Bundesanstalt
für den Digitalfunk der Behörden und
Organisationen mit Sicherheitsaufgaben

# Bluetooth im Digitalfunk BOS

Sicherheitsrichtlinie

**Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS)**

Fehrbelliner Platz 3, 10707 Berlin

Postanschrift: 11014 Berlin

Inhaltsverzeichnis

1 Zweck ..... 5

2 Geltungsbereich ..... 5

3 Abgrenzung ..... 5

4 Verweise ..... 5

5 Bluetooth ..... 7

5.1 Bekannte Sicherheitslücken ..... 7

5.2 Pairing-Modi ..... 7

5.2.1 Gegenseitige Authentifizierung „Just Works“ ..... 8

5.2.2 Numeric Comparison ..... 8

5.2.3 Passkey Entry ..... 8

5.2.4 Out of Band (OoB) ..... 8

6 Mindestanforderungen an die Kopplung von Bluetoothgeräten mit Digitalfunkendgeräten ..... 9

6.1 Informationssicherheitsmanagement ..... 9

6.1.1 Nutzung von privaten Bluetoothgeräten ..... 9

6.2 Zertifizierung ..... 9

6.3 Technik ..... 10

7 Bekanntgabe ..... 10

8 Aktualisierung ..... 10

9 Inkrafttreten ..... 11

# Dokumenteneigenschaften

**Produktbezeichnung**

| **Bezeichnung** | **Bluetooth im Digitalfunk BOS - Sicherheitsrichtlinie** |
|---|---|
| Version | 1.0.0 |
| Letzte Änderung | 09.02.2023 |
| Status | Freigegeben per KoKo-Beschluss 36/009 |
| | Ein Dokument des gemeinsamen Informationssicherheitsmanagements der Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS) und von Bund und Ländern |

**Produkthistorie**

| **Version** | **Datum** | **Bemerkung** | **Status** | **Bearbeiter** |
|---|---|---|---|---|
| 0.0.1 | 22.02.2021 | Erster Entwurf auf Basis der Sicherheitsrichtlinie „Nutzung von Bluetooth im Digitalfunk BOS“ der AS Bayern | Entwurf | BDBOS |
| 0.0.2 | 20.04.2021 | Entwurf nach Diskussion in der 2. Sitzung der FG Bluetooth | Entwurf | EG Bluetooth |
| 0.0.3 | 09.06.2021 | Fortschreibung auf Basis der Rückmeldungen der FG Bluetooth als Diskussionsgrundlage für die 3. Sitzung der FG.<br>Entwurf nach Diskussion in der 3. Sitzung der FG Bluetooth | Entwurf | EG Bluetooth |
| 0.0.4 | 12.08.2021 | Vorläufig finalisierter Entwurf nach Diskussion in der 4. Sitzung der FG Bluetooth. | Entwurf | EG Bluetooth |
| 0.0.5 | 22.06.2022 | Einarbeitung der Kommentare im Nachgang der 24. Sitzung der AG Sicherheit | Entwurf | BDBOS |
| 0.0.6 | 17.11.2022 | Einarbeitung der Rückmeldung aus der 43. Sitzung des AK Betriebs | Entwurf | EG Bluetooth |

| Version | Datum | Bemerkung | Status | Bearbeiter |
|---|---|---|---|---|
| 1.0.0 | 09.02.2023 | Einarbeitung der Änderungen gemäß Protokolltext zu TOP C.2 der 36. Sitzung der KoKo<br>Umsetzung der Freigabe per KoKo-Beschluss 36/008 | Freigabe | BDBOS |

**Ansprechpartner**

| Organisationseinheit |
|---|
| BDBOS<br>Referat K 2 - Betriebskonzeption<br>11014 Berlin<br>Email: k2@bdbos.bund.de |

# 1 Zweck

Ziel dieser Sicherheitsrichtlinie ist, ein bundesweit einheitliches Sicherheitsniveau bei der Verwendung von Bluetoothgeräten mit Digitalfunkendgeräten[1] im Digitalfunk BOS zu etablieren und damit durch eine sichere operativ-taktische Nutzung zu einem sicheren Betrieb beizutragen.

# 2 Geltungsbereich

Diese Sicherheitsrichtlinie gilt im Geltungsbereich der Informationssicherheitsleitlinie für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben [1].

# 3 Abgrenzung

Dieses Dokument bezieht sich ausschließlich auf die Nutzung von Bluetooth.

Andere auf dem Markt verfügbare Verbindungstechnologien, die für eine Anbindung von Geräten an Digitalfunkendgeräte prinzipiell geeignet sind, werden nicht betrachtet.

Insbesondere sind die Standards IEEE 802.11 (WLAN) und ZigBee nicht Gegenstand dieser Sicherheitsrichtlinie.

# 4 Verweise

[1] Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS), *Informationssicherheitsleitleitlinie für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (ISL Digitalfunk BOS),* Berlin, 2021.

[2] Bundesamt für Sicherheit in der Informationstechnik, „CERT Bund - CB-K18/0810 Update 8," [Online]. Available: https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/2020/05/warnmeldung_cb-k18-0810_update_8.html.

[1] Definition gemäß [4].

[3] Bundesamt für Sicherheit in der Informationstechnik, „IT-Grundschutz-Kompendium," [Online]. Available: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html. [Zugriff am 25. Februar 2021].

[4] Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS), *Benutzerdefinierter Grundschutzbaustein SYS.3.b5 Digitalfunkendgeräte,* Berlin, 2021.

[5] Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS), *IT-Grundschutz-Profil Digitalfunk BOS – Endanwender,* Berlin, 2021.

[6] Bundesministerium der Justiz und für Verbraucherschutz, „Gesetze im Internet - Gesetz über die Errichtung einer Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS-Gesetz - BDBOSG)," 28 Juni 2021. [Online]. Available: https://www.gesetze-im-internet.de/bdbosg/BJNR203900006.html. [Zugriff am 12. August 2021].

[7] Bluetooth Special Interest Group, „Erratum 10734: Pairing Updates," 16. Juli 2018. [Online]. Available: https://www.bluetooth.org/docman/handlers/downloaddoc.ashx?doc_id=447440. [Zugriff am 17. Mai 2020].

[8] Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS), *Kopplung von Fremdinformationsverbünden mit dem Digitalfunk BOS - Sicherheitsrichtlinie,* Berlin, 2023.

# 5 Bluetooth

Bluetooth ist ein seit 1990 von der Bluetooth Special Interest Group entwickelter Standard zur Vernetzung von (lokalen) Geräten über kurze Distanz.[2]

Bluetooth nutzt für Funkübertragungen ebenso wie WLAN das in Deutschland von der Bundesnetzagentur freigegebene ISM-Band von 2,4 bis 2,4835 GHz. Deshalb können Bluetooth-Signale auch durch Dritte mit einfachsten Mitteln empfangen werden, was eine besondere Sicherheitsbetrachtung rechtfertigt.

## 5.1 Bekannte Sicherheitslücken

In der Spezifikation des Bluetooth-Protokolls bestanden bis zum 16.07.2018 mehrere Schwachstellen[3], von denen die Produkte der meisten Hersteller betroffen waren. Ein Angreifer in Funkreichweite kann Sicherheitsvorkehrungen umgehen und dadurch die Bluetooth-Kommunikation manipulieren. Alle standardkonformen Geräte, die von Sicherheitsforschern überprüft wurden, wiesen diese Sicherheitslücke auf. [2]

Versionen von Bluetooth, die nicht mindestens den Versionsstand 2.1 aufweisen, sind als prinzipiell unsicher zu bewerten, da sie die Verschlüsselung auf Nutzdatenebene nicht explizit fordern, bzw. die Verschlüsselung jederzeit pausiert werden kann. Zudem wiederholen sich die verwendeten Schlüssel (key-stream) aufgrund des auf Protokollebene neu startenden Timers nach 23,3 Stunden. Dies ermöglicht eine Korrumpierung der verwendeten Schlüssel. Die Vertraulichkeit bei Geräten unter Bluetooth-Version 2.1 ist nicht gewährleistet.

## 5.2 Pairing-Modi

Ab der Bluetooth-Version 2.1 (EDR) wurde Secure Simple Pairing (SSP) als ein weiterentwickeltes, sicheres Pairing-Verfahren eingeführt. Dieses enthält den allgemeinen Protokollablauf zum Aufbau einer neuen Bluetooth-Verbindung (genannt: Pairing). Generell gibt es hierbei vier Modi, die abhängig von den Kapazitäten der verwendeten Geräte den Ablauf des Verbindungsaufbaus beeinflussen. Zusätzlich zu den standardisierten Pairing–Modi existieren auch proprietäre Pairing-Modi.

---

[2] Die aktuellste Version des Standards zum Zeitpunkt der Erstellung dieser Dokumentenversion ist Bluetooth 5.2 mit Veröffentlichung am 31. Dezember 2019

[3] Die betroffenen Protokollversionen lauten: 5.0, 4.2, 4.1, 4.0, 3.0 + HighSpeed (HS) und 2.1 + Enhanced Data Rate (EDR), vgl. [7].

Von den nachfolgend näher erläuterten Pairing-Modi stellt lediglich die Pairing-Methode Passkey Entry eine gegenseitige Authentifizierung sicher. Insbesondere bei Geräten, die über kein Display und keine Eingabemöglichkeit verfügen, steht häufig lediglich die Variante „Just Works“ zur Verfügung.

### 5.2.1 Gegenseitige Authentifizierung „Just Works“

Digitalfunkendgeräte und Peripheriegeräte werden gleichzeitig in den Pairing-Modus versetzt und versuchen, sich gegenseitig auf festgelegten Frequenzen zu entdecken. Bei Erfolg werden die Geräte verbunden, es findet jedoch keine gegenseitige Authentifizierung statt. Daher ist dieser Modus anfällig für einen Man-In-The-Middle (MitM)-Angriff, bei dem ein drittes Bluetooth-Gerät die Verbindung zwischen beiden Geräten überbrückt und abfängt.

### 5.2.2 Numeric Comparison

Entspricht grundsätzlich der Methodik von „Just Works“, allerdings wird abhängig von den ausgehandelten Parametern (geheimer Schlüssel) von jedem Gerät eine 6-stellige Prüfziffer gebildet. Der Nutzer vergleicht diese Zahlen auf beiden Geräten und bestätigt ggf. die Übereinstimmung, woraufhin sichergestellt ist, dass kein MitM-Angriff stattgefunden hat.

### 5.2.3 Passkey Entry

Wie Numeric Comparison, allerdings wird der Vergleich der Prüfziffern von dem Gerät durchgeführt, an dem der Nutzer diese eingibt.

### 5.2.4 Out of Band (OoB)

Grundlegend wird die unter Numeric Comparison beschriebene Methodik verwendet, allerdings tauschen die zu verbindenden Geräte die Prüfziffern nicht unter Verwendung von Bluetooth aus, sondern beispielsweise über Near Field Communication (NFC).

# 6 Mindestanforderungen an die Kopplung von Bluetoothgeräten mit Digitalfunkendgeräten

## 6.1 Informationssicherheitsmanagement

Durch das Informationssicherheitsmanagement der jeweils zentral zuständigen Stelle MUSS gemäß der Verantwortungsteilung im Digitalfunk BOS [1] ein Sicherheitskonzept erstellt und umgesetzt werden. Die Verwendung des jeweils aktuellen Grundschutzbausteins zu mobilen Endgeräten [3], des benutzerdefinierten Grundschutzbausteins für Digitalfunkendgeräte [4] sowie des IT-Grundschutz-Profils Digitalfunk BOS – Endanwender [5] SOLLTE dazu in Erwägung gezogen werden.

### 6.1.1 Nutzung von privaten Bluetoothgeräten

Private Bluetoothgeräte dürfen grundsätzlich dienstlich nicht genutzt werden.

Die zentral zuständige Stelle kann abweichend bewusste und dokumentierte Ausnahmeregelungen schaffen.

## 6.2 Zertifizierung

Gemäß § 15a BDBOSG [5] dürfen im Digitalfunk BOS nur solche Endgeräte verwendet werden, die von der BDBOS als hierfür geeignet zertifiziert worden sind. Die Anforderungen für eine Zertifizierung ergeben sich aus den aktuell gültigen IOP-Richtlinien.

Zusätzlich sind die jeweils geltenden Anforderungen[4] an die Kopplung mit Geräten, die weitere externe Schnittstellen hin zu Drittnetzen parallel aktiv nutzen, zu berücksichtigen.

[4] bspw. das derzeit in Abstimmung befindliche Endgeräteschutzprofil (Protection Profile for a „Secure Coupling Solution for TETRA to Public Networks“) und ggf. weitere, heute noch unbekannte Anforderungen

### 6.3 Technik

Die Kopplung und damit die Verwendung von Bluetoothgeräten mit Digitalfunkendgeräten ist zulässig, wenn Geräte eingesetzt werden, die

1. mindestens die Version „Bluetooth 2.1 EDR“ unterstützen und die
2. in einem der Modi
   - Numeric Comparison oder
   - Passkey Entry,

betrieben werden.

Der Einsatz von Bluetooth in den Pairing-Modi „Just Works“ und OoB[5] bedarf zusätzlich einer gesonderten Risikoanalyse, Sicherheitsbetrachtung und abschließenden Bewertung durch die zentral zuständige Stelle.

Proprietäre Pairing-Modi müssen ein mindestens gleichwertiges Sicherheitsniveau zu den standardisierten Pairing-Modi bieten. Sie dürfen daher nur nach positiver Prüfung durch das BSI verwendet werden.

Das Aktualisieren der Gerätefirmware soll jeweils durch die verwendete Hardware unterstützt werden. Der Organisations- und/oder Betriebsablauf der Updateprozesse ist durch die Betreiber regelmäßig und zeitnah zu regeln.

Ausschließlich Digitalfunkendgeräte, die vollständig gemäß Abschnitt 6.2 zertifiziert sind, DÜRFEN mit Bluetoothgeräten gekoppelt werden, die weitere externe Schnittstellen hin zu Drittnetzen parallel aktiv nutzen.

## 7 Bekanntgabe

Die Sicherheitsrichtlinie ist im Nutzungs- und Betriebshandbuch für den Digitalfunk BOS (NBHB) veröffentlicht.

## 8 Aktualisierung

Die Sicherheitsrichtlinie wird regelmäßig, mindestens alle zwei Jahre, überprüft und aktualisiert.

[5] aufgrund der zusätzlich benötigten Übertragungstechnologie

# 9 Inkrafttreten

Die Sicherheitsrichtlinie tritt nach Beschluss durch die KoKo und mit Veröffentlichung im NBHB in Kraft.