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

Contents

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

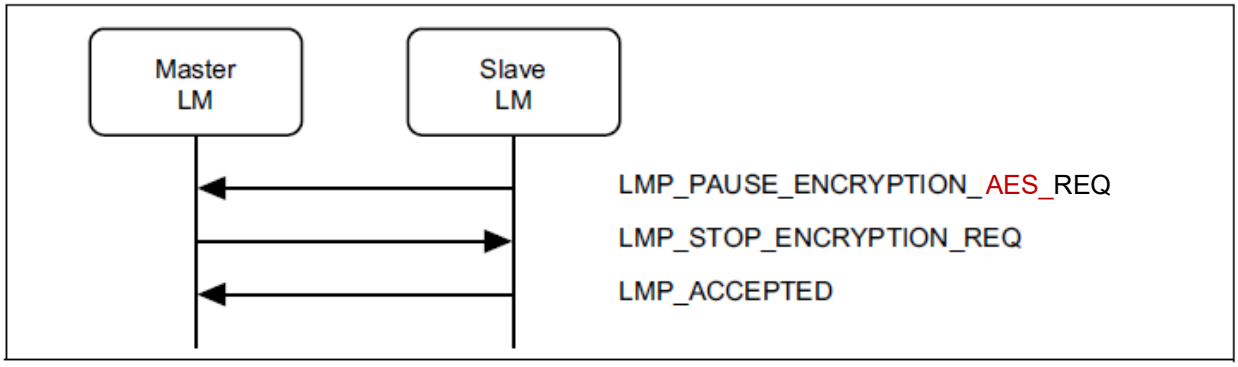
2 Changes to Core Specification v5.2

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)

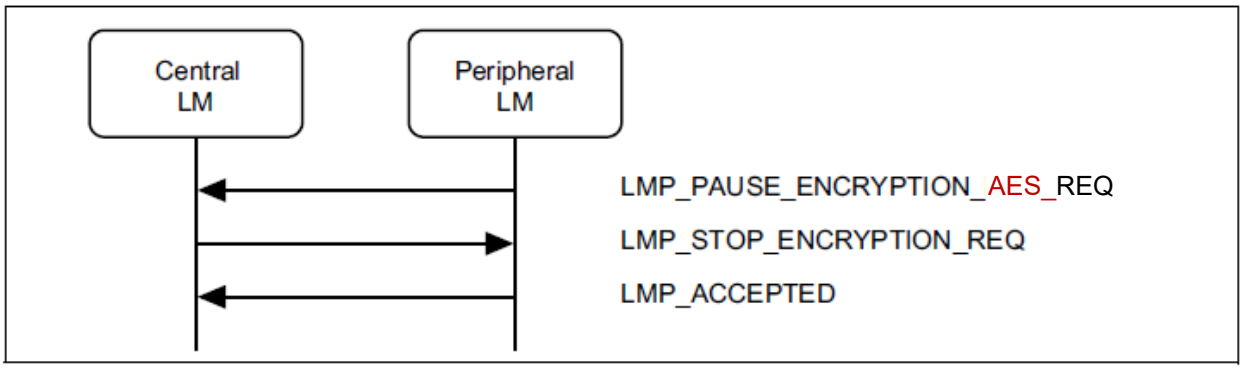
3 Changes to Core Specification v5.3

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)

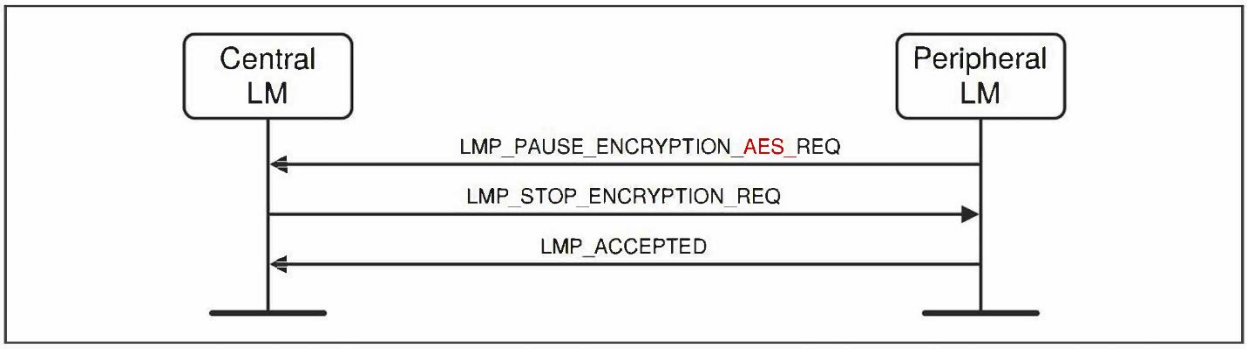
4 Changes to Core Specification v5.4

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)

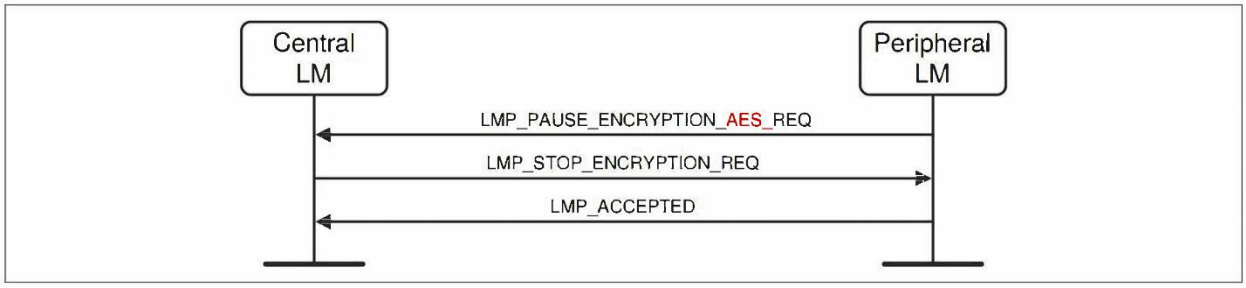
5 Changes to Core Specification v6.0

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)

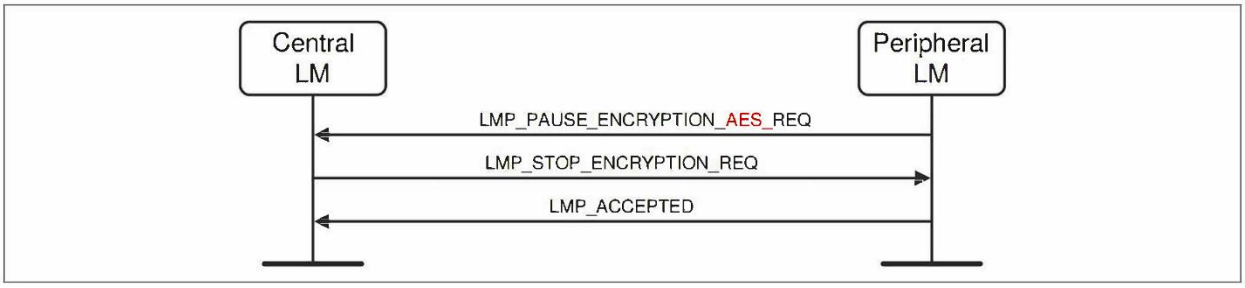
6 Changes to Core Specification v6.1

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