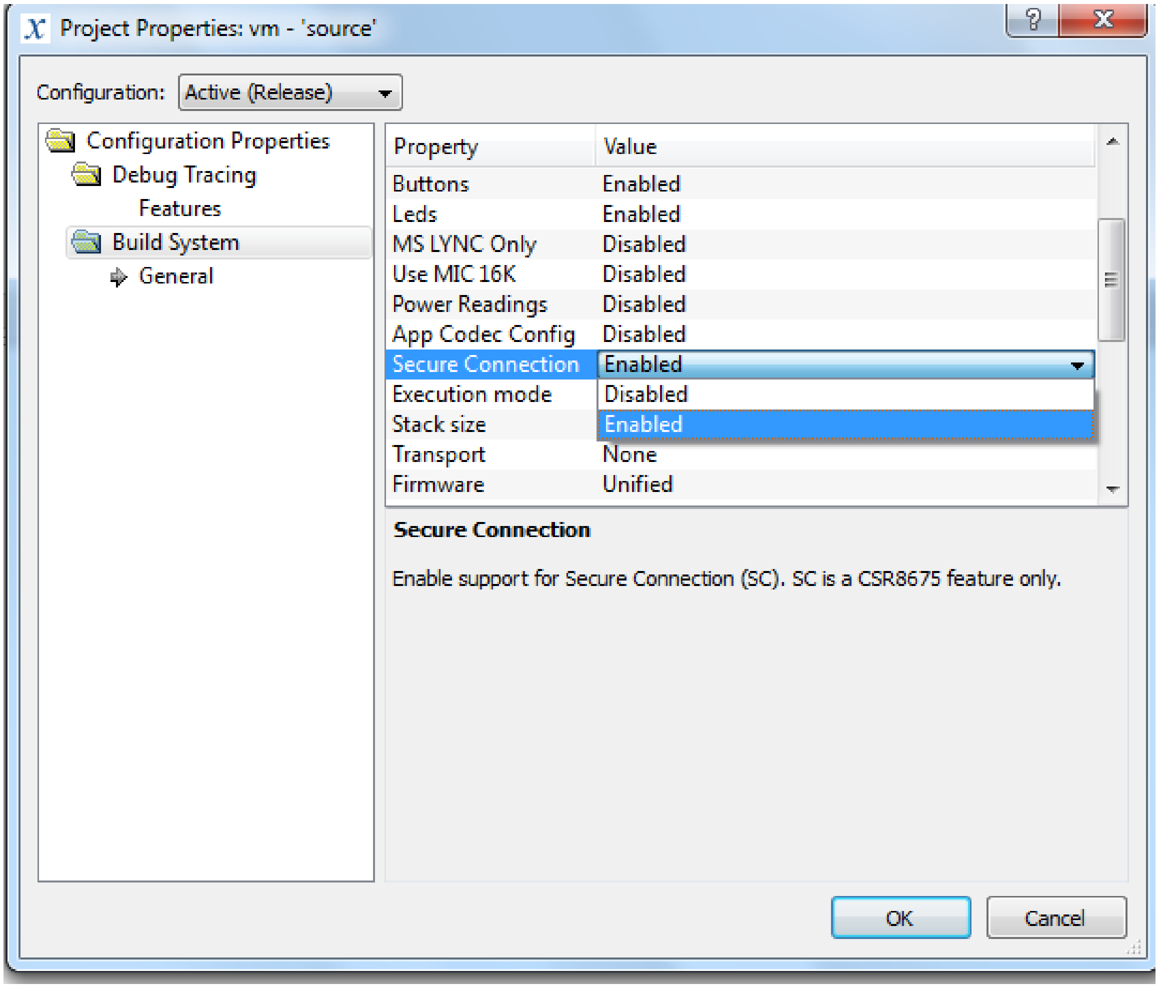
5 Enabling the SC feature in a source application

To enable the BR/EDR SC feature in a source application.

1. Enable the BR/EDR SC in the **Project Properties**:
   a. Set the **BR/EDR Secure Connection** field in the **Project Properties > Built System** to **Enabled**, see Figure 5-1.
   b. Build the image and Flash it to the device.

NOTE (1) This feature is only applicable for CSR8675.

[2] The Bluetooth low energy technology SC feature is enabled by default for CSR8670 and CSR8765.



Configuration: Active (Release)

Property	Value
Buttons	Enabled
Leds	Enabled
MS LYNC Only	Disabled
Use MIC 16K	Disabled
Power Readings	Disabled
App Codec Config	Disabled
Secure Connection	Enabled
Execution mode	
Stack size	
Transport	None
Firmware	Unified

Secure Connection

Enable support for Secure Connection (SC). SC is a CSR8675 feature only.

Figure 5-1 Enabling BR/EDR technology SC in a source application

NOTE A test flag `TEST_SCOM` has been added to indicate the use of Secure Connection Only Mode with MITM support. Since, there are no events or audio prompts supported in the source application, enabling this test flag, by default accepts the MITM pairing, mandated by Secure Connections Only Mode.

5.1 PS Keys and Source Configuration Tool changes

5.1.1 PS Keys

PSKEY_USR3: Feature configuration

PSKEY_USR3 holds the configuration for the Audio Sink application’s major feature set.

Word 4 has of PSKEY_USR3 been modified to allow enabling/disabling of the SC feature, see Table 5-1.

Table 5-1 Source feature configuration

Bits	Feature	Description

Word4 [1:0]	Secure Connection Mode	`0 = No BR/EDR Secure Connection`
		`1 = BR/EDR Secure Connection Enable`
		`2 = BR/EDR SC Only Mode and Bluetooth low energy technology SC Only Mode`
		NOTE For Secure Connection Only Mode MITM needs to be enabled.

PSKEY_USR8: Timers configuration

Table 5-2 describes the timer added to PSKEY_USER8 that can be used to configure the Authenticated Payload Timeout Value for a source application.

Table 5-2 Description of SC timer values added to PSKEY_USR8

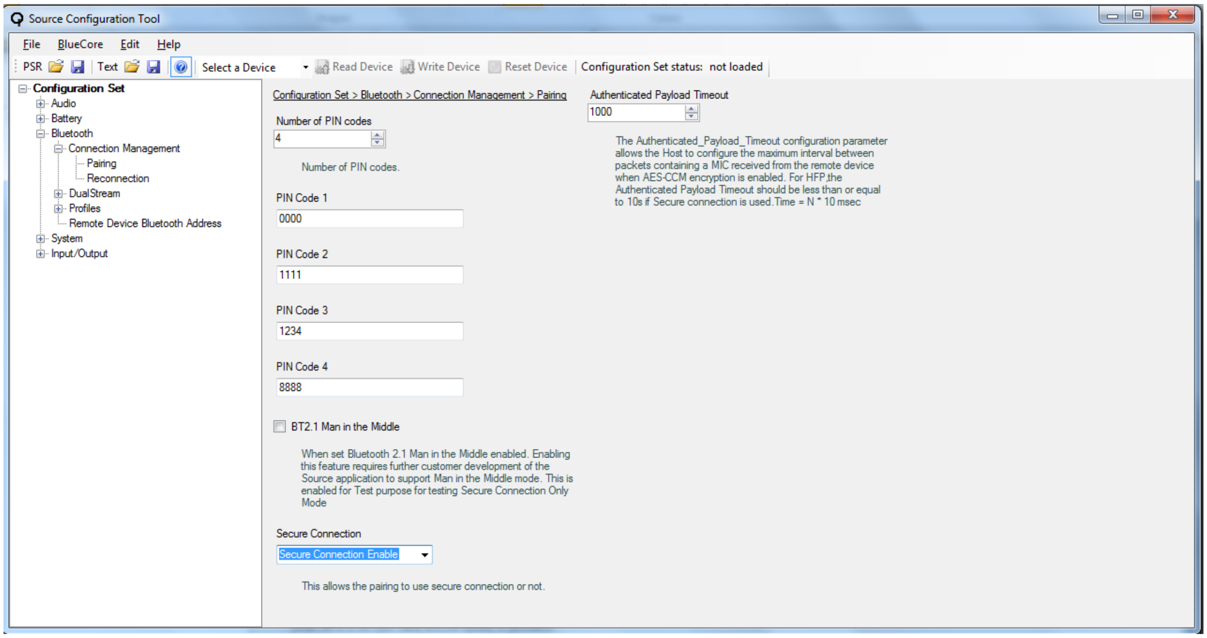
Bits	Feature	Description
Word16 `[15-0]`	`authenticated_payload_timeout_s (N)`	The Authenticated_Payload_Timeout configuration parameter allows the Host to configure the maximum interval between packets containing a MIC received from the remote device when AES-CCM encryption is enabled. Time = N * 10 msec

While writing the APT value to the controller the sink application also configures BlueCore to handle APT expiry. This results in link termination from BlueCore if the APT expires.

Default values of BR/EDR APT are set as 10 seconds and for Bluetooth low energy technology APT as 30 seconds. If SC is used with the HFP profile, the APT value should be ≤10 seconds.

5.1.2 Source Configuration Tool

The **Pairing** page of the Source Configuration Tool has been updated to allow the SC feature to be set, see Figure 5-2.



Configuration Set status: not loaded

Configuration Set > Bluetooth > Connection Management > Pairing

Number of PIN codes: 4

Number of PIN codes.

PIN Code 1: 0000

PIN Code 2: 1111

PIN Code 3: 1234

PIN Code 4: 8888

□ BT2.1 Man in the Middle

When set Bluetooth 2.1 Man in the Middle enabled. Enabling this feature requires further customer development of the Source application to support Man in the Middle mode. This is enabled for Test purpose for testing Secure Connection Only Mode

Secure Connection: Secure Connection Enable

This allows the pairing to use secure connection or not.

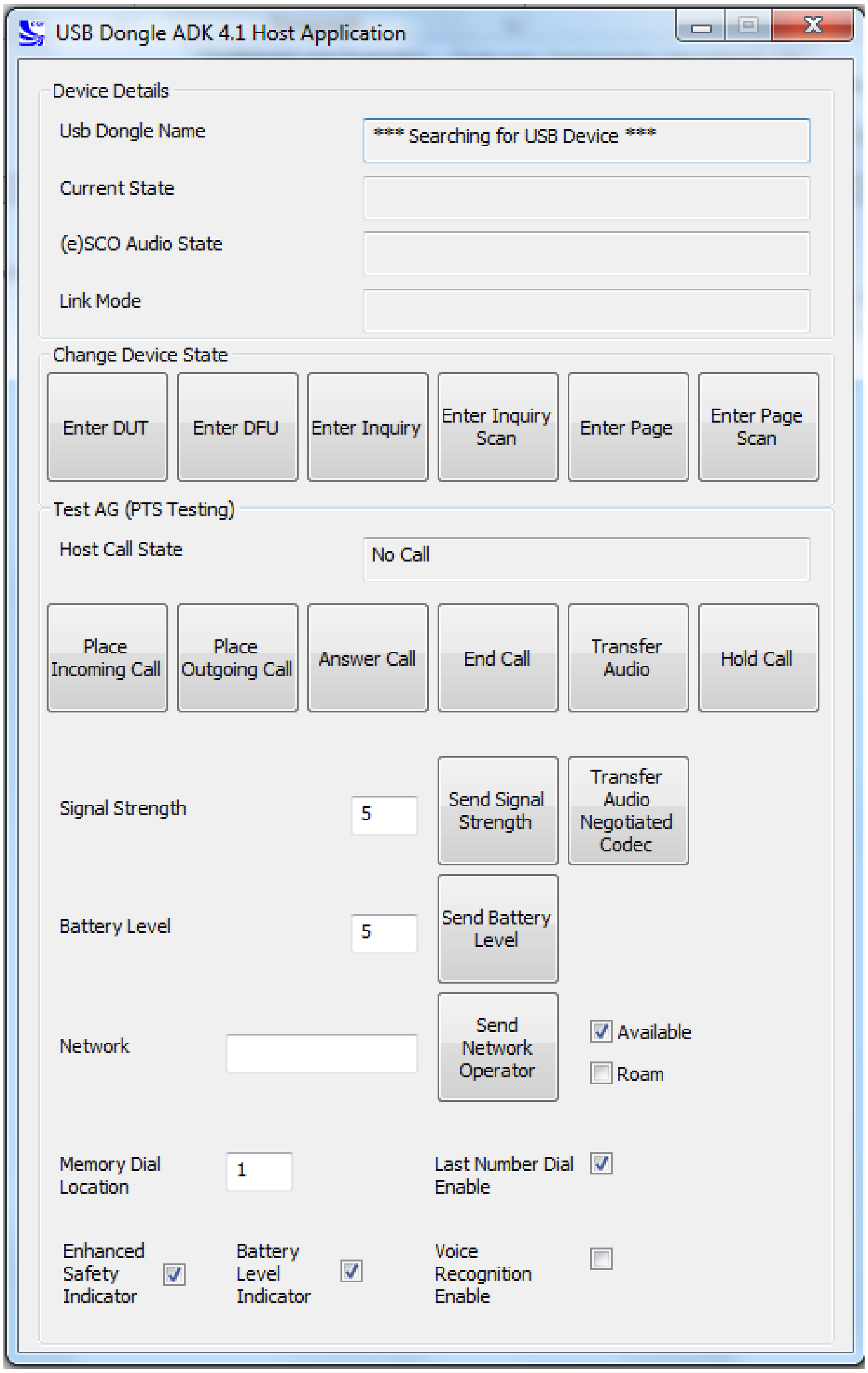
Authenticated Payload Timeout: 1000

The Authenticated_Payload_Timeout configuration parameter allows the Host to configure the maximum interval between packets containing a MIC received from the remote device when AES-CCM encryption is enabled. For HFP,the Authenticated Payload Timeout should be less than or equal to 10s if Secure connection is used.Time = N * 10 msec

Figure 5-2 Source Configuration Tool

5.2 Source dongle host executable

The source dongle host application has been modified to support BR/EDR SC. A new tab **Link Mode** has been added in the dongle host executable that now displays **Secure Link** or **No Secure Link** when an AGHFP SLC is established by the AG.



USB Dongle ADK 4.1 Host Application

Device Details

Usb Dongle Name: *** Searching for USB Device ***

Current State:

(e)SCO Audio State:

Link Mode:

Change Device State

Test AG (PTS Testing)

Host Call State: No Call

Signal Strength: 5

Battery Level: 5

Network:

☑ Available

□ Roam

Memory Dial Location: 1

Last Number Dial Enable ☑

Enhanced Safety Indicator ☑

Battery Level Indicator ☑

Voice Recognition Enable □

Figure 5-3 Dongle host application

Document references

Document	Reference
Bluetooth Core Specification v4.2	www.bluetooth.org
Hands-Free Profile 1.7 Bluetooth Profile Specification	www.bluetooth.org
ADK Audio Sink Application Configuration User Guide	80-CT451-1/CS-00334708-UG

Terms and definitions

Term	Defintion
ADK	Application Development Kit
AG	Audio Gateway
App	Application
APT	Authenticated Payload Timeout
BlueCore	Group term for the range of QTIL Bluetooth wireless technology ICs
BR/EDR	Bluetooth Radio/Extended Data Rate
CL	Client
DM	Device Manager
FIPS	Federal Information Processing Standards
HF	Hands Free
HFP	Hands Free profile
IC	Integrated Circuit
LTK	Long Term Key
MIC	Message Integrity Check
MITM	Man In the Middle
PS	Persistent Store
QTIL	Qualcomm Technologies International, Ltd.
SC	Secure Connection
SLC	Service Level Connection
SSP	Secure Simple Pairing