Understanding Security Features of SimpleLink™ *Bluetooth*® Low Energy CC13x2 and CC26x2 Wireless MCUs

Device/family description

The SimpleLink CC13x2 and CC26x2 family of wireless microcontrollers (MCUs) target Bluetooth 5 Low Energy, Zigbee, Thread and proprietary Sub-1 GHz and 2.4-GHz systems to easily enable the addition of mobile device connectivity to Internet of Things designs while achieving ultra-low power consumption. These highly integrated system-on-chips include an ARM® Cortex®-M4F central processing unit, an ultra-low-power flexible radio and a programmable sensor controller core. Optimized for embedded low-power wireless applications, these devices deliver the longest distance for the lowest power. They are supported by the SimpleLink software development kit (SDK) for CC13x2 and CC26x2 devices and the free Code Composer Studio™ integrated development environment.

This document will describe the CC2642R; however, the same features and functionality apply to all Bluetooth Low Energy-enabled SimpleLink CC13x2 and CC26x2 wireless MCUs.

Interested in developing your next product with these advanced security features? See ti.com/ble for design and development resources including development kits, SimpleLink software and software development tools.

Security problem targeted: Typical threats / security measures

The SimpleLink™ CC2642R wireless MCU enables the connection of an application to a smart device or to low-power infrastructure networks using Bluetooth Low Energy wireless technology. When designing for applications ranging from building automation (door locks, security sensors and asset-tracking beacons), medical health (non-life-critical applications like blood glucose meters and patient monitoring), and appliances and factory automation (device configuration, condition monitoring and asset management), you need to implement security measures to maintain communication data privacy and connect to only trusted sources.

TI's SimpleLink CC2642R wireless MCU running Bluetooth 5 (which is backwards-compatible with peer devices running Bluetooth 4.2 and earlier Bluetooth Low Energy specifications) helps you build devices that can enter secure connections with security measures towards being intercepted or tracked by untrusted observers (scanners). The Bluetooth 5 protocol stack component in the SimpleLink SDK leverages the CC2642R device's hardware Advanced Encryption Standard (AES) accelerator and elliptic-curve cryptography (ECC) public key accelerator (PKA) to facilitate the implementation of network security measures with energy and performance optimizations.

The network-connected applications support device firmware updates over the air (OTA) in the field. It is very important that the devices only update/program firmware images coming from valid, trusted parties, and furthermore, only execute valid firmware on-chip. The SimpleLink SDK's integrated boot image manager (BIM) software component implements an increased security OTA solution that verifies the authenticity of a new firmware image – received and stored on-chip or off-chip – before programming it onto on-chip application memory. The BIM software, along with the device's hardware security features, also support a secure boot functionality that verifies the firmware's authenticity on-chip upon every device reset.

Security features details

The CC2642R wireless MCU offers multiple security enablers to help mitigate security risks. **Table 1** lists the security enablers offered in SimpleLink™ CC13x2 and CC26x2 hardware and software to enable you to design your products with increased security.

- **Device identity** – Each device is programmed with a 128-bit unique device identifier at TI production

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

programming. This identifier is stored as a read-only factory configuration information block that is accessible by the application software. In addition, TI assigns each CC2642R device with a unique 48-bit Institute of Electrical and Electronics Engineers (IEEE) assigned Bluetooth address.

- **Debug security** – Debug security enables locking debug access to the device. When locked, the debug lock configuration can only be reset with a factory reset (mass erase) process that erases all user-accessible internal flash memory contents and then resets the device security configuration settings to the chip-default values that enable device debug access. The factory reset is only achievable with local Joint Test Action Group (JTAG) access. The factory reset process itself can be optionally disabled, thus preserving the configured debugging security settings from alterations by JTAG.
- **Cryptographic accelerators** – An energy- and performance-optimized AES encryption hardware accelerator, a PKA and a true random number generator (TRNG) are fundamental security enablers that you can use to implement the appropriate security solutions for your products. In addition to their use by the Bluetooth protocol stack, these accelerators are also accessible to the application developers for implementing their own application-level security for end-to-end point protection.
- **Network security** – As part of Bluetooth 4.2 and later specifications, the secure connections (pairing) and privacy features are supported.
- **Link layer encryption** – The AES CCM accelerator on-chip (128-bit key size) is used by CC2642R device's link/media access control layer to perform authenticated encryption of the packet data units transmitted between two devices in a Bluetooth Low Energy connection when using the encryption feature. Additionally, the Bluetooth Low Energy ping feature (introduced in Bluetooth 4.1) enables the encryption of ping requests between peers. This way, a local attacker who does not possess the valid link layer encryption key is unable to respond to the ping request, thus helping prevent "spoofing" attacks.
- **Secure key exchange (pairing)** – As part of the Bluetooth Low Energy secure connections pairing feature (introduced in Bluetooth 4.2), the ECDH key agreement protocol is supported in order to securely derive session keys used for link layer encryption during Bluetooth Low Energy connections. ECDH allows two parties with no previously shared information to establish a secret long-term key that is known only to them without exchanging any secrets during the pairing process. This enables the Bluetooth Low Energy secure connections pairing protocol to be increasingly

Security enablers:

Device	Security enablers	Detailed security features
CC2642R CC1352R CC1352P CC2652R	Device identity	128-bit unique device identifier, 48-bit IEEE assigned Bluetooth device address.
	Debug security	Permanent debug lock. Device factory reset disables debug security.
	Cryptographic acceleration	• AES hardware accelerator: - 128-, 192- and 256-bit keys. - Electronic Codebook Mode (ECB), Cipher Blockchain Mode (CBC), Cipher Block Chaining Message-Authentication Code (CBC-MAC), Counter Mode (CTR), Counter with CBC-MAC (CCM) and Galois/Counter Mode (GCM). • Secure Hash Algorithm (SHA)-2 (SHA-224, SHA-384, SHA-256, SHA-512). • PKA: -Elliptic curves up to 521 bits (National Institute of Standards and Technology [NIST] P, Brainpool, Curve25519, elliptic curve Diffie-Hellman [ECDH]). -Rivest-Shamir-Adleman (RSA), up to 2,048-bit key support. • TRNG (true random number generator).
	Software intellectual property protection	Flash memory region read-only protection.
	Secure boot	BIM software in conjunction with device hardware security features including flash memory protection, controlled read-only memory (ROM) boot exit and cryptographic acceleration. The BIM software is available as part of the SimpleLink SDK.
	Secure OTA download (OAD)	BIM software using device cryptographic algorithms for firmware image validation is available as part of the SimpleLink CC13x2 and CC26x2 SDK.
	Network security	The Bluetooth 5 protocol stack, available as part of the SimpleLink SDK, supports Bluetooth 5 with Bluetooth Low Energy secure connections (pairing) using device cryptographic acceleration. Cryptographic accelerators are also accessible to application developers who wish to implement their own application-level security for end-to-end point protection.

Table 1: SimpleLink™ Bluetooth® Low Energy CC13x2 and CC26x2 Wireless MCUs Security Enablers.
Note: This set of security enablers (including network security) are applicable to all CC26x2 and CC13x2 devices.

resistant to eavesdropping attacks during key exchange in the local wireless network.

The Bluetooth 5 protocol stack for CC2642R devices complies with the Bluetooth Low Energy secure connections pairing by using the on-chip PKA for ECDH key exchange, combined with random number generation using the hardware TRNG. Additionally, the Bluetooth 5 protocol stack also supports device authentication mechanisms, including passkey entry and numeric comparison (introduced in Bluetooth 4.2). These mechanisms can help developers mitigate local man-in-the-middle attacks, where an attacker pretends to be the valid party with which the device is pairing.

- **Enhanced privacy protection (Bluetooth 4.2 and later versions)** – Advertising the Bluetooth Low Energy peripheral device's Bluetooth device address regularly makes it easy to track the presence and locations of peripheral devices by simple passive scanning (observing). Since more of these peripherals are worn constantly by their owners, it is effectively the owner who is tracked. Bluetooth privacy protection requires that Bluetooth devices regularly choose a new and random Bluetooth device address for use in their advertisements. The random address is derived from a cryptographic function and changes periodically (typically every 15 minutes). Only after an encrypted connection is set up with a trusted peer device will the peripheral device's real address be disclosed, along with an identity resolving key (IRK) that the trusted peer device uses to decode the seemingly random address back to the device's public address. Untrusted devices (without the IRK) wanting to track advertising peripherals will not be able to resolve the real Bluetooth device address based on the randomly chosen advertising address, and tracking the random address will only last until the device chooses a new Bluetooth device address. The Bluetooth 5 stack for CC2652 devices supports this enhanced privacy protection.
- **Secure boot** – Secure boot verifies the integrity and authenticity of the firmware to be executed on the device upon every boot. The BIM software component is a bare-metal microapplication available as part of the SimpleLink SDK that handles this boot-time verification before transferring execution to the main firmware image. The BIM uses secure hash (SHA-2) and asymmetric cryptographic algorithms (ECDSA) to implement the secure boot verification process. The flash memory region read-only protection can help maintain the integrity of the BIM software and associated public key used for firmware image verification, thus making the secure boot verification code and key immutable in on-chip flash. Additionally, the controlled exit from the device ROM boot execution to always execute the BIM secure boot software upon any device reset enables root-of-trust secure boot implementation on the CC2642R wireless MCU.
- **Secure OAD** – Secure OAD verifies the integrity and authenticity of a new firmware image to be programmed onto the device's on-chip flash. The BIM software available as part of the SimpleLink SDK handles the new firmware image verification in addition to the secure boot functionality described above. Upon device reset, the BIM software checks if a new signed firmware image (stored in an on-chip partition or off-chip serial flash) is available. If a new firmware image exists, the BIM uses secure hash and asymmetric cryptographic algorithms to validate the new image. Once successfully validated, the BIM replaces the active firmware image with the new image. Finally, a secure boot validation check is performed on the newly programmed image to protect against local attackers who may have replaced the image during copying from external to internal flash memory.

Additional resources

- Learn more about TI's embedded security.
- Read the blog post, "How Bluetooth 4.2 can help enable product security."
- Learn more about TI's Bluetooth Low Energy solutions.
- Read "Secure Boot in SimpleLink™ CC13x2/CC26x2 Wireless MCUs."

Security is hard, TI makes it easier

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

Important Notice: The products and services of Texas Instruments Incorporated and its subsidiaries described herein are sold subject to TI's standard terms and conditions of sale. Customers are advised to obtain the most current and complete information about TI products and services before placing orders. TI assumes no liability for applications assistance, customer's applications or product designs, software performance, or infringement of patents. The publication of information regarding any other company's products or services does not constitute TI's approval, warranty or endorsement thereof.

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