White Paper

Bluetooth® Low Energy Technology that Brings the IoT to Life

Tomohiko Ohtsu, Senior Staff Engineer, MCU Product Marketing,
Renesas Electronics Corporation
January 2019

Abstract

Renesas Electronics offers a lineup of Bluetooth® Low Energy MCUs that enable wireless communications with low power consumption. Bluetooth Low Energy is an essential wireless method of communication in this era of IoT in which an internet connection is necessary for the sharing of information between not only computers and microcontroller-based devices, but nearly all equipment and appliances used throughout the world. To understand this further, this paper will delve deeper into the mechanics of Bluetooth Low Energy technology.

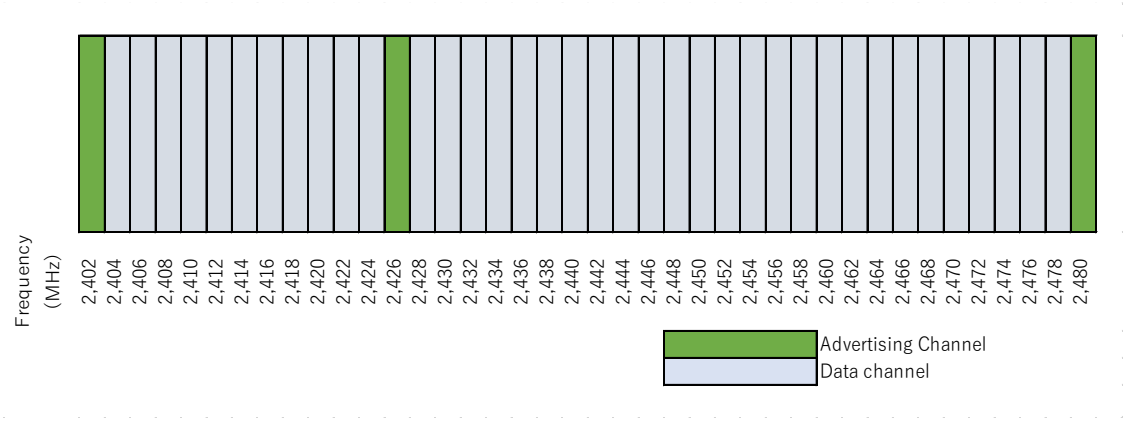
Introduction

Bluetooth Low Energy employs short-distance wireless networks called Wireless Personal Area Network (WPAN). WPANs boast data exchange within 10 or so meters while consuming much less power than any other wireless specifications. Various types of WPANs are available; ZigBee® and Bluetooth are the two main standardized wireless networks, while there are also many independent, non-standardized communication protocols available. Bluetooth Low Energy is employed in many smartphone applications, making it the most widely used format in the market.

When discussing Bluetooth Low Energy communication technology, it is important to remember that this Bluetooth wireless technology is not the same specification as the

Bluetooth wireless technology referred to in conventional voice communications. Bluetooth Low Energy technology operates in an 80MHz band with a range from 2.400GHz to 2.480GHz and is separated into 40 channels with 2MHz spacing. There are two types of channels:

- Advertising channels: 3
- Data channels: 37



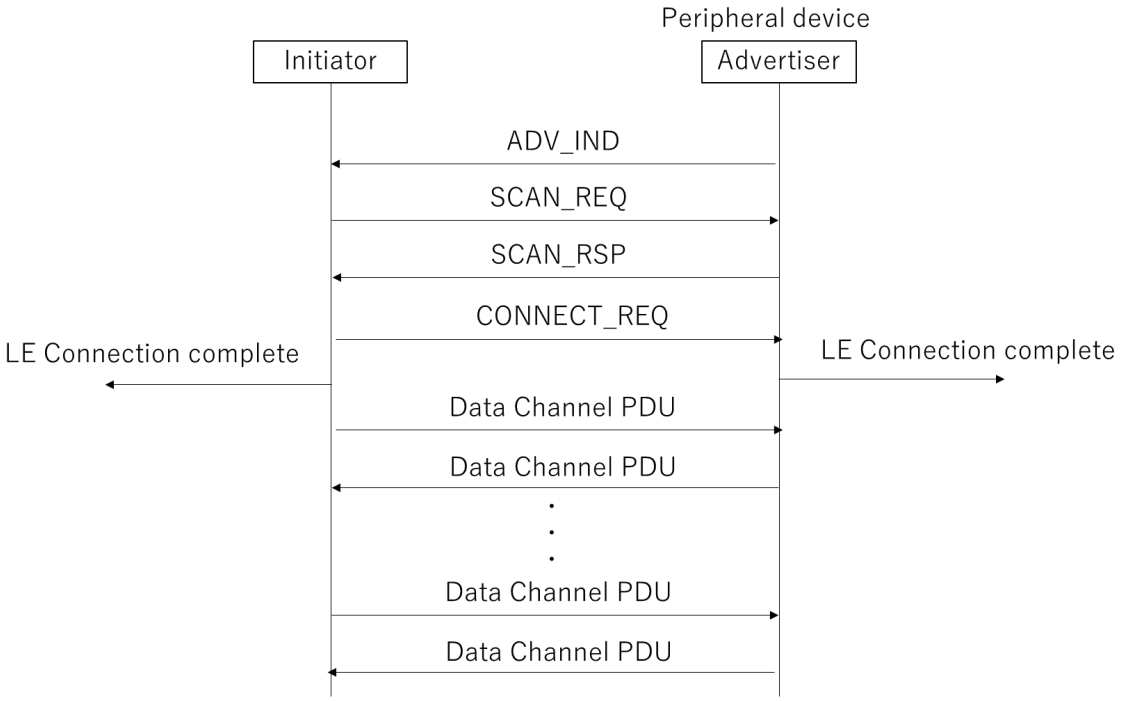
Bluetooth Low Energy Communication Frequency Channels

The two types of channels are used as follows:

Peripheral devices send advertising packets on the advertising channels. The advertising packet broadcasts (transmits) its device location to other devices in the area via three different channels in advertising intervals. It then detects and wirelessly connects with other Bluetooth Low Energy devices. The advertising interval is between 20 milliseconds and 10.24 seconds, as stipulated in the Bluetooth specifications. The length of the interval affects the ease of the connection and the amount of power consumed.

Data channels are used for communication between devices after the connection is completed. With Bluetooth Low Energy, data channels employ Adaptive Frequency Hopping (AFH) for robust communication in which transmission switches from channel to channel based on the connection interval. The term “adaptive” is used to indicate channel switching to counteract frequency interference. Bluetooth Low Energy also applies a time-out wait, implementing hopping to ensure continued communication even when, for example, communication would otherwise be interrupted due to multiple transmissions. Bluetooth Low Energy communication is structured so that communications are not interrupted even when some channels incur interference. The Bluetooth specifications define the connection

interval period from 7.5 milliseconds to four seconds. The length of the interval period affects throughput and power consumption.



Example of Bluetooth Low Energy Operational Flow

Now let's discuss Bluetooth security.

Bluetooth data transmissions can be encrypted. To enable encrypted transmissions, first unique information is exchanged between two devices, a process referred to as "pairing." Pairing leads to "bonding," where unique security and identifying information is exchanged and stored. In other words, devices are paired by exchanging security features, and then bonded by storing the device and pairing information exchanged by the devices.

Bluetooth Low Energy security requirements are described with the terms "security mode" and "security level." Pairing is required to satisfy each security requirement. There are two types of pairing: authenticated pairing, which protects from Man-in-the-Middle (MITM) attacks and unauthenticated pairing, which does not protect from such attacks.

Bluetooth Low Energy uses four types of pairing, as described here.

- Just Works: Pairing by simply selecting a device without any other confirmations. This is LE Security Mode 1 Level 2; not authenticated and no MITM protection.
- Passkey Entry: Pairing based on input of a 6-digit authentication code. This is LE Security Mode 1 Level 3; authenticated and MITM protected.
- Out of Band (OOB): Pairing with communication types other than Bluetooth (wired, NFC, etc.) This is LE Security Mode 1 Level 3; authenticated and MITM protected.
- Numeric Comparison: Pairing that is the same as 'Just Works', but with an added step in which each device generates and displays a 6-digit code, requiring a match to be confirmed. This method can only be used for LE Secure Connections that were added to Bluetooth 4.2.

Security Mode	Security Level	Overview	Notes
LE Security Mode 1	1	No security (no confirmation, no encryption)	
	2	Encrypted based on unauthenticated pairing	Pairing with Just Works
	3	Encrypted based on authenticated pairing	Pairing with Passkey and OOB
	4	Encrypted based on authenticated LE secure connections pairing	Not supported by RL78/G1D
LE Security Mode 2	1	Data signature based on unauthenticated pairing	
	2	Data signature based on authenticated pairing	

LE Security Modes and Levels

LE Security Mode 1 Level 3 satisfies the security requirements of LE Security Mode 2.

Data signing in LE Security Mode 2 is used mainly for high-speed connection, disconnection and transfer and, therefore, mostly used when data is not encrypted. Data signing employs the Connection Signature Resolving Key (CSRK), as well as encryption and authentication.

The method used to generate keys in each pairing method depends on the configuration of the device. Out of Band (OOB) can be used for protection against MITM attacks if the device is configured with OOB as the key exchange protocol.

Passkey Entry is another method, requiring a 6-digit temporary key. Passing the 6-digit number between devices reduces MITM attack success rate to only 1/1,000,000. In other words, the danger of falling victim to an MITM attack is extremely low. Further, since Bluetooth Low Energy communications are limited to short distances, any perpetrator would have to be very close to “listen in.” As the possibility of eavesdropping during pairing is low, Passkey Entry is considered highly protective when used indoors. Connections made after Passkey Entry is confirmed are encryption secured and can be used with confidence.

Other suggestions for MITM protection: set the system so that pairing is not carried out unless it is in the pairing mode, or only allow pairing in physically isolated areas to avoid MITM attacks. Mode settings can be either physical settings or communication settings.

The RL78/G1D does not support the LE Secure connection option added to Bluetooth 4.2. LE Secure connections can only be paired using ‘Numeric Comparison’, which requires a display function on both devices. Depending on the product, there may not be enough space to mount a display function. Such issues should be considered before proceeding with any application design.

The following table summarizes pairing methods and device structure (IO Capabilities) mapping.

	Transmitting Device				
Responding Device	Display Only	Display Yes No	Keyboard Only	No Input No Output	Keyboard Display
Display Only	Just Works	Just Works	Passkey Entry	Just Works	Passkey Entry
Display Yes No	Just Works	Just Works	Passkey Entry	Just Works	Passkey Entry:
		Numeric Comparison (For LE Secure connections)			Numeric Comparison (For LE Secure Connections)
Keyboard Only	Passkey Entry	Passkey Entry	Passkey Entry	Just Works	Passkey Entry
No Input No Output	Just Works	Just Works	Just Works	Just Works	Just Works
Keyboard Display	Passkey Entry	Passkey Entry	Passkey Entry	Just Works	Passkey Entry
		Numeric Comparison (For LE Secure connections)			Numeric Comparison (For LE Secure connections)

Device Structure (IO Capabilities) Mapping

The following describes key exchange methods used for encryption. Key exchange is carried out in phases.

Phase 1: Pairing Feature Exchange (device structure (IO Capabilities), authentication requirements, etc.)

Phase 2: Short Term Key (STK) Generation. STK Generation is based on the information exchanged in Phase 1.

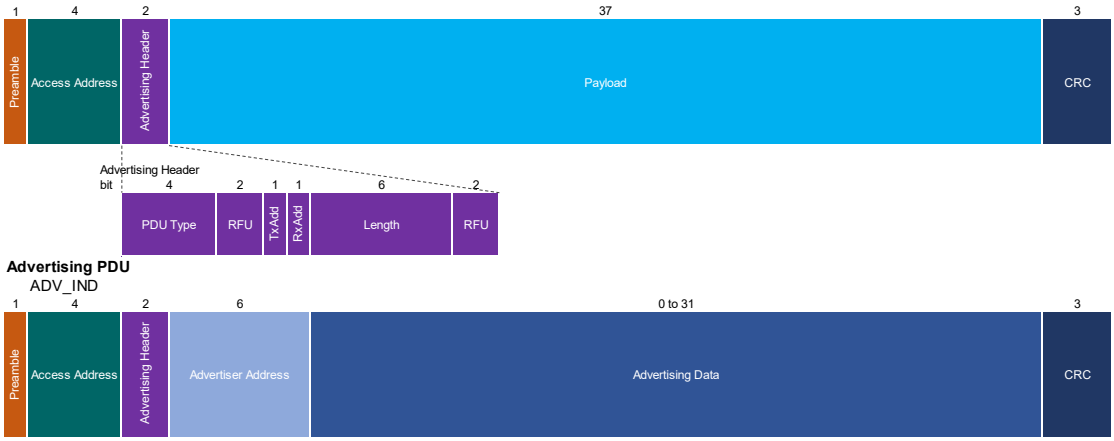
Phase 3: Transport Specific Key Distribution. Distribution is carried out with the link encrypted using the key generated in Phase 2.

The following is a list of keys handled in pairing, encryption, private address resolution, signed data and the like. These keys are used in each phase.

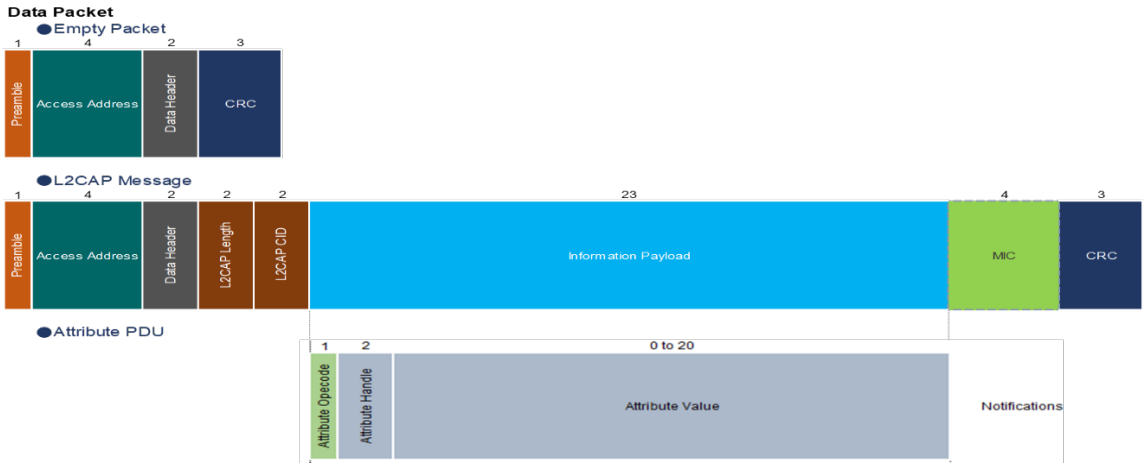
Key Type	Description	Generation
TK (Temporary Key)	128 bits Used in pairing phase 2 to generate STK.	Generated in the application.
STK (Short Term Key)	128 bits Generated in pairing phase 2 using the TK. Used after phase 2 for link encryption.	Generated in Bluetooth Low Energy software.
LTK (Long Term Key)	128 bits (partially used according to the agreed upon key size) Used to generate the session key required for encryption.	Generated in the application.
EDIV (Encrypted Diversifier)	16 bits Used to identify the LTK. EDIV is generated each time the LTK is distributed.	Generated in the application.
RAND (Random Number)	64 bits Used to identify the LTK. RAND is generated each time the LTK is distributed.	Generated in the application.
IRK (Identity Resolving Key)	128 bits Used to create and resolve a random address.	Generated in the application.
CSRK (Connection Signature Resolving Key)	128 bits Used to create a signature and confirm the signature of received data.	Generated in the application.

Bluetooth Low Energy Key Types

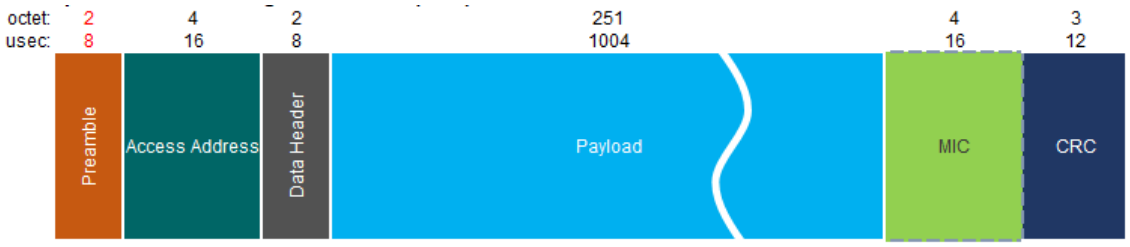
Now let’s move on to transmission packets. The advertising packet specified in the Bluetooth 4.0 Specification (Low Energy) uses 31 bytes for advertising data. The new Bluetooth beacon is hardware used by low energy devices to broadcast (transmit) this advertising packet at regular intervals and which is then received as a beacon. An application example of a beacon (broadcasting) device is provided later in this paper.



A packet employed to communicate between devices using a data channel can use up to 20 bytes for data transmission, as shown in the structure below. If the data does not fit into 20 bytes, it is split into 20-byte units.

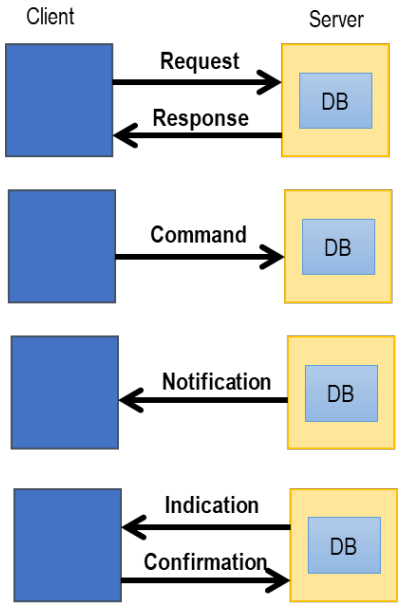


With the LE Data Extension added to Bluetooth 4.2, transmission packets can be further extended, as shown below. This LE Data Extension is an optional specification and is not supported by the RL78/G1D.



Next let's look at how communication packets are handled. There are two kinds of packets: those with and those without communication confirmation/response. Communication processing combinations are as follows.

In communication with a Bluetooth Low Energy response, the response (Response/Confirmation) is sent in the next interval operation. In other words, in a 1-second interval operation, a response transmission is sent one second later, meaning that it takes two intervals to complete a communication's transmission/response. In high-speed data communication, the process can be accelerated by using communication that does not send a response of transmission confirmation; instead, the application side should be set to confirm the transmission.



The Bluetooth Low Energy data exchange specification was described earlier in detail. The original concept of Bluetooth Low Energy, as indicated by its name, was to provide low power consumption operations. To do so, it was more effective to send small amounts of data. This concept extended the life of batteries, enabling use for several years without replacement. The goal was to use Bluetooth connections to connect low-power devices and battery-operated applications, and then transmit the data via an internet connection.

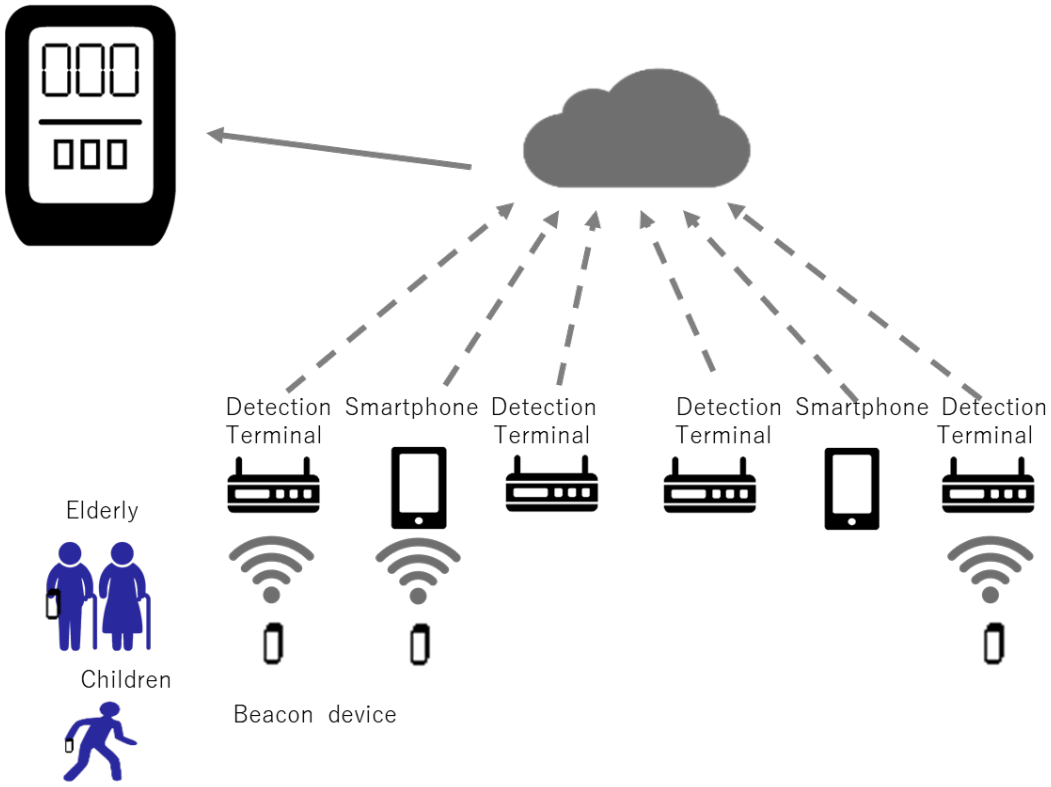
Recently, Bluetooth Low Energy in the Bluetooth specification was revised based on Bluetooth 4.0. The specification added large capacity, high-speed communications and

long-distance communications. Bluetooth 5 was released in 2016 with these features offered as options.

In the future, the core standard of Bluetooth Low Energy (as established in Bluetooth 4.0) will be a required function and will support all Bluetooth Low Energy ready products. Using this Bluetooth Low Energy core specification will ensure reliable connections and will, therefore, be implemented in a multitude of devices going forward. We can also expect Bluetooth Low Energy to help avoid connectivity issues.

Let’s move on to a couple of sample applications. To begin with, we look at a beacon device that brings an application to life by broadcasting an advertising packet, a feature unavailable in conventional Bluetooth.

Beacon devices are often used as locators carried by the elderly or young children. A sensing terminal is installed at a related facility to receive radio waves from the beacon device. Detection terminals would, for example, be installed in schools for children and community centers for elderly members, as well as in the home and other public places. Another example would be to have local volunteers carry around a smartphone installed with a special application that allows the smartphone to receive radio waves from the beacon device. The received beacon information is stored in the cloud along with the location information of the detection terminal or smartphone. The stored data is then used to indicate the beacon location on a smartphone map, which only family members or guardians linked to the beacon device can access. Using Bluetooth Low Energy in a beacon device allows caregivers to be mindful of and protect their charges, even when not located in the same vicinity.



Example of Protective Locator Terminal

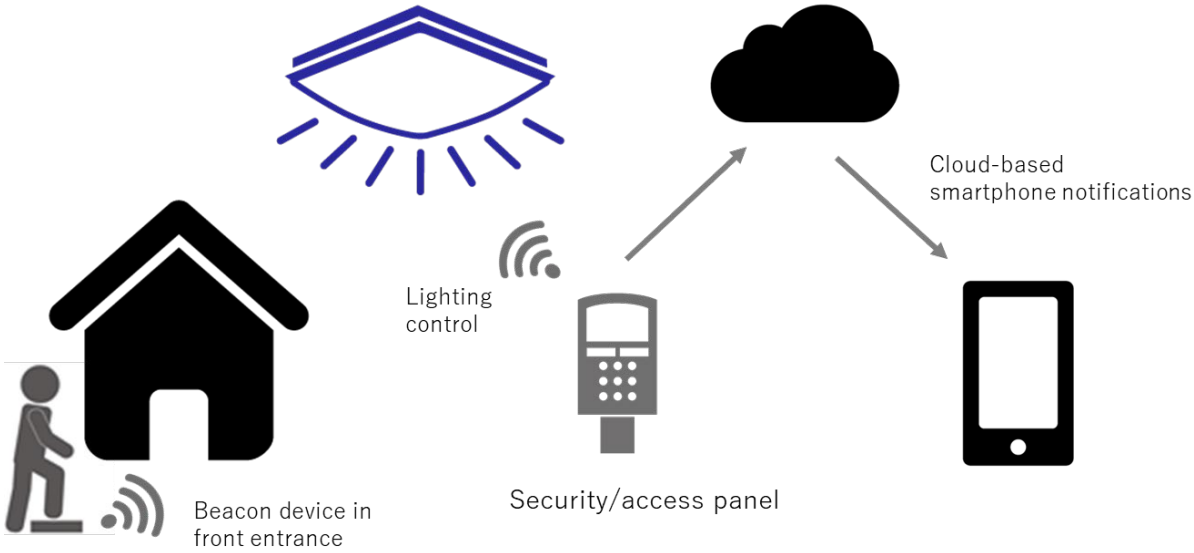
This example is described on the Renesas home page. Please use the link below to view.

A Bluetooth Low Energy solution advancing the features of the protective locater service “otta” with IoT technology:
https://www.renesas.com/promotions/cases/bluetooth-low-energy-1.html

The following is another sample application implementing the advertising packet broadcast function. This sample takes advantage of Bluetooth Low Energy in a sensing device. The beacon device is placed in the front entrance of a home, allowing the user to detect break-ins as well as remotely control household appliances. The application achieves home automation, eliminating the need for a remote controller or human intervention.

Bluetooth Low Energy is a low-power consumption standard. This means Bluetooth Low Energy devices can send advertising packets using very little energy. In the example shown below, energy harvested by stepping on a special floor mat can be used to send beacons (advertising packets). The mat boasts semi-permanent operations without battery

replacement. Radio waves from the beacon are received by a security/access panel. From there, the user can control lighting while informing other family members via the cloud. This application is also useful as protection from break-ins and to keep a watchful eye on elderly family members.



Sample Sensing Device Application

In this manner, a customized beacon stack can be prepared for beacon devices that integrate applications utilizing the advertising packet broadcasting function. This beacon stack enables broadcasting (sending) and receiving (scanning) advertising packets used by the beacon device without employing all the Bluetooth Low Energy functions.

As the beacon stack has limited functions, the program features a simple configuration and small size. This means users can compile programs using the build function in the evaluation version. Start up and operations are both carried out with low power consumption.

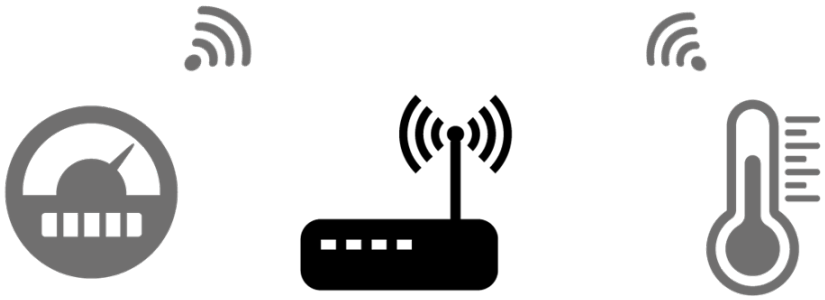
Now let's look at an application that uses data transferred after connection to a Bluetooth Low Energy device. The smartphone in this example supports the Bluetooth Low Energy specification, which is used for easy data collection using a low-power wireless interface. Most healthcare-related equipment can be wirelessly connected to a smartphone, benefiting from Bluetooth Low Energy functions. As the example shows, a wide range of measurement and sensing devices, such as a heart rate monitor, blood pressure monitor, and bathroom

scale, can be used with the Bluetooth Low Energy ready smartphone.

Smartphone Connection Example

Data communication based on Bluetooth Low Energy device connections can also be used to transmit data between devices, as shown in the example below.

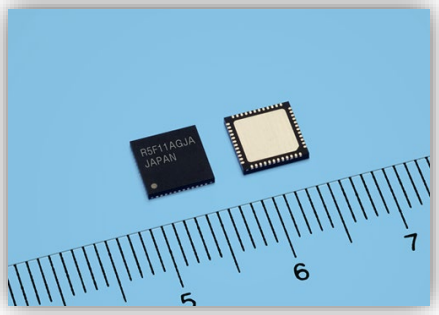
Bluetooth Low Energy sensors can be used to store data in the Cloud via a Bluetooth Low Energy and LTE/3G gateway (bridge), thanks to the minimal amount of power used in Bluetooth Low Energy transmissions. Bluetooth Low Energy is used for data transfer by the sensor end device, with the device on the other end of the gateway (bridge) based on wireless standards for long-distance transmission.



Examples of Wireless Device Connections

As shown here, the Bluetooth Low Energy MCUs can be used in two key ways: applications implementing the advertising packet broadcast function and applications using data transferred after connection to a Bluetooth Low Energy device. Therefore, Renesas offers two types of software stacks: Bluetooth low energy protocol stack and beacon stack. The user can select the stack based on the target usage.

In addition, Renesas offers both IC and module products certified under Bluetooth 4.2. Whether needed in mass production, for the development period, or with/without RF technology, Renesas has the IC or module to meet all application needs.



RL78/G1D (R5F11A)

RL78/G1D Module (RY0711)

Find Renesas Electronics' Bluetooth® Low Energy solutions at the following link.
https://www.renesas.com/solutions/bluetooth