Understanding Security Features for SimpleLink[™] Sub-1 GHz CC13x2 MCUs

TEXAS INSTRUMENTS

Device/family description

The SimpleLink CC13x2/CC26x2 wireless microcontrollers (MCUs) are a family of devices targeting Bluetooth® Low Energy, Zigbee, Thread, and proprietary (Sub-1 GHz and 2.4 GHz) systems. The CC13x2 MCUs support Sub-1 GHz networks, with some devices offering dual-band (Sub-1 GHz and 2.4 GHz) connectivity. These wireless MCUs enable the addition of long range connectivity to your design while maintaining ultra-low power consumption. These highly integrated CC13x2 Systems-on-Chips (SoCs) include an ARM® Cortex ® -M4F MCU, ultra-low power flexible radio, and programmable sensor controller core for low power sensor acquisition and processing. The CC13x2 devices are a part of the SimpleLink[™] platform and are supported by the SimpleLink SDK.

While there is no central standard for Sub-1 GHz star network solutions. Texas Instruments offers an out-of-box network solution to simplify development and lower final product time to market for customers. Based on the IEEE 802.15.4 standard and FCC/ETSI certification-ready, the TI 15.4-Stack is a network solution for implementing low power, long range wireless networks in the home, building, or city. The 15.4-Stack supports data rates ranging from 50 kbps, 200 kbps, to long range 5 kbps. This network implementation can support 200+ nodes, and frequency bands of 433 MHz, 863 MHz, and 915 MHz. The 15.4-Stack utilizes MAC layer acknowledgements, listen-beforetalk, and CMSA/CA in order to ensure successful packet transmissions. For more information on the TI 15.4-Stack visit TI.com/sub1ghz

Security problem targeted: Typical threats / security measures

The SimpleLink[™] CC13x2 wireless MCU is enabling developers in the industry to add long range star network connectivity to their application using Sub-1 GHz wireless technology. When designing for applications ranging from building automation (door locks, security systems, thermostats), metering (water, gas, and flow metering), medical health (non-life critical applications like blood glucose meter, patient monitoring), appliances and factory automation (device configuration, health status, asset tracking) developers need to implement security measures to maintain communication data privacy and connect to only trusted sources. TI's SimpleLink CC13x2 wireless MCUs running the TI 15.4-Stack Sub-1 GHz network solution allows developers to design devices that can enter secure Sub-1 GHz connections without being intercepted or tracked by unwanted interferers. The 15.4-Stack within the SimpleLink SDK leverages the CC13x2 devices' hardware AES accelerator and ECC public key accelerator (PKA) which helps developers implement network security measures with energy and performance optimizations.

Interested in developing your next product with these advanced security features? See <u>ti.com/sub-</u> <u>1ghz</u> for design and development resources including development kits, SimpleLink software and software development tools.

Security features details

The CC13x2 wireless MCUs offer multiple security enablers to help developers design products with increased security to mitigate security risks in their system. This includes:

- Device identity involves each device programmed with a 128-bit unique device identifier at TI production programming. This identifier is stored as a read-only factory configuration information.
- Debug security enables locking debug access to device permanently. 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 the device debug access. The factory reset is only accessible with the local JTAG access.

The SimpleLink CC13x2 family of devices offers energy and performance optimized AES encryption hardware accelerator, a public key accelerator (PKA), a true random number generator (TRNG). These *cryptographic accelerators* are

fundamental security enablers that enable developers to implement appropriate security solutions for their products. These accelerators are accessible to the application developer and can enable them to implement their own applicationlevel security for end-to-end point protection.

Network Security

The TI 15.4 stack has several security attributes to deter a variety of network communication threats.

Secure key exchange (pairing) –

During device provisioning process (when a sensor node is provisioned onto the sub-1 GHz star network), in order to increase security against passive eavesdropping attacks, secure exchange of encryption keys between the collector and sensor node is supported. The TI 15.4-Stack uses Elliptic Curve Diffie-Hellman (ECDH)-based cryptographic function to allow two parties, each having an elliptic curve public-private key pair, to establish a shared secret over an insecure channel. The shared secret is used to further derive the device link key (secret key) that is unique to the collector and sensor node pair. This way, ECDH allows two parties with no previously shared information to establish a secret encryption key that is known only to them and the

secret key derived is never shared in plaintext over the air. The device link key is subsequently used for encrypted communications between the sensor node and collector.

Key derivation for deriving the device link key is based on AES-CMAC and TRNG. FIPS-approved cryptographic algorithms for key exchange and key derivation are used. TI 15.4-Stack also provides hooks for device link key refreshments that are triggered by application inputs.

 Device authentication – During device provisioning, TI 15.4 stack and application supports using passkey entry or default code mechanisms for authenticating the network connections, there by mitigating the risks of man-in-themiddle (MITM) attacks. If using passkey entry based authentication, the connecting devices are required to be provided with a passkey, which should match with that of the passkey that is also provided to the collector side during the device provisioning phase. If using default code, a user-configurable code should be pre-installed on every device before joining the network and this should match with the preinstalled code on the collector side as well for the authentication to succeed. The code used for authentication during device provisioning, either the default or the passkey, is never revealed over the wireless communication.

 Link layer encryption – On-chip AES CCM accelerator (with key sizes up to 128 bits) encrypts packets in link/MAC layer transmitted between two devices in a Sub-1 GHz star network using the device link key (derived with the ECDH key exchange during provisioning phase). For broadcast communications, a collector encrypts broadcast messages with a preconfigured network key. All the sensor nodes in the network use the same network key to decrypt the broadcast messages.

Device	Security enablers	Detailed security features
CC1312R CC1352R CC1352P	Device identity	128-bit unique device identifier, BLE device identifier (if BLE 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 HW security features including flash memory protection, controlled ROM boot exit and cryptographic acceleration. The BIM software is available as part of CC2642R SDK.
	Secure OTA download (OAD)	Boot Image Manager (BIM) software library using device cryptographic acceleration for FW image validation is available as part of CC13x2 SDK.
	Network security	About the 15.4-Stack. The cryptographic accelerators are also accessible to the application developer to implement their own application- level security for end-to-end point protection.

Table 1: These set of security enablers (including network security) are applicable to all CC26x2 and CC13x2 devices, although only CC13x2 devices operate in the Sub-1 GHz band.

Security enablers:

• Secure boot - verifies the authenticity of the firmware to be executed on the device upon every boot. The boot image manager (BIM) software library available as part of the SimpleLink CC13x2-CC26x2 SDK handles this boot time verification. The BIM uses the on-chip hash and asymmetric cryptographic accelerators to speed up the secure boot verification process. The flash memory region read-only protection is used to maintain the integrity of the BIM software and the public key used for verification; thus making the secure boot verification code and key increasingly immutable on-chip. Additionally, the controlled exit from the device ROM boot execution to always execute the BIM secure boot software enables the secure boot functionality on the CC13x2 wireless devices.

Additional resources:

- Read "Secure Boot in SimpleLink™ CC13x2/CC26x2 Wireless MCUs"
- Explore TI's full security enablers
- Learn more about Sub-1 GHz solutions from TI
- Learn about TI Sub-1 GHz
 15.4-Stack Modes

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.

The platform bar is a trademarks of Texas Instruments. All other trademarks are the property of their respective owners.



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 Copyright © 2019, Texas Instruments Incorporated