Security Manager (SM)

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

- **Revision:** SM.ICS.p12
- **Revision Date:** 2024-07-01
- **Prepared By:** BTI
- **Published during TCRL:** TCRL.2024-1

Contents

1 Identification of the implementation 4
1.1 Implementation Under Test (IUT) identification 4
1.2 Roles 5
1.3 Security properties 5
1.4 Pairing algorithms 5
1.4.1 Pairing method 5
1.5 Key distribution and usage 6
1.5.1 Signing algorithm 6
1.5.2 Key distribution 6
1.5.3 Cross-transport key derivation 7
2 References 8
3 Revision history and acknowledgments 9

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 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.

1.3 Security properties

Table 2: Security Properties

Item	Capability	Reference	Status
1	Authenticated MITM protection	[1] 2.3.1	O
2	Unauthenticated no MITM protection	[1] 2.3.1	C.1
3	No security requirements	[1] 2.3.1	M
4	No longer used	N/A	N/A
5	LE Secure Connections	[1] 2.3.1	O

C.1: Mandatory IF SM 2/1 “Authenticated MITM protection”, otherwise Optional.

1.4 Pairing algorithms

Table 3: Encryption Key Size

Prerequisite: SM 2/1 “Authenticated MITM protection” OR SM 2/2 “Unauthenticated no MITM protection” OR SM 4/3 “Out of Band”

Item	Capability	Reference	Status
1	Encryption Key Size	[1] 2.3.4	M

1.4.1 Pairing method

Table 4: Pairing Method

Item	Capability	Reference	Status
1	Just Works	[1] 2.3.5	O
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 IF SM 2/1 “Authenticated MITM protection”, otherwise Excluded.

1.5 Key distribution and usage

Table 5: Security Initiation

Item	Capability	Reference	Status
1	Encryption Setup using STK	[1] 2.4	C.3
2	Encryption Setup using LTK	[1] 2.4	O
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 2/1 “Authenticated MITM protection” OR SM 2/2 “Unauthenticated no MITM protection” OR SM 4/3 “Out of Band”, 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.

1.5.1 Signing algorithm

Table 6: Signing Algorithm

Item	Capability	Reference	Status
1	Signing Algorithm - Generation	[1] 2.4	O
2	Signing Algorithm - Resolving	[1] 2.4	O

1.5.2 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	Encryption Key	[1] 2.4.3	O
2	Identity Key	[1] 2.4.3	O
3	Signing Key	[1] 2.4.3	O

Table 7b: Key Distribution by Peripheral

Prerequisite: SM 1/2 "Peripheral Role (Responder)"

Item	Capability	Reference	Status
1	Encryption Key	[1] 2.4.3	O
2	Identity Key	[1] 2.4.3	O
3	Signing Key	[1] 2.4.3	O

1.5.3 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 2/5 "LE Secure Connections", 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 2/5 "LE Secure Connections", otherwise Excluded.

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

2 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

3 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_ICS_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.

Acknowledgments

Name	Company
Mike Tsai	Atheros
Magnus Sommansson	CSR