BR/EDR Security (SEC)

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

- **Revision:** SEC.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: Security Mechanisms

Item	Capability	Reference	Status
1	Legacy Security	[1] 1	M
2	Secure Simple Pairing	[1] 1	M
3	Secure Connections	[1] 1	O

Table 2 (auto-fill): Security Algorithms

Item	Capability	Reference	Status
1	E0 encryption	[1] 1	C.1
2	AES-CCM encryption	[1] 1	C.2
3	Legacy authentication	[1] 1	C.1
3a	Secure Simple Pairing Authentication	[1] 1	C.5
4	Secure authentication	[1] 1	C.2
5	E3 key generation	[1] 1	C.3
6	AES key generation h3	[1] 1	C.5
7	P-192 elliptic curve	[1] 1	C.4
8	P-256 elliptic curve	[1] 1	C.2

C.1: Mandatory IF SEC 1/1 “Legacy Security” OR SEC 1/2 “Secure Simple Pairing”, otherwise Excluded.

C.2: Mandatory IF SEC 1/3 “Secure Connections”, otherwise Excluded.

C.3: Mandatory IF SEC 1/1 “Legacy Security”, otherwise Excluded.

C.4: Mandatory IF SEC 1/2 “Secure Simple Pairing”, otherwise Excluded.

C.5: Mandatory IF SEC 1/2 “Secure Simple Pairing” OR SEC 1/3 “Secure Connections”, otherwise Excluded.

Table 3: Broadcast Encryption Options

Item	Capability	Reference	Status
1	No encryption	[1] 4.2	M
2	Point-to-point only encryption	[1] 4.2	M
3	Point-to-point and broadcast encryption	[1] 4.2	C.1

C.1: Excluded IF NOT SEC 4/4 “Broadcast encryption”, otherwise Mandatory IF SEC 1/1 “Legacy Security” OR SEC 1/2 “Secure Simple Pairing”, otherwise Optional.

1.4 LMP requirements

Table 4 (auto-fill): LMP Requirements

Item	Capability	Reference	Status	Inter-Layer Dependency
1	Encryption	[1] 1	M	[2] LMP 2/3
2	Secure Simple Pairing (Controller Support)	[1] 1	C.1	[2] LMP 2/19b
3	Secure Connections (Controller Support)	[1] 1	C.2	[2] LMP 2/26
4	Broadcast encryption	[1] 4.2	C.3	[2] LMP 2/14
5	AES CCM Encryption	[1] 1	C.4	[2] LMP 6/11

C.1: Mandatory IF SEC 1/2 “Secure Simple Pairing”, otherwise not defined.

C.2: Mandatory IF SEC 1/3 “Secure Connections”, otherwise not defined.

C.3: Mandatory IF SEC 3/3 “Point-to-point and broadcast encryption”, otherwise not defined.

C.4: Mandatory IF SEC 2/2 “AES-CCM encryption”, otherwise not defined.

2 References

[1] Specification of the Bluetooth System, Volume 2, Part H (Security Specification)

[2] ICS Proforma for Link Management Protocol (LMP)

[3] Specification of the Bluetooth System, Volume 2, Part C (Link Manager Protocol Specification)

3 BR/EDR Security tests

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

4 Bridge mapping between SEC and LMP

The BR/EDR security mechanisms used by the Link Manager Protocol (LMP) [3] but defined in the Security Specification (SEC) [1] are listed in this ICS.

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

Table 4.1 provides a mapping from SEC capabilities to LMP capabilities. If an implementation that pre-dates the introduction of the SEC.ICS supports an LMP capability listed in the table, then it also supports the associated SEC capability, and vice versa. “Always supported” indicates that all implementations of LMP are required to support the corresponding SEC capability.

SEC ICS	Description	Corresponding LMP ICS [2] selections
SEC 1/1	Legacy Security	**Always supported**
SEC 1/2	Secure Simple Pairing	**Always supported**
SEC 1/3	Secure Connections	LMP 2/26 “Secure Connections (Controller Support)”
SEC 2/1	E0 encryption	**Always supported**
SEC 2/2	AES-CCM encryption	LMP 2/26 “Secure Connections (Controller Support)”
SEC 2/3	Legacy authentication	**Always supported**
SEC 2/4	Secure authentication	LMP 2/26 “Secure Connections (Controller Support)”
SEC 2/5	E3 key generation	**Always supported**
SEC 2/6	AES key generation h3	**Always supported**
SEC 2/7	P-192 elliptic curve	**Always supported**
SEC 2/8	P-256 elliptic curve	LMP 2/26 “Secure Connections (Controller Support)”
SEC 2/3a	Secure Simple Pairing Authentication	**Always supported**
SEC 3/1	No encryption	**Always supported**
SEC 3/2	Point-to-point only encryption	**Always supported**
SEC 3/3	Point-to-point and broadcast encryption	LMP 2/14 “Broadcast encryption”
SEC 4/1	Encryption	**Always supported**
SEC 4/2	Secure Simple Pairing (Controller Support)	**Always supported**
SEC 4/3	Secure Connections (Controller Support)	LMP 2/26 “Secure Connections (Controller Support)”
SEC 4/4	Broadcast encryption	LMP 2/14 “Broadcast encryption”
SEC 4/5	AES CCM Encryption	LMP 6/11 “AES CCM Encryption”

Table 4.1: Bridge mapping between SEC and supported LMP capabilities for QDIDs

5 Revision history and acknowledgments

Revision History

Publication Number	Revision Number	Date	Comments
	p0r00–r02	2023-05-02 – 2023-12-19	TSE 24100 (rating 2): New ICS document covering the Security Specification, created to support new Core Configurations material.
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.
Robert Cole	Bluetooth SIG, Inc.
Magnus Sommansson	Qualcomm Technologies, Inc