

Errata Correction 18898: Cross-Transport Key Derivation Requirements

Bluetooth® Errata Correction

- **Revision:** v1.0
- **Revision Date:** 2022-06-21
- **Prepared By:** Generic Audio Working Group

This Errata Correction applies to the following specification:

- Common Audio Profile (CAP), Version 1.0 ("Source Specification")

Abstract:

This erratum clarifies the requirements for the use of Cross-Transport Key Derivation (CTKD) to generate Long Term Keys (LTKs) for devices operating over both the Low Energy (LE) and Basic Rate/Enhanced Data Rate (BR/EDR) transports, harmonizing the requirements with updated Basic Audio Profile (BAP) requirements.



Revision History

Revision Number	Date (yyyy-mm-dd)	Comments
v1.0	2022-06-21	Adopted by the Bluetooth SIG Board of Directors.

Acknowledgments

Name	Company
Rasmus Abildgren	Bose Corporation
Chris Church	Qualcomm Technologies International, Ltd
Georg Dickmann	Sonova AG
Erik Peterson	Microsoft

Use of this specification is your acknowledgement that you agree to and will comply with the following notices and disclaimers. You are advised to seek appropriate legal, engineering, and other professional advice regarding the use, interpretation, and effect of this specification.

Use of Bluetooth specifications by members of Bluetooth SIG is governed by the membership and other related agreements between Bluetooth SIG and its members, including those agreements posted on Bluetooth SIG's website located at www.bluetooth.com. Any use of this specification by a member that is not in compliance with the applicable membership and other related agreements is prohibited and, among other things, may result in (i) termination of the applicable agreements and (ii) liability for infringement of the intellectual property rights of Bluetooth SIG and its members. This specification may provide options, because, for example, some products do not implement every portion of the specification. All content within the specification, including notes, appendices, figures, tables, message sequence charts, examples, sample data, and each option identified is intended to be within the bounds of the Scope as defined in the Bluetooth Patent/Copyright License Agreement ("PCLA"). Also, the identification of options for implementing a portion of the specification is intended to provide design flexibility without establishing, for purposes of the PCLA, that any of these options is a "technically reasonable non-infringing alternative."

Use of this specification by anyone who is not a member of Bluetooth SIG is prohibited and is an infringement of the intellectual property rights of Bluetooth SIG and its members. The furnishing of this specification does not grant any license to any intellectual property of Bluetooth SIG or its members. THIS SPECIFICATION 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 WARRANTIES OF MERCHANTABILITY, TITLE, NON-INFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, OR THAT THE CONTENT OF THIS SPECIFICATION IS FREE OF ERRORS. For the avoidance of doubt, Bluetooth SIG has not made any search or investigation as to third parties that may claim rights in or to any specifications or any intellectual property that may be required to implement any specifications and it disclaims any obligation or duty to do so.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, BLUETOOTH SIG, ITS MEMBERS AND THEIR AFFILIATES DISCLAIM ALL LIABILITY ARISING OUT OF OR RELATING TO USE OF THIS SPECIFICATION AND ANY INFORMATION CONTAINED IN THIS SPECIFICATION, 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 THE DAMAGES.

Products equipped with Bluetooth wireless technology ("Bluetooth Products") and their combination, operation, use, implementation, and distribution may be subject to regulatory controls under the laws and regulations of numerous countries that regulate products that use wireless non-licensed spectrum. Examples include airline regulations, telecommunications regulations, technology transfer controls, and health and safety regulations. You are solely responsible for complying with all applicable laws and regulations and for obtaining any and all required authorizations, permits, or licenses in connection with your use of this specification and development, manufacture, and distribution of Bluetooth Products. Nothing in this specification provides any information or assistance in connection with complying with applicable laws or regulations or obtaining required authorizations, permits, or licenses.

Bluetooth SIG is not required to adopt any specification or portion thereof. If this specification is not the final version adopted by Bluetooth SIG's Board of Directors, it may not be adopted. Any specification adopted by Bluetooth SIG's Board of Directors may be withdrawn, replaced, or modified at any time. Bluetooth SIG reserves the right to change or alter final specifications in accordance with its membership and operating agreements.

Copyright © 2022. All copyrights in the Bluetooth Specifications themselves are owned by Apple Inc., Ericsson AB, Intel Corporation, Lenovo (Singapore) Pte. Ltd., Microsoft Corporation, Nokia Corporation, and Toshiba Corporation. 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	Drafting conventions.....	5
1.1	Language	5
1.2	Formatting and color	5
2	Changes to CAP v1.0	6
2.1	Changes to CAP v1.0	6
2.1.1	[Modified Section] Section 9.2: Security requirements for BR/EDR	6
3	References	7



1 Drafting conventions

1.1 Language

Refer to and follow any terminology, language conventions, and interpretation sections of the Source Specification(s).

1.2 Formatting and color

The formatting and color conventions described in [Table 1.1](#) below are used in this Errata Correction to describe the specific changes and additions to the Source Specification(s) identified on the cover page.

Text Color	Description
black	Text that is unmodified from the Source Specification.
red	Text that is added to the Source Specification.
red-strikethrough	Text that is deleted from the Source Specification.
[green bracketed text]	Comments that are intended to aid the reader.
blue	Default color used for section numbers and headings of this document.

Table 1.1: Color key for headings, captions, and body text

2 Changes to CAP v1.0

This Section sets forth the specific changes and additions, using the formatting and color conventions described in Section 1.2, to CAP, Version 1.0 [1].

2.1 Changes to CAP v1.0

2.1.1 [Modified Section] Section 9.2: Security requirements for BR/EDR

[The modified text with changes is shown below.]

This section describes the security requirements for the BR/EDR transport.

The security requirements for all characteristics defined by underlying profiles shall be Security Mode 4 Level 2 (defined in Volume 3, Part C, Section 5.2.2.8 in [3]) or higher if a stronger requirement is inherited from underlying profiles.

Access to all characteristics defined by underlying profiles shall require an encryption key with at least 128 bits of entropy, derived from any of the following:

- BR/EDR Secure Connections
- LE Secure Connections, if CTKD is used
- OOB method

~~If a BR/EDR/LE device is generating a BR/EDR link key with another BR/EDR/LE device that has set the CoD Major Service Class bit 14 to a value of 0b1, then both devices shall support and use CTKD to derive an LE LTK to help avoid a poor user experience of requiring to pair a second time.~~

~~If the Privacy feature is used, then BR/EDR/LE devices shall distribute their Identity Addresses (IAs) and Identity Resolving Keys (IRKs).~~

~~If a BR/EDR/LE device uses CTKD to derive an LE Long Term Key (LTK) as part of the BR/EDR pairing procedure and the device supports the Privacy feature, then the device shall distribute its IA and IRK.~~

3 References

- [1] Common Audio Profile (CAP), Version 1.0