BLUETOOTH BLOG

Bluetooth Pairing Part 2 Key Generation Methods

June 9, 2016 | Kai Ren | Bluetooth Low Energy

In Bluetooth Pairing Part 1: Pairing Feature Exchange, we talked about the pairing feature exchange in *Bluetooth*® with low energy. The pairing feature exchange is used to make both devices, initiator and responder, understand each other's pairing features.

The pairing features that can be enabled are:

- **OOB Data Flag bit**
- **MITM—Man-In-The-Middle bit**
- **SC—LE secure connection indicator bit**
- **IO Cap—IO Capabilities**

**For an introduction to these features, please refer to Bluetooth Pairing Part 1: Pairing Feature Exchange.*

After this exchange, both devices can select which key generation method is used in subsequent phases. Here is the list of key generation methods for Bluetooth LE legacy pairing and Bluetooth LE Secure Connection.

Bluetooth LE Legacy Pairing:

- **Just Works**
- **Passkey**
- **Out-of-Band(OOB)**

Bluetooth LE Secure Connection includes the three methods above and adds one new one:

- **Numeric Comparison**

Workflow

Here is the workflow on how a device decides which key generation method to use.

Step 1: Check SC bit in pairing feature exchange frame. If the SC bit is equal to 1 on both sides, an LE secure connection is used, go to step 2. Otherwise, it is LE legacy pairing, and go to step 3.

Step 2: When it is LE secure connection, below is the matrix that initiator and responder will follow.

		Initiator			
		OOB Set	**OOB Not Set**	**MITM Set**	**MITM Not Set**
Responder	**OOB Set**	Use OOB	Use OOB		
	OOB Not Set	Use OOB	Check MITM		
	MITM Set			Use IO Capabilities	Use IO Capabilities
	MITM Not Set			Use IO Capabilities	Use Just Works

- "Use OOB" means Out-of-Band is selected.
- "Check MITM" means ignore "OOB Data Flag" and check MITM flag, "Man-In-The-Middle" flag.
- "Use IO Capabilities," go to step 4 to select the key generation method depending on IO Capabilities of both devices.

Step 3: When it is LE legacy pairing, below is the matrix that initiator and responder will follow.

- "Use OOB" means Out-of-Band is selected.
- "Check MITM" means ignore "OOB Data Flag" and check the MITM flag, "Man-In-The-Middle" flag.
- "Use IO Capabilities", go to step 4 to select the key generation method depending on IO Capabilities of both device.

Step 4: Below is a mapping of the IO Capabilities to Key Generation Method. With this table, both devices, initiator and responder, will find an appropriate method for connecting depending on their pairing features.

After this, the initiator and responder understand the method that will be used in the key generation phase. In part 3, I will introduce how to generate the corresponding key in Bluetooth® LE legacy pairing by using the Passkey method.

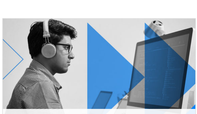
FEATURED DOWNLOAD

Bluetooth 5: Go Faster, Go Further

Download this comprehensive overview to discover how Bluetooth 5 significantly increases the range, speed, and broadcast messaging capacity of Bluetooth applications, making use cases in smart home automation, enterprise, and industrial markets a reality.

INSTANT DOWNLOAD

Blog Posts | Member Blogs | Papers | Study Guides | Videos



Blog Post

Best Practices for Using a Standalone Auracast™ Transmitter

The recently released Auracast™ Simple Transmitter Best Practices Guide describes a typical, qualified implementation...

READ MORE

Blog Post

Auracast™ Broadcast Audio Introduces New Opportunities for Product Developers & Public Locations

Bluetooth® technology recently introduced a new Bluetooth capability, Auracast™ broadcast audio, that will deliver life-changing...

READ MORE

Blog Post

Introducing: The Bluetooth Low Energy Primer

Bluetooth® technology has been around for more than 20 years. Initially created to allow...

READ MORE

© 2022 Bluetooth SIG, Inc. All rights reserved.