Errata Correction 23366: Security improvement for Broadcast_Code relay

***Bluetooth*® Errata Correction**

- **Version:** v1.0
- **Version Date:** 2024-10-01
- **Prepared By:** Generic Audio Working Group

This Errata Correction applies to the following specification (“Source Specification”):

- Broadcast Audio Scan Service v1.0 [1]

Abstract:

This correction mitigates an attack that can allow unauthorized access to the Broadcast_Code.

Version History

Version Number	Date (yyyy-mm-dd)	Comments
v1.0	2024-10-01	Adopted by the Bluetooth SIG Board of Directors.

Acknowledgments

Name	Company
Rasmus Abildgren	Bose Corporation
Chris St. John	Bose Corporation

Contents

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 explain the changes to be made to the Source Specification.
[…]	Indicates the section of the Source Specification 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 Broadcast Audio Scan Service v1.0

This Section sets forth the specific changes and additions, using the formatting and color conventions described in Section 1.2, to Broadcast Audio Scan Service v1.0.

2.1 Changes to Broadcast Audio Scan Service v1.0

2.1.1 **[Modified Section]** Section 3.1.1.4 Add Source operation

[The modified text with changes is shown below.]

[…]

- If the BIS is encrypted and the server has the correct encryption key to decrypt the BIS, the server shall write a value of 0x02 (Decrypting) to the BIG_Encryption field of the selected Broadcast Receive State characteristic.

- If the BIS is encrypted and the server has detected that a Broadcast_Code parameter value written by a client is not the correct encryption key to decrypt the BIS, the server shall write a value of 0x03 (Bad_Code) to the BIG_Encryption field of the selected Broadcast Receive State characteristic and the server shall write the value ~~of the incorrect encryption key~~0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF to the Bad_Code field of the selected Broadcast Receive State characteristic.

- If the BIS is not encrypted, the server shall write a value of 0x00 (Not encrypted) to the BIG_Encryption field of the selected Broadcast Receive State characteristic.

[…]

2.1.2 **[Modified Section]** Section 3.1.1.5 Modify Source operation

[The modified text with changes is shown below.]

[…]

- If the BIS is encrypted and the server has the correct encryption key to decrypt the BIS, the server shall write a value of 0x02 (Decrypting) to the BIG_Encryption field of the Broadcast Receive State characteristic.

- If the BIS is encrypted and the server has detected that a Broadcast_Code parameter value written by a client is not the correct encryption key to decrypt the BIS, the server shall write a value of 0x03 (Bad_Code) to the BIG_Encryption field of the Broadcast Receive State characteristic and the server shall write the value ~~of the incorrect encryption key~~0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF to the Bad_Code field of the selected Broadcast Receive State characteristic.

- If the BIS is not encrypted, the server shall write a value of 0x00 (Not encrypted) to the BIG_Encryption field of the Broadcast Receive State characteristic.

[…]

2.1.3 **[Modified Section]** Section 3.2 Broadcast Receive State

[The modified text with changes is shown below.]

[…]

BIG_Encryption	1	0x00: Not encrypted 0x01: Broadcast_Code required 0x02: Decrypting 0x03: Bad_Code (incorrect encryption key) All other values: RFU
Bad_Code	Varies	If BIG_Encryption field value = 0x00, 0x01, or 0x02: empty (zero length) If BIG_Encryption field value = 0x03 (Bad_Code), Bad_Code shall be set to the value ~~of the incorrect 16-octet Broadcast_Code that fails to decrypt the BIG~~0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
Num_Subgroups	1	Number of subgroups

[…]

2.1.4 **[Modified Section]** Section 3.2.1.7 BIG_Encryption field

[The modified text with changes is shown below.]

[…]

If the server has autonomously synchronized to a BIS that is encrypted, and the server has the correct encryption key to decrypt the BIS, the server shall write a value of 0x02 (Decrypting) to the BIG_Encryption field of the Broadcast Receive State characteristic.

If the server has autonomously synchronized to a BIS that is encrypted, and the server has detected that a received encryption key is not the correct encryption key to decrypt the BIS (the server can receive encryption keys via writes to the Broadcast Audio Scan Control Point or by other means), the server shall write a value of 0x03 (Bad_Code) to the BIG_Encryption field of the Broadcast Receive State characteristic and the server shall write the value ~~of the received incorrect 16-octet encryption key~~0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF to the Bad_Code field of the Broadcast Receive State characteristic.

If the server has autonomously synchronized to a BIS that is not encrypted, the server shall write a value of 0x00 (Not encrypted) to the BIG_Encryption field of the Broadcast Receive State characteristic.

3 References

[1] Broadcast Audio Scan Service, Version 1.0