Security, Bluetooth Low Energy

To make sure the communication over Bluetooth® with its low energy feature (Smart, BLE, LE) is always secure and protected, the Bluetooth Core Specification provides several features to cover the encryption, trust, data integrity and privacy of the user's data. We will further explain the technical details of those features in this article.

Pairing

The pairing mechanism is the process where the parties involved in the communication exchange their identity information to set up trust and get the encryption keys ready for the future data exchange. Depending on the user's requirement and the capability of the device, Bluetooth has several options for pairing.

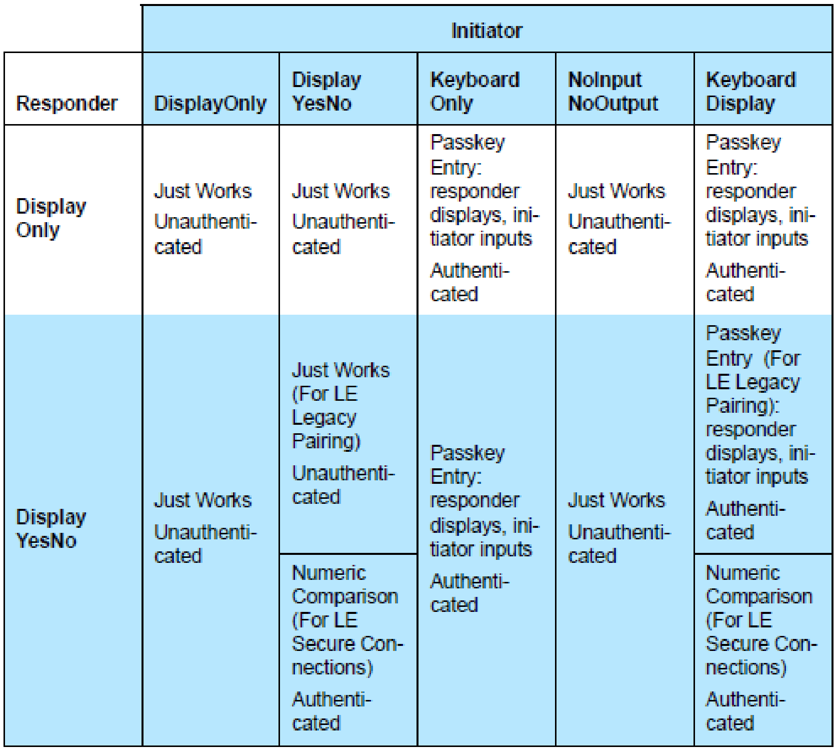
In version 4.0 and 4.1 of the core specification, Bluetooth with its low energy functionality uses the Secure Simple Pairing model (referred to as LE Legacy after the Bluetooth 4.2 release), in which devices choose one method from Just Works, Passkey Entry and OOB based on the input/output capability of the devices.

With the release of the Bluetooth Core Specification version 4.2, security is greatly enhanced by the new LE Secure Connections pairing model. In this new model, the numeric comparison method is added to the other three methods and the Elliptical Curve Hellman-Diffie (ECDH) algorithm is introduced for key exchange in this process.

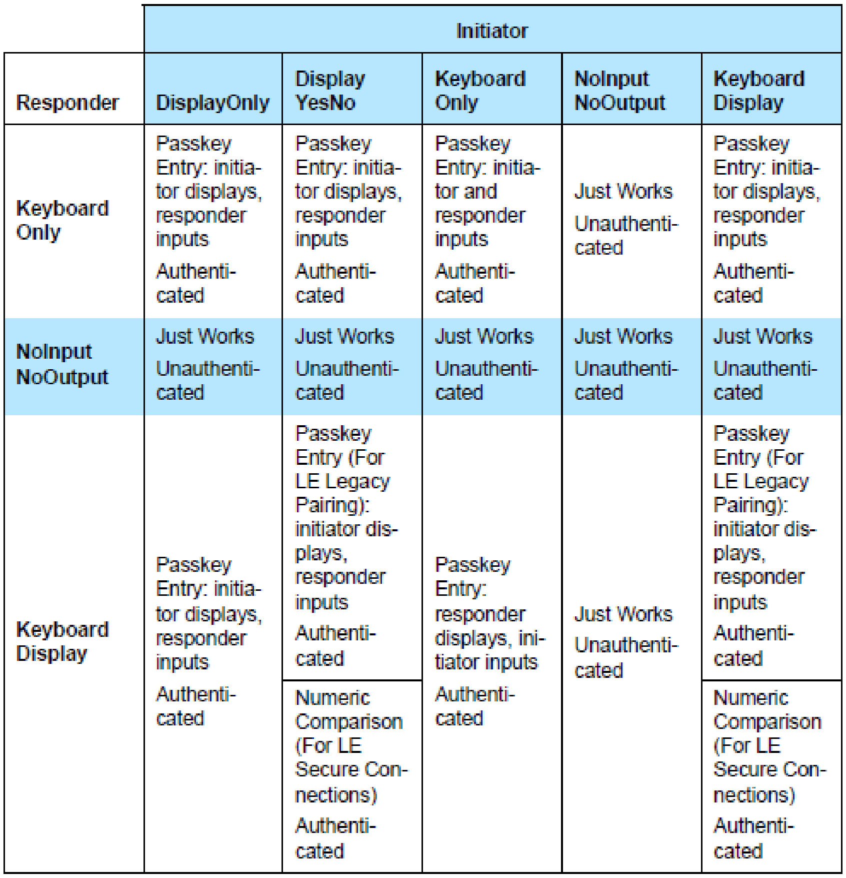
Reference:

- BLUETOOTH SPECIFICATION Version 4.2 [Vol 1, Part A] 5.4.2 Key Generation
- BLUETOOTH SPECIFICATION Version 4.2 [Vol 3, Part H] 3.6.1 Key Distribution and Generation

If you use LE legacy pairing, each of these association models is similar to BR/EDR Secure Simple Pairing with the exceptions that Just Works and Passkey Entry do not provide any passive eavesdropping protection. In LE Secure Connections pairing, the four association models are functionally equivalent to BR/EDR Secure Connections. The use of each association model is based on the I/O capabilities of the devices. You could choose the best pairing method based on the following table.



	Initiator				
Responder	DisplayOnly	Display YesNo	Keyboard Only	NoInput NoOutput	Keyboard Display
Display Only	Just Works Unauthenticated	Just Works Unauthenticated	Passkey Entry: responder displays, initiator inputs Authenticated	Just Works Unauthenticated	Passkey Entry: responder displays, initiator inputs Authenticated
Display YesNo	Just Works Unauthenticated	Just Works (For LE Legacy Pairing) Unauthenticated Numeric Comparison (For LE Secure Connections) Authenticated	Passkey Entry: responder displays, initiator inputs Authenticated	Just Works Unauthenticated	Passkey Entry (For LE Legacy Pairing): responder displays, initiator inputs Authenticated Numeric Comparison (For LE Secure Connections) Authenticated



	Initiator				
Responder	DisplayOnly	Display YesNo	Keyboard Only	NoInput NoOutput	Keyboard Display
Keyboard Only	Passkey Entry: initiator displays, responder inputs Authenticated	Passkey Entry: initiator displays, responder inputs Authenticated	Passkey Entry: initiator and responder inputs Authenticated	Just Works Unauthenticated	Passkey Entry: initiator displays, responder inputs Authenticated
NoInput NoOutput	Just Works Unauthenticated	Just Works Unauthenticated	Just Works Unauthenticated	Just Works Unauthenticated	Just Works Unauthenticated
Keyboard Display	Passkey Entry: initiator displays, responder inputs Authenticated	Passkey Entry (For LE Legacy Pairing): initiator displays, responder inputs Authenticated Numeric Comparison (For LE Secure Connections) Authenticated	Passkey Entry: responder displays, initiator inputs Authenticated	Just Works Unauthenticated	Passkey Entry (For LE Legacy Pairing): initiator displays, responder inputs Authenticated Numeric Comparison (For LE Secure Connections) Authenticated

Reference:

- BLUETOOTH SPECIFICATION Version 4.2 [Vol 1, Part A] 5.4.1 Association Models

Key Generation

Key generation in Bluetooth with low energy is performed by the Host on each low energy device independent of any other. Note: Key generation in BR/EDR is performed in the Controller. By performing key generation in the Host, the key generation algorithms can be upgraded without the need to change the Controller.

When using Bluetooth LE Secure Connections, the following keys are exchanged between master and slave:

- Connection Signature Resolving Key (CSRK) for Authentication of unencrypted data
- Identity Resolving Key (IRK) for Device Identity and Privacy

In LE Secure Connections, the public/private key pair is generated in the Host and a Secure Connection Key is generated by combining contributions from each device involved in pairing.

Encryption

Encryption in Bluetooth with low energy uses AES-CCM cryptography. Like BR/EDR, the LE Controller will perform the encryption function. This function generates 128-bit encryptedData from a 128-bit key and 128-bit plaintextData using the AES-128-bit block cypher as defined in FIPS-1971.

Reference:

- BLUETOOTH SPECIFICATION Version 4.2 [Vol 3, Part H] 3.6.2 Encryption Information

Signed Data

Bluetooth with its low energy features supports the ability to send authenticated data over an unencrypted transport between two devices with a trusted relationship. This means that in some circumstances where the communication channel is not encrypted, the device could still have a method to maintain and ensure the data authentication. This is accomplished by signing the data with a CSRK. The sending devices place a signature after the Data Protocal Data Unit (PDU). The receiving device verifies the signature and, if the signature is verified, the Data PDU is assumed to come from the trusted source. The signature is composed of a Message Authentication Code generated by the signing algorithm and a counter. The counter is used to protect against a replay attack and is incremented on each signed Data PDU sent.

Reference:

- BLUETOOTH SPECIFICATION Version 4.2 [Vol 3, Part H] 3.6.6 Signing Information

Privacy Feature

Since Bluetooth 4.0, Bluetooth with low energy supports a feature that reduces the ability to track a LE device over a period of time by changing the Bluetooth device address on a frequent basis. The frequently changing address is called the private address and the trusted devices can resolve it.

In order to use this feature, the devices involved in the communication need to be previously paired. The private address is generated using the devices IRK exchanged during the previous pairing/bonding procedure.

There are two variants of the privacy feature. In the first variant, private addresses are resolved and generated by the Host. This is used in the pre-4.2 Bluetooth stacks. In the second variant, private addresses are resolved and generated by the Controller without involving the Host after the Host provides the Controller device identity information. Bluetooth 4.2 compliant devices use this design.

Reference:

- BLUETOOTH SPECIFICATION Version 4.2 [Vol 6, Part B]

How Bluetooth Utilizes these Features to Protect Your Information

The goal of the low energy security mechanism is to protect communication between devices at different levels of the stack. Below are commons types of attacks against various wireless communication protocols, and how Bluetooth addresses them.

Man-in-the-Middle (MITM)

A MITM requires an attacker to have the ability to both monitor and alter or inject messages into a communication channel. One example is active eavesdropping, in which the attacker makes independent connections with the victims and relays messages between them to make them believe they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker. The attacker must be able to intercept all relevant messages passing between the two victims and inject new ones.

In LE Legacy pairing, MITM protection is obtained by using the passkey entry pairing method or may be obtained using the out of band pairing method. In LE Secure Connections pairing, MITM protection could be obtained by using the numeric comparison method as well as the previous two methods. To ensure that Authenticated MITM Protection (the protection through authentication) is generated, the selected Authentication Requirements option must have MITM protection specified.

Passive Eavesdropping

Passive Eavesdropping is secretly listening (by using a sniffing device) to the private communication of others without consent. LE Secure Connection uses ECDH public key cryptography as a means to thwart passive eavesdropping attacks. ECDH provides a very high degree of strength against passive eavesdropping attacks. The algorithm provides a mechanism to exchange keys over an unsecured channel.

Privacy/Identity Tracking

Since most of the Bluetooth with low energy advertisement and data packets have the source addresses of the devices that are sending the data, third-party devices could associate these addresses to the identity of a user and track the user by that address. This can be protected by frequently changing private addresses so only the trusted parties could resolve them.

Reference:

- BLUETOOTH SPECIFICATION Version 4.2 [Vol 6, Part B]

Bluetooth with low energy specification has defined powerful security features to protect the communication of a user's data and identity. Those features are either NIST compliant or FIPS approved. The Bluetooth SIG encourages and actively promotes the proper implementation of these security measures built into Bluetooth technology.