

Security Manager (SM)

Bluetooth® Implementation Conformance Statement (ICS) Proforma

- **Revision:** SM.ICS.p13
- **Revision Date:** 2025-11-04
- **Prepared By:** BTI
- **Published during TCRL:** TCRL.pkg101



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 © 2009–2025 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
- 2 ICS declarations..... 5**
 - 2.1 Roles 5
 - 2.2 Pairing properties..... 5
 - 2.3 Key distribution and usage 6
 - 2.3.1 Signing algorithm 6
 - 2.3.2 Key distribution 6
 - 2.3.3 Cross-transport key derivation 7
- 3 References 8**
- 4 Bridge mapping (informational)..... 9**
- 5 Revision history and acknowledgments 10**



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.

2 ICS declarations

2.1 Roles

Table 1: Role Requirements

Item	Role	Reference	Status
1	Central Role (Initiator)	[1] 2.4	C.1
2	Peripheral Role (Responder)	[1] 2.4	C.1

C.1: Mandatory to support at least one.

2.2 Pairing properties

Table 2: No longer used

Table 2a: Pairing Algorithms

Item	Capability	Reference	Status
1	Legacy pairing	[1] 2.3	C.1
2	LE Secure Connection pairing	[1] 2.3	C.1

C.1: Mandatory to support at least one.

Tables 3–4: No longer used

Table 4a: Legacy Pairing Methods

Prerequisite: SM 2a/1 “Legacy pairing”

Item	Capability	Reference	Status
1	Just Works	[1] 2.3.5	C.1
2	Passkey Entry	[1] 2.3.5	C.1
3	Out of Band	[1] 2.3.5	C.1

C.1: Mandatory to support at least one.

Table 4b: LE Secure Connections Pairing Methods

Prerequisite: SM 2a/2 “LE Secure Connection pairing”

Item	Capability	Reference	Status
1	Just Works	[1] 2.3.5.6.2	C.1
2	Passkey Entry	[1] 2.3.5.6.3	C.1
3	Out of Band	[1] 2.3.5.6.4	C.1
4	Numeric Comparison	[1] 2.3.5.6.2	C.1

C.1: Mandatory to support at least one.



2.3 Key distribution and usage

Table 5: Security Initiation

Item	Capability	Reference	Status
1	Encryption Setup using STK	[1] 2.4.4.1	C.3
2	Encryption Setup using LTK	[1] 2.4.2.3, 2.4.4.2, 2.4.6	M
3	Peripheral Initiated Security	[1] 2.4.6	C.1
4	Peripheral Initiated Security – Central response	[1] 2.4.6	C.2
5	CT2 bit	[2] 2.4.2.4, 3.5.2	C.4
6	No longer used	N/A	N/A

C.1: Optional IF SM 1/2 “Peripheral Role (Responder)”, otherwise Excluded.

C.2: Mandatory IF SM 1/1 “Central Role (Initiator)”, otherwise Excluded.

C.3: Mandatory IF SM 2a/1 “Legacy pairing”, otherwise Excluded.

C.4: Excluded IF NOT SM 8a/1 “Cross Transport Key Derivation Supported” AND NOT SM 8b/1 “Cross Transport Key Derivation Supported”, otherwise Mandatory IF CORE 2a/50 “Host Core v5.0 or later”, otherwise Optional.

2.3.1 Signing algorithm

Table 6: Signing Algorithm

Item	Capability	Reference	Status
1	Signing Algorithm - Generation	[1] 2.4.2.2, 2.4.5	O
2	Signing Algorithm - Resolving	[1] 2.4.2.2, 2.4.5	O

2.3.2 Key distribution

Table 7: No longer used

Table 7a: Key Distribution by Central

Prerequisite: SM 1/1 “Central Role (Initiator)”

Item	Capability	Reference	Status
1	Long Term Key (LTK)	[1] 2.4.1, 2.4.2.3, 2.4.3.1	C.1
2	Identity Resolving Key (IRK)	[1] 2.4.1, 2.4.3.1, 2.4.3.2	O
3	Connection Signature Resolving Key (CSRK)	[1] 2.4.1, 2.4.3.1, 2.4.3.2	O

C.1: Optional IF SM 2a/1 “Legacy pairing”, otherwise Excluded.



Table 7b: Key Distribution by Peripheral*Prerequisite: SM 1/2 "Peripheral Role (Responder)"*

Item	Capability	Reference	Status
1	Long Term Key (LTK)	[1] 2.4.1, 2.4.2.3, 2.4.3.1	C.1
2	Identity Resolving Key (IRK)	[1] 2.4.1, 2.4.3.1, 2.4.3.2	O
3	Connection Signature Resolving Key (CSRK)	[1] 2.4.1, 2.4.3.1, 2.4.3.2	O

C.1: Optional IF SM 2a/1 "Legacy pairing", otherwise Excluded.

2.3.3 Cross-transport key derivation

Table 8: No longer used**Table 8a: Cross-Transport Key Derivation by Central***Prerequisite: SM 1/1 "Central Role (Initiator)"*

Item	Capability	Reference	Status
1	Cross Transport Key Derivation Supported	[1] 2.3.5.7	C.1
2	Derivation of LE LTK from BR/EDR Link Key	[1] 2.4.2.5	C.2
3	Derivation of BR/EDR Link Key from LE LTK	[1] 2.4.2.4	C.2

C.1: Optional IF SM 2a/2 "LE Secure Connection pairing", otherwise Excluded.

C.2: Mandatory to support at least one IF SM 8a/1 "Cross Transport Key Derivation Supported", otherwise Excluded.

Table 8b: Cross-Transport Key Derivation by Peripheral*Prerequisite: SM 1/2 "Peripheral Role (Responder)"*

Item	Capability	Reference	Status
1	Cross Transport Key Derivation Supported	[1] 2.3.5.7	C.1
2	Derivation of LE LTK from BR/EDR Link Key	[1] 2.4.2.5	C.2
3	Derivation of BR/EDR Link Key from LE LTK	[1] 2.4.2.4	C.2

C.1: Optional IF SM 2a/2 "LE Secure Connection pairing", otherwise Excluded.

C.2: Mandatory to support at least one IF SM 8b/1 "Cross Transport Key Derivation Supported", otherwise Excluded.

3 References

- [1] Specification of the Bluetooth System, Volume 3, Part H (SM), Versions 4.2 or later
- [2] Specification of the Bluetooth System, Volume 3, Part H (SM), Versions 5.0 or later



4 Bridge mapping (informational)

Table 4.1 provides the mapping between new and old ICS items where the new item was not in older TCRL releases. An implementation qualified under an older TCRL release will use the bridge mapping to indicate support of the new ICS item. The mapping can change depending on the older TCRL release. For newer TCRL releases, the bridge mapping table is not applicable.

New ICS item	Description	Mapping from Old ICS Item
SM 2a/1	Legacy pairing	≥ TCRL p101: Not applicable ≤ TCRL p100: GAP 25/2 OR GAP 25/7 OR GAP 25/8 OR GAP 35/2 OR GAP 35/7 OR GAP 35/8
SM 2a/2	LE Secure Connection pairing	≥ TCRL p101: Not applicable ≤ TCRL p100: GAP 25/9 OR GAP 25/11 OR GAP 25/12 OR GAP 35/9 OR GAP 35/11 OR GAP 35/12
SM 4a/1	Just Works (Legacy Pairing)	≥ TCRL p101: Not applicable ≤ TCRL p100: SM 4/1 AND SM 2a/1
SM 4a/2	Passkey Entry (Legacy Pairing)	≥ TCRL p101: Not applicable ≤ TCRL p100: SM 4/2 AND SM 2a/1
SM 4a/3	Out of Band (Legacy Pairing)	≥ TCRL p101: Not applicable ≤ TCRL p100: SM 4/3 AND SM 2a/1
SM 4b/1	Just Works (LE Secure Connection pairing)	≥ TCRL p101: Not applicable ≤ TCRL p100: SM 4/1 AND SM 2a/2
SM 4b/2	Passkey Entry (LE Secure Connection pairing)	≥ TCRL p101: Not applicable ≤ TCRL p100: SM 4/2 AND SM 2a/2
SM 4b/3	Out of Band (LE Secure Connection pairing)	≥ TCRL p101: Not applicable ≤ TCRL p100: SM 4/3 AND SM 2a/2

Table 4.1: Bridge mapping (informational)

5 Revision history and acknowledgments

Revision History

Publication Number	Revision Number	Date	Comments
0	4.0.0	2010-06-30	Publication.
	4.0.1r0	2011-12-09	TSE 3856, Added Table 7; renamed Table 5
1	4.0.1	2012-03-30	Prepare for publication.
	4.1.0r01	2012-11-11	Updated revision to 4.1.0 Updated top sheet to include version 4.1
2	4.1.0	2013-12-03	Prepare for Publication
	4.1.1r00	2014-04-08	Template Conversion (Template_ICCS_2014r01) Updated conditional conventions to match latest BTI language. TSE 5434: Added C.2 to Table 1 and updated the status of 1/2 from C.1 to C.2.
	4.1.1r01	2014-06-16	BTI Review, Alicia, correction to Table 1, C.1 as agreed in BTI and reflected in updated TSE 5434.
3	4.1.1	2014-07-07	TCRL 2014-1 Publication
	4.2.0r00	2014-11-13	Integrated changes from Core_LE_Secure_Connections.TS.CR.R16
	4.2.0r01	2014-11-20	Integrated reviews by Jason, Alicia, Magnus. Added reference to 4.2 or later per Magnus' comments
4	4.2.0	2014-12-05	Prepared for TCRL 2014-2 publication
	4.2.1r00	2015-05-06	TSE 6322: Updated C.1 of Table 5 to Optional to reflect Core Spec accurately.
	4.2.1r01	2015-06-05	Deleted Section 1.2 (Global Statement of Conformance) per current ICS template standards.
5	4.2.1	2015-07-14	Prepared for TCRL 2015-1 publication
	5.0.0r00	2016-10-12	TSE 7576: Added "Link Key Conversion Function h7" capability (Item 5) and C.4 footnote to Table 5.
	5.0.0r01	2016-11-08	Updated to current template. Removed unnecessary parentheses and replaced with quotation marks.
	5.0.0r02	2016-11-11	Issue 7884: Global edit. Added support in conditionals for Core Spec version 5.0.
6	5.0.0	2016-12-13	Approved by BTI. Prepared for TCRL 2016-2 publication.
	5.1.0r00-r01	2018-11-13 – 2018-11-27	Updated revision number to 5.1.0 to align with the adoption of Core Specification version 5.1. Updated conditionals in Tables 1, 2, 5 for Core 5.1.
7	5.1.0	2018-12-07	Approved by BTI. Prepared for TCRL 2018-2 publication.
	5.1.1r00-r01	2019-04-01– 2019-06-12	TSE 11559 (rating 1): Fixed Table 1 C.1 to "IF" and C.2 to: "Optional IF GAP 5/3 "LE Roles – Peripheral Role" OR GAP 38/3 "BR/EDR/LE Roles – Peripheral Role" are supported, otherwise Excluded."

Publication Number	Revision Number	Date	Comments
8	5.1.1	2019-08-01	Approved by BTI. Prepared for TCRL 2019-1 publication.
	p9r00	2019-11-27	Revised document numbering convention, setting last release publication of 5.1.1 as p8; added publication number column to Revision History.
9	p9	2020-01-07	Approved by BTI on 2019-12-22. Prepared for TCRL 2019-2 publication.
	p10r00–r03	2020-08-17 – 2020-11-18	TSE 15188 (rating 2): Updated Table 2 by removing C.2 and updating Status of item 5 accordingly; updated Table 5 to add item 6, update reference for item 5, update text of C.4, and add new C.5; added new section for Cross-Transport Key Derivation, including new Table 8; added a reference to SM Part H, Versions 5.0 or later. TSE 15453 (rating 1): Editorials to address Erratum 15361, globally change “Master” to “Central” and “Slave” to “Peripheral”. Consistency Checker fixes and template-related editorials (added Appropriate Language link).
10	p10	2020-12-22	Approved by BTI on 2020-12-03. Prepared for TCRL 2020-1 publication.
	p10ed2r00–r01	2022-04-05 – 2022-04-21	TSE 18366 (rating 1): Removed “is/are/not supported” language to align with the latest ICS conventions. Performed template-related editorials, including aligning the copyright page with v2 of the DNMD. Per BTI review feedback, updated title to align with Core spec and removed Appropriate Language Mapping Tables reference.
	p10 edition 2	2022-04-25	Approved by BTI on 2022-04-25. Prepared for edition 2 publication.
	p11r00–r03	2022-07-28 – 2022-12-15	TSE 18425 (rating 2): Removed item 5/6 and related conditional C.5, updated reference for item 5/5 and made editorial changes to it and related conditional C.4. Removed intro text after Section headings 1.5 and 1.6. TSE 19221 (rating 3): Updated status of 1/2 and related C.1 (deleted now-unused C.2); replaced Table 7 with Tables 7a and 7b and replaced Table 8 with Tables 8a and 8b. Removed reference to GAP. Removed draft revision history entries (pre-initial publication) to align with current BTI conventions.
11	p11	2023-02-07	Approved by BTI on 2022-12-28. Prepared for TCRL 2022-2.

Publication Number	Revision Number	Date	Comments
	p12r00-r01	2023-08-07 – 2023-09-26	TSE 23380 (rating 2): Removed 2/4. Removed reference to Core v4.0 and updated cross refs globally to Core v4.2. Updated conditionals and section titles to align with the latest ICS template. TSE 24079 (rating 2): Replaced SUM ICS references with CORE ICS references. Updated Table 5 conditional C.4, affecting 5/5.
12	p12	2024-07-01	Approved by BTI on 2024-05-22. Prepared for TCRL 2024-1 publication.
	p13r00-r05	2025-08-01 – 2025-09-16	TSE 26036 (rating 3): Set Table 2 to “No longer used” and created new Pairing Algorithms Table 2a; set Tables 3 and 4 to “No longer used” and added new Tables 4a and 4b to cover pairing methods; updated the Status of 5/2 to Mandatory and corrected references for 5/1 and 5/2; corrected references for 6/1 and 6/2; updated capability names of 7a/1–7a/3, added C.1 to update 7a/1 Status, and corrected references for 7a/1–7a/3; updated capability names for 7b/1–7b/3, added C.1 to update 7b/1 Status, and corrected references for 7b/1–7b/3; corrected conditionals in Tables 5, 8a, and 8b to align; added a new section for Bridge Mapping.
13	p13	2025-11-04	Approved by BTI on 2025-10-05. Prepared for TCRL pkg101 publication.

Acknowledgments

Name	Company
Mike Tsai	Atheros
Magnus Sommansson	CSR