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

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