LE LL Security (LESEC)

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

- **Revision:** LESEC.ICS.p2
- **Revision Date:** 2026-11-03
- **Prepared By:** BTI
- **Published during TCRL:** TCRL.pkg105

This document, regardless of its title or content, is not a Bluetooth Specification as defined in the Bluetooth Patent/Copyright License Agreement ("PCLA") and Bluetooth Trademark License Agreement. Use of this document by members of Bluetooth SIG is governed by the membership and other related agreements between Bluetooth SIG Inc. ("Bluetooth SIG") and its members, including the PCLA and other agreements posted on Bluetooth SIG's website located at www.bluetooth.com.

THIS DOCUMENT IS PROVIDED "AS IS" AND BLUETOOTH SIG, ITS MEMBERS, AND THEIR AFFILIATES MAKE NO REPRESENTATIONS OR WARRANTIES AND DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING ANY WARRANTY OF MERCHANTABILITY, TITLE, NON-INFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, THAT THE CONTENT OF THIS DOCUMENT IS FREE OF ERRORS.

TO THE EXTENT NOT PROHIBITED BY LAW, BLUETOOTH SIG, ITS MEMBERS, AND THEIR AFFILIATES DISCLAIM ALL LIABILITY ARISING OUT OF OR RELATING TO USE OF THIS DOCUMENT AND ANY INFORMATION CONTAINED IN THIS DOCUMENT, INCLUDING LOST REVENUE, PROFITS, DATA OR PROGRAMS, OR BUSINESS INTERRUPTION, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY, AND EVEN IF BLUETOOTH SIG, ITS MEMBERS, OR THEIR AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

This document is proprietary to Bluetooth SIG. This document may contain or cover subject matter that is intellectual property of Bluetooth SIG and its members. The furnishing of this document does not grant any license to any intellectual property of Bluetooth SIG or its members.

This document is subject to change without notice.

Copyright © 2024–2026 by Bluetooth SIG, Inc. The Bluetooth word mark and logos are owned by Bluetooth SIG, Inc. Other third-party brands and names are the property of their respective owners.

Contents

1 General principles 4
1.1 Implementation Under Test (IUT) identification 4
1.2 Enforcement of inter-layer dependencies 4
2 ICS declarations 5
2.1 Features 5
2.2 LL requirements 5
3 References 6
4 LL Security tests 7
5 Bridge mapping (informational) 8
6 Revision history and acknowledgments 9

1 General principles

1.1 Implementation Under Test (IUT) identification

Using the Bluetooth SIG qualification tool, the implementer is expected to declare details about what will be implemented.

1.2 Enforcement of inter-layer dependencies

This ICS includes one or more tables with inter-layer dependencies (ILDs). ILDs are used for specification requirements that are dependent on other supporting specifications. ILDs can refer to an individual ICS item in a separate layer (individual ILD), or it can refer to the full layer (full-layer ILD).

ILDs residing in an X2Core layer will be enforced from the Bluetooth SIG qualification tool in the following conditions, depending on where the referred ILD is residing:

Referred ILD resides in	Individual ILD	Full-layer ILD
Controller layer	Core-Complete configuration, or Referred layer is supported	N/A
Lower HCI layer	HCI is supported	N/A
Upper HCI layer	Core-Host configuration, or UHCI is supported	N/A
Host layer	Core-Host configuration, or Core-Complete configuration, or Referred layer is supported	N/A
X2Core layer	Core-Host configuration, or Core-Complete configuration, or Referred layer is supported	Core-Host configuration, or Core-Complete configuration

Table 1.1: Enforcement of an ILD within the Bluetooth SIG qualification tool

2 ICS declarations

2.1 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

2.2 LL requirements

Table 2: LL Requirements

Item	Capability	Reference	Status	Inter-Layer Dependency
1	LE Encryption with Diversifiers	[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.

3 References

[1] Bluetooth Core Specification, Volume 6, Part E, Low Energy Link Layer Security (LESEC)

[2] ICS Proforma for Link Layer (LL)

4 LL Security tests

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

5 Bridge mapping (informational)

Bridge mapping provides a logical mapping for ICS items defined in the latest TCRL release to one or more ICS items present in an older TCRL release. The bridge mapping logic can change depending on the old TCRL release. An implementation qualified under an older TCRL release will use the bridge mapping logic to indicate support for an ICS item that is missing from the old TCRL release when upgrading to a new TCRL release. Using bridge mapping when upgrading a design to a new TCRL release should prevent unnecessary consistency check errors.

Table 5.1 provides a bridge mapping example for GAP 7/3a (from the GAP ICS as defined in TCRL pkg103). Depending on the TCRL of the old design, the following apply:

- GAP 7/3a was introduced in TCRL pkg103. Therefore, bridge mapping is not applicable for designs qualified on TCRL pkg103 or newer TCRL releases.
- For old designs qualified before TCRL pkg103, but not before TCRL 2019-2, support for GAP 7/3a in the upgraded design is determined by the support of LL 9/33 in the old design and by whether GAP itself was selected in the original design. The addition of GAP into the bridge mapping logic prevents the GAP layer from being added to the old design in the event that it did not exist before (e.g., in the case of a Core-Controller design), unless it is intended (e.g., automatically adding SEC or LESEC to an older design from before Core v6.0).
- For old designs qualified before TCRL 2019-2, GAP 7/3a is not supported in the upgraded design.

ICS Item	Description	Bridge Mapping Logic	TCRL Information
GAP 7/3a	Isochronous Broadcaster	Not applicable	≥ TCRL pkg103
		GAP AND LL 9/33	< TCRL pkg103
		Not supported	< TCRL 2019-2 (Core v5.2)

Table 5.1: Bridge mapping (Example)

Bridge mapping for this layer is provided in Table 5.2:

ICS Item	Description	Bridge Mapping Logic	TCRL Information
LESEC 1/1	Counter with Cipher Block Chaining-Message Authentication Code (CCM) Mode	Not applicable	≥ TCRL 2024-1
		LL 9/1	< TCRL 2024-1 (Core v6.0)
LESEC 1/2	Group Session Key Derivation h8	Not applicable	≥ TCRL 2024-1
		LL 9/1 AND (LL 1/6 OR LL 9/34)	< TCRL 2024-1 (Core v6.0)
LESEC 2/1	LE Encryption with Diversifiers	Not applicable	≥ TCRL 2024-1
		LL 9/1	< TCRL 2024-1 (Core v6.0)
LESEC 2/2	Receiving Encrypted Broadcast Isochronous Stream	Not applicable	≥ TCRL 2024-1
		LL 9/1 AND LL 9/34	< TCRL 2024-1 (Core v6.0)
LESEC 2/3	Transmitting Encrypted Broadcast Isochronous Stream	Not applicable	≥ TCRL 2024-1
		LL 12/1	< TCRL 2024-1 (Core v6.0)

Table 5.2: Bridge mapping (informational)

6 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.
	p1r00	2024-10-30	TSE 26596 (rating 1): Updated the title of the ICS document (mirrored on the TCRL top sheet) to better align with the spec naming.
1	p1	2025-02-18	Approved by BTI on 2024-12-26. Prepared for TCRL 2025-1 publication.
	p2r00–r03	2026-07-29 – 2026-08-21	TSE 29199 (rating 1): Updated Bridge mapping section to allow for easier automatic import. Editorial updates to template and references to align with BTI's desired test doc conventions.
2	p2	2026-11-03	Approved by BTI on 2026-10-12. Prepared for TCRL pkg105 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