Understanding security features for SimpleLink™ Sub-1 GHz CC13x0 MCUs

Texas Instruments

Device/Family description

The SimpleLink™ Sub-1 GHz CC13xx wireless microcontroller (MCU) family is a part of the **SimpleLink MCU portfolio**, offering both the ultra-low power Sub-1 GHz CC1310 device and the dual-band (Sub-1 GHz + *Bluetooth*® low energy) CC1350 device. These wireless MCUs easily add ultra-low power and long-range connectivity to your Internet of Things (IoT) designs. Additionally, the dual-band capability of the CC1350 device allows for over-the-air updates, smart commissioning, beaconing, remote display and proximity detection directly from your smartphone, while achieving long range and multi-year battery operation. This highly integrated single-chip family includes an ARM® Cortex®-M3 MCU, ultra-low power radio and sensor controller, all in a tiny 4 mm-by-4 mm package.

TI Embedded Security Portfolio –

Security is hard, TI makes it easier

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

Security problem targeted: Typical threats / security measures

The **SimpleLink Sub-1 GHz CC13xx wireless MCUs** enable developers to design a wide range of industrial end equipments primarily in the building automation and grid infrastructure sectors. The SimpleLink CC13xx portfolio and SimpleLink CC13xx SDK allow designers to develop Sub-1 GHz solutions or add Sub-1 GHz to legacy IoT designs at a level of ease like never before, leading to an expanding market of devices with Sub-1 GHz connectivity. While this expansion in the IoT space opens up many new end application possibilities, it also opens up a wide range of security threats to these network-connected devices, specifically within building automation where Sub-1 GHz solutions are often used for security and safety systems (i.e., motion detectors, smoke/fire detectors, glass break detectors and door/window sensors).

One prominent threat to security in these systems is sensitive user data being transmitted over a Sub-1 GHz network. This data can be intercepted and manipulated by third parties causing a liability to these networks and increasing the danger to sensitive user data and end-user safety.

Realizing these threats, TI designed the CC13xx platform with a variety of security enablers to address these security concerns.

Security features details

The CC13xx portfolio offers a highly efficient AES encryption hardware module, security crypto library in ROM (Elliptic Curve + SHA2), 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.

- **Secure pairing/joining** – 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 802.15.4e. This is supported by the AES hardware accelerator included in the CC1310/CC1350 wireless MCUs. **TI 15.4-Stack** is a star network protocol designed for the CC13xx family. As a part of the solution, AES encryption with shared keys is implemented as a part of the IEEE 802.15.4e security standard for the MAC layer.
- **Secure key exchange** – Solutions with shared keys are widely used today, however, this technique

Security enablers:

Device	Security enablers	Detailed security features
CC1310 / CC1350	Cryptographic acceleration	128-bit AES hardware accelerator True random number generator (TRNG) Elliptic Curve Cryptographic (ECC) algorithm, SHA256
	Device identity	Unique die ID
	Debug security / Software IP protection	Locking debug interfaces maintaining firmware confidentiality

does not provide a way for two devices that are being paired 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 for example Bluetooth 4.2, where the Elliptic Curve Diffie-Hellman (ECDH) key agreement protocol is introduced. ECDH is today's gold standard in key-agreement schemes and allows two parties with no previously shared information to establish a secret key that is known to them only. The Elliptic Curve Cryptographic (ECC) algorithm is implemented in ROM on board the CC13x0 wireless MCU to leave as much Flash memory as possible available for the application.

- **Effective processing** – In addition to a 128-bit AES encryption hardware module, the CC1310 / CC1350 devices contain a highly efficient ARM Cortex-M3 with an active current consumption at 51 µA/MHz (at 3.6 V, 48 MHz). This enables a low power and fast software solution for existing and future security enhancements and standards.

Additional resources

- **CC1310 product page**
- **CC1350 product page**
- **SimpleLink CC13x0 SDK**
- **End equipment information**
- **Full Sub-1 GHz portfolio**

Security is hard, TI makes it easier

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

IMPORTANT NOTICE FOR TI DESIGN INFORMATION AND RESOURCES

Texas Instruments Incorporated ('TI") technical, application or other design advice, services or information, including, but not limited to, reference designs and materials relating to evaluation modules, (collectively, "TI Resources") are intended to assist designers who are developing applications that incorporate TI products; by downloading, accessing or using any particular TI Resource in any way, you (individually or, if you are acting on behalf of a company, your company) agree to use it solely for this purpose and subject to the terms of this Notice.

TI's provision of TI Resources does not expand or otherwise alter TI's applicable published warranties or warranty disclaimers for TI products, and no additional obligations or liabilities arise from TI providing such TI Resources. TI reserves the right to make corrections, enhancements, improvements and other changes to its TI Resources.

You understand and agree that you remain responsible for using your independent analysis, evaluation and judgment in designing your applications and that you have full and exclusive responsibility to assure the safety of your applications and compliance of your applications (and of all TI products used in or for your applications) with all applicable regulations, laws and other applicable requirements. You represent that, with respect to your applications, you have all the necessary expertise to create and implement safeguards that (1) anticipate dangerous consequences of failures, (2) monitor failures and their consequences, and (3) lessen the likelihood of failures that might cause harm and take appropriate actions. You agree that prior to using or distributing any applications that include TI products, you will thoroughly test such applications and the functionality of such TI products as used in such applications. TI has not conducted any testing other than that specifically described in the published documentation for a particular TI Resource.

You are authorized to use, copy and modify any individual TI Resource only in connection with the development of applications that include the TI product(s) identified in such TI Resource. NO OTHER LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE TO ANY OTHER TI INTELLECTUAL PROPERTY RIGHT, AND NO LICENSE TO ANY TECHNOLOGY OR INTELLECTUAL PROPERTY RIGHT OF TI OR ANY THIRD PARTY IS GRANTED HEREIN, including but not limited to any patent right, copyright, mask work right, or other intellectual property right relating to any combination, machine, or process in which TI products or services are used. Information regarding or referencing third-party products or services does not constitute a license to use such products or services, or a warranty or endorsement thereof. Use of TI Resources may require a license from a third party under the patents or other intellectual property of the third party, or a license from TI under the patents or other intellectual property of TI.

TI RESOURCES ARE PROVIDED "AS IS" AND WITH ALL FAULTS. TI DISCLAIMS ALL OTHER WARRANTIES OR REPRESENTATIONS, EXPRESS OR IMPLIED, REGARDING TI RESOURCES OR USE THEREOF, INCLUDING BUT NOT LIMITED TO ACCURACY OR COMPLETENESS, TITLE, ANY EPIDEMIC FAILURE WARRANTY AND ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF ANY THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

TI SHALL NOT BE LIABLE FOR AND SHALL NOT DEFEND OR INDEMNIFY YOU AGAINST ANY CLAIM, INCLUDING BUT NOT LIMITED TO ANY INFRINGEMENT CLAIM THAT RELATES TO OR IS BASED ON ANY COMBINATION OF PRODUCTS EVEN IF DESCRIBED IN TI RESOURCES OR OTHERWISE. IN NO EVENT SHALL TI BE LIABLE FOR ANY ACTUAL, DIRECT, SPECIAL, COLLATERAL, INDIRECT, PUNITIVE, INCIDENTAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES IN CONNECTION WITH OR ARISING OUT OF TI RESOURCES OR USE THEREOF, AND REGARDLESS OF WHETHER TI HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

You agree to fully indemnify TI and its representatives against any damages, costs, losses, and/or liabilities arising out of your non-compliance with the terms and provisions of this Notice.

This Notice applies to TI Resources. Additional terms apply to the use and purchase of certain types of materials, TI products and services. These include; without limitation, TI's standard terms for semiconductor products http://www.ti.com/sc/docs/stdterms.htm), evaluation modules, and samples (http://www.ti.com/sc/docs/sampterms.htm).

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