

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



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 © 2024. 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 Broadcast Audio Scan Service v1.0	6
2.1	Changes to Broadcast Audio Scan Service v1.0.....	6
2.1.1	[Modified Section] Section 3.1.1.4 Add Source operation.....	6
2.1.2	[Modified Section] Section 3.1.1.5 Modify Source operation.....	6
2.1.3	[Modified Section] Section 3.2 Broadcast Receive State	6
2.1.4	[Modified Section] Section 3.2.1.7 BIG_Encryption field	7
3	References.....	8



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 BIG0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
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 key0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF** 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

