Understanding Security Features for SimpleLink™ Zigbee CC13x2 and CC26x2 Wireless MCUs

Texas Instruments

Device/family description

The SimpleLink CC13x2 and CC26x2 family of wireless microcontrollers (MCUs) target Bluetooth® Low Energy, Zigbee, Thread and proprietary Sub-1 GHz and 2.4-GHz systems. CC1352 and CC2652 MCUs support Zigbee networks, with some devices offering dual-band Sub-1 GHz and 2.4-GHz connectivity. These highly integrated wireless MCUs enable the implementation of a self-healing mesh network of wireless nodes while maintaining ultra-low power consumption.

The devices include an ARM® Cortex®-M4F central processing unit, an ultra-low-power flexible radio, and a programmable sensor controller core for low-power data acquisition and processing. Part of the SimpleLink platform, the CC1352R, CC1352P, and CC2652R are supported by the SimpleLink software development kit (SDK) and the free Code Composer Studio™ integrated development environment.

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

Security problem targeted: Typical threats / security measures

SimpleLink CC1352 and CC2652 wireless MCUs enable you to add robust mesh network connectivity to your applications using Zigbee wireless technology. When designing for applications ranging from building automation (lighting, security systems, thermostats and electronic locks) to smart metering (water, gas and flow metering), you need to implement security measures to maintain communication data privacy and connect only to trusted sources.

TI's SimpleLink CC1352 and CC2652 wireless MCUs running the SimpleLink SDK help you design devices that can join secure Zigbee networks without being intercepted or tracked by undesirable sources. The SimpleLink SDK leverages the CC1352 and CC2652 devices' hardware Advanced Encryption Standard (AES) accelerator and true random number generator (TRNG), which help you implement network security measures with energy and performance optimizations.

Security features details

CC1352 and CC2652 wireless MCUs offer 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 during TI production programming. This identifier is stored as a read-only factory configuration accessible by the application software.
- **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 process that erases all user application firmware and security settings on-chip before enabling device debug access. The factory reset is only accessible with local Joint Test Action Group access.
- **Cryptographic accelerators** – An AES encryption hardware accelerator, a public key accelerator (PKA) and TRNG are fundamental security enablers that you can use to implement the appropriate security solutions for your products. These accelerators are accessible to application developers for implementing application-level security for end-to-end point protection.
- **Network security** – Per the Zigbee PRO 2017 specification, the

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

AES-128 CCM accelerator is used for network and application support sublayer (APS) encryption policies. For each individual packet, devices may specify the use of encryption at the network layer, the APS layer, neither or both, depending on the required security policy for that specific data.

- **Link layer encryption** – To comply with the Institute of Electrical and Electronics Engineers (IEEE) 802.15.4 specification, the AES CCM accelerator (128-bit key size) is used by the device link layer to perform authenticated encryption of the packets transmitted between devices. Unicast communications can be secured by a 128-bit APS link key shared between two devices, while broadcast communications and any network layer communications can be secured by a 128-bit network key shared among all devices.
- **Secure key transport** – The Zigbee PRO Specification defines certain measures that can help mitigate eavesdropping during network provisioning. The trust center in the network (as specified in the Zigbee PRO Specification) is required to enable permit joining mode, for a node to join the network. With in-network entities controlling when and how long the trust center enters permit join, this process increases deterrence of spoofing and device impersonation attacks.

  Zigbee 3.0, which is built on top of Zigbee PRO, offers the option to use preconfigured APS keys and install code-derived APS keys in order to implement network key exchanges. Install codes are 128 bits of randomly generated data and a 16-bit cyclic redundancy check (CRC) that pass through a hash function (Matyas-Meyer-Oseas (MMO)) using the AES encryption engine to generate the APS link key. Rather than using the well-known APS link key (specified in the Zigbee standard), Zigbee 3.0 enables the generation of these APS link keys with install codes. This method avoids the use of global link keys for over-the-air encryption, thereby helping potentially protect the network from a range of vulnerabilities.
- **Network Frame Counter** – Zigbee Pro 2017 requires that devices keep the outgoing network frame counters persistent across device resets. Frame counters can be used as protection against potential replay attacks. If an incoming packet has a frame counter value less than or equal to what was saved in the non-volatile memory, then security processing should fail and no further packet handling should take place. Neighbor devices on a network have a neighbor table entry for the network frame counter value that a device had when it was last on the network. If a device joins a network for a second time with new security material and an outgoing network frame counter of zero, the devices in that network will reject those frames as a security measure.

Security enablers:

Device	Security enablers	Detailed security features
CC1352P CC1352R CC2652R	Device identity	128-bit unique device identifier, Bluetooth Low Energy device identifier (if Bluetooth Low Energy is supported).
	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	Boot image manager (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 CC13x2 and CC26x2 SDK.
	Network security	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.*
This set of security enablers (including network security) are applicable to all CC26x2 and CC13x2 devices, although only the CC1352 and CC2652 devices in this family support Zigbee

Additional resources

- Read the blog post, "The 'key' to security: Zigbee 3.0's security features."
- Learn more about TI's embedded security.
- Order the SimpleLink CC13x2-CC26x2 SDK.
- Learn more about SimpleLink Zigbee wireless MCUs.
- 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 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