Understanding security features of SimpleLink™ *Bluetooth*® Low Energy CC13x2 and CC26x2 wireless MCUs

Texas Instruments

Security problem targeted: Typical threats / security measures

The **SimpleLink™ CC2640R2F wireless MCU** is enabling any developer in the industry to connect an application to a smart device using *Bluetooth*® low energy wireless technology. Optimized for Internet of Things (IoT) applications, it delivers the longest distance for the lowest power. When designing for applications ranging from building automation (door lock, beacons), medical health (non-life critical applications like blood glucose meter, patient monitoring), appliances and automotive (key fobs and telematics), developers need to implement security measures to maintain data privacy and connect to only trusted sources.

TI's SimpleLink CC2640R2F wireless MCU running Bluetooth 4.2 and higher, offers significantly improved security and privacy over first-generation Bluetooth low energy devices allowing developers to build devices that can enter secure connections without being intercepted or tracked by untrusted observers (scanners). The SimpleLink Bluetooth software development kit (SDK) leverages the CC2640R2F device's hardware AES accelerator and ECC code running from ROM which helps developers implement their security measures while maintaining ultra-low power consumption.

Device/Family description

The SimpleLink Bluetooth low energy CC2640R2F device is a wireless microcontroller (MCU) targeting Bluetooth 5 (and supporting Bluetooth 4.2 / 4.1 / 4.0 features) for single-mode Bluetooth low energy applications. It is part of the **SimpleLink MCU platform**.

TI Embedded Security Portfolio –

Security is hard, TI makes it easier

Security features details

The SimpleLink CC26xx platform offers a highly efficient AES encryption hardware module, security crypto library in ROM (Elliptic Curve), a true random number generator (TRNG) as well as low-power digital signal processing. These features are important tools to enable designers to create the appropriate level of security for their products. In addition to being used by the Bluetooth protocol stack, these security features are also accessible to the application developer to implement their own application-level security. There are two independent security upgrades that come with Bluetooth 4.2 and newer specifications: **Secure Connections (Pairing)** and **Privacy**.

- **Strong encryption** – Securely encrypting the packets transmitted between two devices in a connection is quite straightforward as long as they both share a secret key. AES in CCM mode is the encryption technique used in many standards like Bluetooth, zigbee® and IEEE 802.15.4 for Link Layer / MAC. This is supported by the AES hardware accelrator included in the CC2640R2F / CC2640R2F-Q1 / CC2640 wireless MCUs for key sizes up to 128 bits.

Security enablers:

Device	Security enablers	Detailed security features
CC2640R2F / CC2640R2F-Q1 / CC2640	Cryptographic acceleration	AES-128, TRNG, Elliptic Curve Cryptographic (ECC) library in ROM
	Debug security/ Software IP protection	Locking debug interfaces maintaining firmware confidentiality and integrity
	Device identity	Unique and immutable die ID and Bluetooth address

TI offers security enablers to help developers implement their security measures to protect their assets (data, code, identity and keys).

- **Secure key exchange (pairing)** – Solutions with shared keys are widely used today, however, this technique does not provide a way for two devices that are being paired (associated) by their owner to exchange a secret key that cannot be read by passive eavesdroppers several meters away. Many standards are either looking at or have already enhanced the security by implementing a better key-exchanging scheme. This is the big improvement in Bluetooth 4.2, where the Elliptic Curve Diffie-Hellman (ECDH) key agreement protocol is introduced with the LE Secure Connections pairing feature. ECDH is today's IoT industry standard for Key Agreement schemes, and allows two parties with no previously shared information to establish a secret key that is known to them only and never shared over the air. The Elliptic Curve Cryptographic (ECC) algorithm is implemented in ROM on board the CC2640R2F / CC2640R2F-Q1 / CC2640 wireless MCUs to leave as much Flash memory as possible available for the application. The use of ECC, combined with the random number generation capability of the hardware-based TRNG ensures that the key is generated in a way that makes it highly resistant to brute-force key attacks.
- **Improving privacy (Bluetooth 4.2 and future standard version)** – In order to enable pairing with new devices, Bluetooth low energy peripherals will send out connectable advertisement broadcasts at regular intervals. The advertisements contain the peripheral device's Bluetooth device address (BD address), and this makes it very simple to track the presence of peripheral devices by passive scanning (observing). Since more and more of these peripherals are constantly worn by their owners, it is effectively the owner who is tracked, and not just the peripheral. For retail chains, this can help them analyze how customers move around in their stores, or even between stores. This collection and use of "analytics" information is in most cases harmless, but the ease with which this type of tracking can be set up means that there are many organizations that will be capable of doing it, as they need not be particularly resourceful or technologically advanced.

  The problem is solved with the privacy enhancements in Bluetooth 4.2, and the solution is quite simple; the Bluetooth peripheral devices regularly choose a new, and what appears to be, random BD address to use in their advertisements. The random address is in fact derived from a cryptographic function and changes on a periodic basis, typically every 15 minutes. Only after an encrypted connection is set up with a trusted Master, is the peripheral device's real BD address disclosed along with an identity resolving key (IRK) which can be used by the peer device to decode or "resolve" the seemingly random address back to the device's public address. Untrusted devices who do not have the IRK wanting to track advertising peripherals will have no way of resolving the real BD address based on the randomly chosen advertising address, and tracking the random address will only last until the device choses a new one.
- **Effective processing** – In addition to a 128-bit AES encryption hardware module, the CC2640R2F / CC2640R2F-Q1 / CC2640 wireless MCUs contain a highly efficient ARM® Cortex®-M3 CPU with an active current consumption at 61 µA/MHz at 3.0 V. This enables low power and fast software solution for existing and future security enhancements and standards.

Additional resources

Blog: How Bluetooth 4.2 can help enable product security

Security is hard, TI makes it easier

For more information about TI's Embedded Security Solutions, visit **www.ti.com/security**

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATASHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES “AS IS” AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for skilled developers designing with TI products. You are solely responsible for (1) selecting the appropriate TI products for your application, (2) designing, validating and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, or other requirements. These resources are subject to change without notice. TI grants you permission to use these resources only for development of an application that uses the TI products described in the resource. Other reproduction and display of these resources is prohibited. No license is granted to any other TI intellectual property right or to any third party intellectual property right. TI disclaims responsibility for, and you will fully indemnify TI and its representatives against, any claims, damages, costs, losses, and liabilities arising out of your use of these resources.

TI’s products are provided subject to TI’s Terms of Sale (www.ti.com/legal/termsofsale.html) or other applicable terms available either on ti.com or provided in conjunction with such TI products. TI’s provision of these resources does not expand or otherwise alter TI’s applicable warranties or warranty disclaimers for TI products.

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265