

Erratum 27195: Pausing of encryption (AES- CCM) uses incorrect PDU

Bluetooth® Expedited Specification Update

- **Version:** v1.0
- **Version Date:** 2025-06-30
- **Prepared By:** Core Specification Working Group

This Expedited Specification Update applies to the following specifications (collectively, the “Source Specifications”):

- Bluetooth Core Specification (amended), Version 5.2 (“Core Specification v5.2”)
- Bluetooth Core Specification (amended), Version 5.3 (“Core Specification v5.3”)
- Bluetooth Core Specification (amended), Version 5.4 (“Core Specification v5.4”)
- Bluetooth Core Specification, Version 6.0 (“Core Specification v6.0”)
- Bluetooth Core Specification, Version 6.1 (“Core Specification v6.1”)

Abstract:

This Expedited Specification Update amends the Link Manager Protocol sequence for Peripheral-initiated pausing of encryption (Advanced Encryption Standard - Counter with CBC-MAC (AES-CCM)) to the correct PDU at the start of sequence diagram 51. The related body text in the Source Specifications is correct, but the sequence diagrams, which implementers often use as definitive sources, are incorrect.

Version History

Version Number	Date (yyyy-mm-dd)	Comments
v1.0	2025-06-30	Adopted by the Bluetooth SIG Board of Directors.

Acknowledgments

Name	Company
Clive D.W. Feather	Samsung Cambridge Solution Centre

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 © 2025. All copyrights in the Bluetooth Specifications themselves are owned by Apple Inc., Ericsson AB, Intel Corporation, Google LLC, 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 Core Specification v5.2	6
2.1	Changes to Core Specification v5.2, Volume 2, Part C, Link Manager Protocol specification	6
2.1.1	[Modified Section] 4.2.5.5 Pause Encryption	6
3	Changes to Core Specification v5.3	7
3.1	Changes to Core Specification v5.3, Volume 2, Part C, Link Manager Protocol specification	7
3.1.1	[Modified Section] 4.2.5.5 Pause Encryption	7
4	Changes to Core Specification v5.4	8
4.1	Changes to Core Specification v5.4, Volume 2, Part C, Link Manager Protocol specification	8
4.1.1	[Modified Section] 4.2.5.5 Pause Encryption	8
5	Changes to Core Specification v6.0	9
5.1	Changes to Core Specification v6.0, Volume 2, Part C, Link Manager Protocol specification	9
5.1.1	[Modified Section] 4.2.5.5 Pause Encryption	9
6	Changes to Core Specification v6.1	10
6.1	Changes to Core Specification v6.1, Volume 2, Part C, Link Manager Protocol specification	10
6.1.1	[Modified Section] 4.2.5.5 Pause Encryption	10
7	References	11

1 Drafting conventions

1.1 Language

Refer to and follow any terminology, language conventions, and interpretation sections of the Source Specifications.

1.2 Formatting and color

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

Text Color	Description
black	Text that is unmodified from the Source Specifications.
red	Text that is added to the Source Specifications.
red strikethrough	Text that is deleted from the Source Specifications.
[green bracketed text]	Comments that explain the changes to be made to the Source Specifications.
[...]	Indicates the section of the Source Specifications that includes additional text that is not included in black text.
blue	Default color used for section numbers and headings of this document.

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

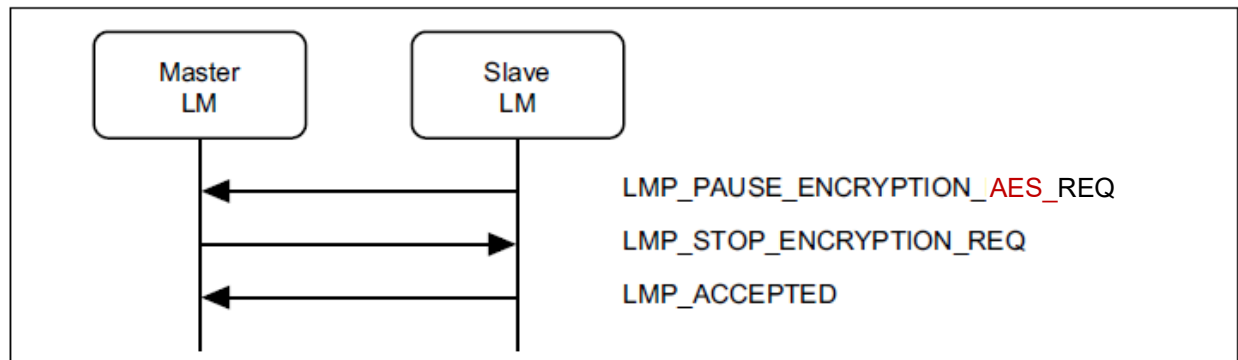
2 Changes to Core Specification v5.2

This section sets forth the specific changes and additions, using the formatting and color conventions described in Section 1.2, to Core Specification v5.2 [1].

2.1 Changes to Core Specification v5.2, Volume 2, Part C, Link Manager Protocol specification

2.1.1 [Modified Section] 4.2.5.5 Pause Encryption

[Modify Sequence 51 as shown.]



Sequence 51: Slave-initiated pausing of encryption (AES-CCM)

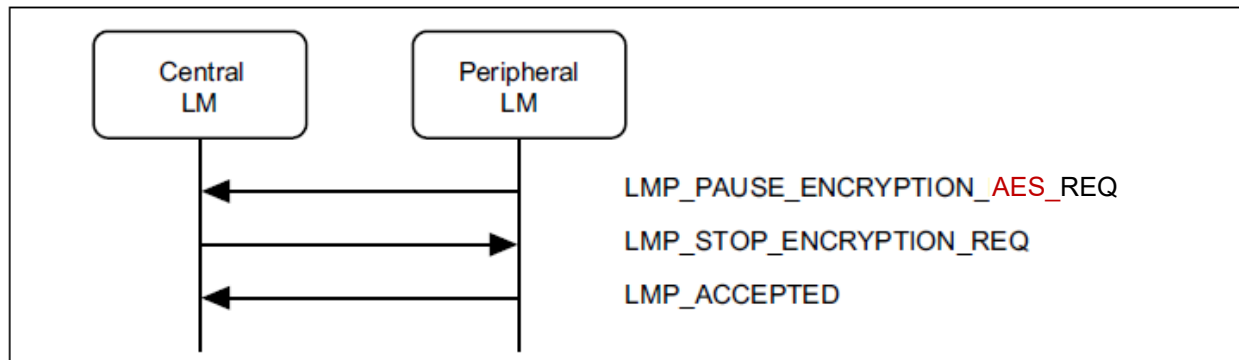
3 Changes to Core Specification v5.3

This section sets forth the specific changes and additions, using the formatting and color conventions described in Section 1.2, to Core Specification v5.3 [2].

3.1 Changes to Core Specification v5.3, Volume 2, Part C, Link Manager Protocol specification

3.1.1 [Modified Section] 4.2.5.5 Pause Encryption

[Modify Sequence 51 as shown.]



Sequence 51: Peripheral-initiated pausing of encryption (AES-CCM)

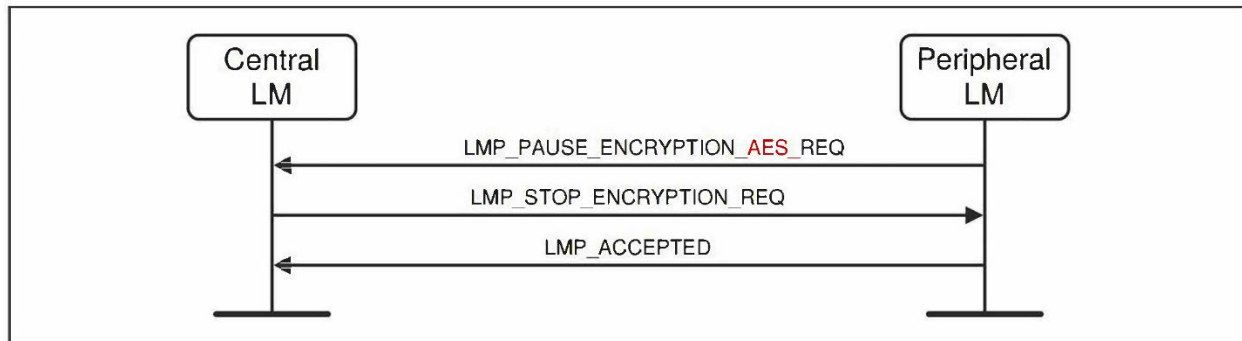
4 Changes to Core Specification v5.4

This section sets forth the specific changes and additions, using the formatting and color conventions described in Section 1.2, to Core Specification v5.4 [3].

4.1 Changes to Core Specification v5.4, Volume 2, Part C, Link Manager Protocol specification

4.1.1 [Modified Section] 4.2.5.5 Pause Encryption

[Modify Sequence 51 as shown.]



Sequence 51: Peripheral-initiated pausing of encryption (AES-CCM)

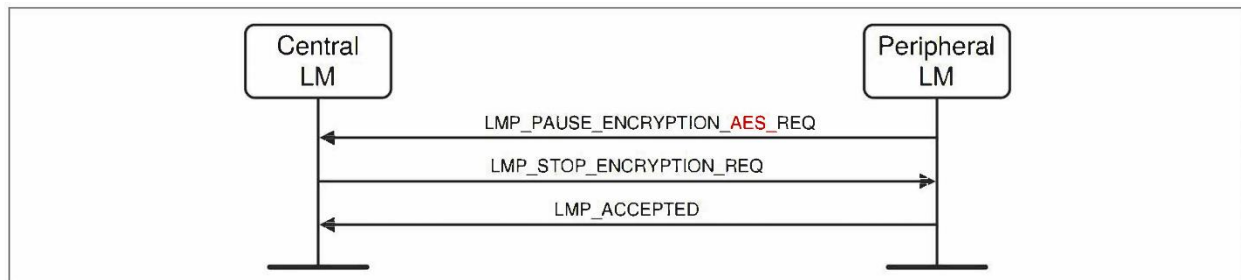
5 Changes to Core Specification v6.0

This section sets forth the specific changes and additions, using the formatting and color conventions described in Section 1.2, to Core Specification v6.0 [4].

5.1 Changes to Core Specification v6.0, Volume 2, Part C, Link Manager Protocol specification

5.1.1 [Modified Section] 4.2.5.5 Pause Encryption

[Modify Sequence 51 as shown.]



Sequence 51: Peripheral-initiated pausing of encryption (AES-CCM)

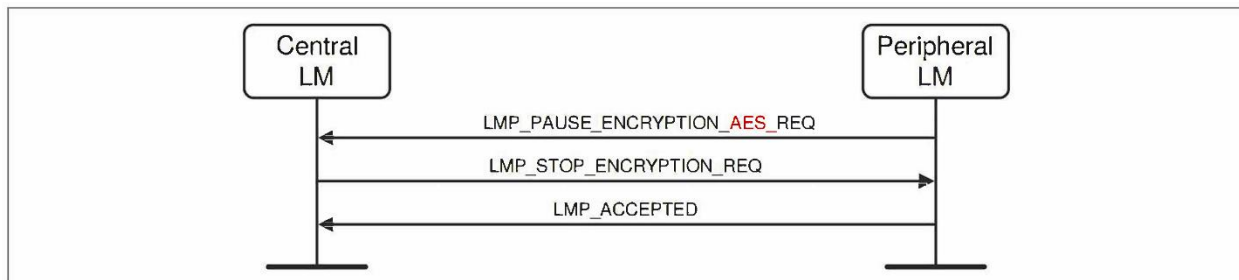
6 Changes to Core Specification v6.1

This section sets forth the specific changes and additions, using the formatting and color conventions described in Section 1.2, to Core Specification v6.1 [5].

6.1 Changes to Core Specification v6.1, Volume 2, Part C, Link Manager Protocol specification

6.1.1 [Modified Section] 4.2.5.5 Pause Encryption

[Modify Sequence 51 as shown.]



Sequence 51: Peripheral-initiated pausing of encryption (AES-CCM)

7 References

- [1] Bluetooth Core Specification (amended), Version 5.2
- [2] Bluetooth Core Specification (amended), Version 5.3
- [3] Bluetooth Core Specification (amended), Version 5.4
- [4] Bluetooth Core Specification, Version 6.0
- [5] Bluetooth Core Specification, Version 6.1