LE Security (LESEC)

***Bluetooth*® Implementation Conformance Statement (ICS) Proforma**

- **Revision:** LESEC.ICS.p0
- **Revision Date:** 2024-07-01
- **Prepared By:** BTI
- **Published during TCRL:** TCRL.2024-1

Contents

1 Identification of the implementation

1.1 Implementation Under Test (IUT) identification

Identification of the Implementation Under Test (IUT) is to be filled in to provide as much detail as possible regarding version numbers and configuration options.

An ICS contact person to respond to queries regarding information supplied in this ICS proforma is named in the Declaration of Compliance: Summary of Selected Specifications in Implementation.

1.2 Auto-fill tables

This ICS includes one or more tables that are defined as auto-fill tables. Auto-fill tables are defined to allow for less-complex conditions within other tables. Auto-fill tables are distinguished from regular ICS tables by the addition of “(auto-fill)” after the Table number, prior to the colon “:”.

An auto-fill table is automatically populated based on selected capabilities elsewhere in the ICS. The populated settings in the auto-fill table are not user editable.

1.3 Features

Table 1: LE Security

Item	Capability	Reference	Status
1	Counter with Cipher Block Chaining-Message Authentication Code (CCM) Mode	[1] 2	O
2	Group Session Key Derivation h8	[1] 1.1	O

1.4 LL requirements

Table 2: LL Requirements

Item	Capability	Reference	Status	Inter-Layer Dependency
1	LE Encryption	[1] 2	C.1	[2] LL 9/1
2	Receiving Encrypted Broadcast Isochronous Stream	[1] 1.1	C.2	[2] LL 9/1 AND LL 9/34
3	Transmitting Encrypted Broadcast Isochronous Stream	[1] 1.1	C.2	[2] LL 12/1

C.1: Mandatory IF LESEC 1/1 “Counter with Cipher Block Chaining-Message Authentication Code (CCM) Mode” OR LESEC 1/2 “Group Session Key Derivation h8”, otherwise not defined.

C.2: Mandatory to support at least one IF LESEC 1/2 “Group Session Key Derivation h8”, otherwise not defined.

2 References

[1] Specification of the Bluetooth System, Volume 6, Part E (Low Energy Link Layer Security)

[2] ICS Proforma for Link Layer (LL)

[3] Specification of the Bluetooth System, Volume 6, Part B (Link Layer)

3 LL Security tests

The capabilities in this ICS are tested in the LL test documents.

4 Bridge mapping between LESEC and LL

The LE security mechanisms used by the Link Layer (LL) [3] but defined in the Low Energy Link Layer Security Specification (LESEC) [1] are listed in this ICS.

LESEC has existed as a complementary part to LL since the earliest adoptions of the Bluetooth Specification. Due to the close association with LL, it was not until the addition of Vol 0, Part D “Core Configurations” in 2023 that the need to create a separate LESEC.ICS was identified. This means that QDIDs supporting LL that were established before this event had their LE security mechanisms tested when qualifying to LL but were unable to explicitly declare support for the various LESEC capabilities.

Table 4.1 provides a mapping from LESEC capabilities to LL capabilities. If an implementation that pre-dates the introduction of the LESEC.ICS supports an LL capability listed in the table, then it also supports the associated LESEC capability, and vice versa.

LESEC ICS	**Description**	**Corresponding LL ICS [2] selections**
LESEC 1/1	Counter with Cipher Block Chaining-Message Authentication Code (CCM) Mode	LL 9/1 “LE Encryption”
LESEC 1/2	Group Session Key Derivation h8	LL 9/1 “LE Encryption” AND (LL 1/6 “Isochronous Broadcasting” State OR LL 9/34 “Synchronized Receiver”)
LESEC 2/1	LE Encryption	LL 9/1 “LE Encryption”
LESEC 2/2	Receiving Encrypted Broadcast Isochronous Stream	LL 9/1 “LE Encryption” AND LL 9/34 “Synchronized Receiver”
LESEC 2/3	Transmitting Encrypted Broadcast Isochronous Stream	LL 12/1 “Encrypting a Broadcast Isochronous Stream”

Table 4.1: Bridge mapping between LESEC and supported LL capabilities for QDIDs

5 Revision history and acknowledgments

Revision History

Publication Number	Revision Number	Date	Comments
	p0r00–406	2023-05-01 – 2024-01-03	TSE 24099 (rating 2): New ICS document covering the Low Energy Link Layer Security Specification, created to support new Core Configurations material. Updated document to align with latest standards.
0	p0	2024-07-01	Approved by BTI on 2024-05-22. Prepared for TCRL 2024-1 publication.

Acknowledgments

Name	Company
Dejan Berec	Bluetooth SIG, Inc.
Gene Chang	Bluetooth SIG, Inc.
Magnus Sommansson	Qualcomm Technologies, Inc
Clive D.W. Feather	Samsung Cambridge Solution Centre