

Understanding security features for SimpleLink™ MSP432P4xx MCUs



Device/Family description

The **SimpleLink™ MSP432™ (MSP432P4xx) microcontroller (MCU) family** includes ultra-low-power 32-bit ARM® Cortex®-M4F MCUs optimized for wireless host MCU operation with integrated 1-Msps SAR-based 14-bit analog-to-digital converter (ADC) and up to 256 kB of Flash and 64 kB of SRAM.



TI Embedded Security Portfolio –
Security is hard,
TI makes it easier

Security problem targeted: Typical threats / security measures

The SimpleLink MSP432 MCUs are optimized as wireless host MCUs that enable embedded developers to design a wide range of industrial-network-connected applications across different industrial markets including building automation, grid infrastructure, test & measurement and factory automation. MSP432 MCUs can be seamlessly interfaced with a wide range of SimpleLink wireless connectivity devices (including **CC1310**, **CC1350**, **CC2640R2F** and **CC3120** network processors) using the **SimpleLink MSP432 Software Development Kit (SDK)** and plug-ins.

Network connected devices may be subject to a wide range of security threats and the MSP432 MCUs aim at providing increased security for the critical security assets (code, data, keys) in these applications. Security is one of the primary concerns for

network-connected products and developers are often tasked with securing their overall system—including the network and the assets (both physical and digital). MSP432 MCUs offer a varied set of security enablers to help developers design an embedded solution with enhanced security to detect, protect and mitigate risks to their system.

Intellectual property (IP) theft including product cloning and manipulation has been a prominent threat to embedded systems. MSP432 MCUs offer security features that enable increased protection of software IP to help developers secure their trade secrets and avoid cloned software/products with inferior safety and reliability standards.

Security features details

MSP432 MCU security features coupled with its analog integration and ultra-low power operation enables embedded designers to address these aforementioned goals for the following security objectives:

Security enablers:

The MSP432P4xx MCUs offer a variety of security enablers, consisting of features embedded within the device hardware, programmed during device manufacture and implemented as part of the user's program code.

Device	Security enablers	Detailed security features
MSP432P401R MSP432P401M	Debug security	Permanent debug lock. Factory reset with optional password protection
	Cryptography acceleration	256-bit AES hardware accelerator true random number seed
	Software IP protection	Regional IP protection, debug lock
	Secure firmware and software update	Boot loader password protection encrypted firmware updates



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

- **Software IP protection** is a key care about for most embedded systems and in microcontroller systems, this correlates to protecting the software IP stored in embedded memories. MSP432 MCUs offer *debug security* to prevent unauthorized access to the device memory. Additionally, MSP432 MCUs support resetting device to default TI factory settings with options to permanently lock or password protect this feature. MSP432 MCUs offer software IP protection (IPP) feature that allows for incremental debug lock-out of up to four IP protected zones to provide regional security for IPs on-chip that is especially beneficial in multi-party software-development scenarios.
- **Secure data communication** in connected systems (remote or local) is essential to allow data to be communicated and encrypted between valid parties only. Cryptographic algorithms are primarily used to maintain confidentiality and integrity of the data in transit and to verify authenticity upon reception. MSP432 MCUs offer a powerful yet efficient hardware accelerator designed for AES encryption / decryption (128-, 192- and 256-bit key length). This

accelerator offers a greater than 40 times cycle reduction compared to regular C implementations. The MSP432 MCUs also typically include a true random number stored within the device memory that can be used as a seed for deterministic random number generation on-chip. Software crypto libraries for MSP432 MCUs for commonly used crypto algorithms like AES, DES, 3-DES and SHA-2 are also available.

- **Secure firmware updates** enable product developers to remotely update device firmware over the network with increased security. In most cases, this translates to mitigating risks against reverse-engineering of a new firmware image that is sent over the network and increasing device security by verifying firmware image integrity and authenticity before it's programmed onto the device. The MSP432 MCU's default bootloader supports an encrypted firmware update mechanism using the hardware AES accelerator on-chip. The pre-programmed bootloader requires a password to program new firmware image onto the MCUs. Additionally, MSP432 MCUs support encrypted firmware update wherein

the MSP432 MCU first decrypts the firmware image and verifies a password appended to the image payload before programming it onto the Flash memory.

Additional resources

- **MSP432 Security Training Module**
- **Configuring Security and Bootloader (BSL) on MSP432P4xx**
- **Secure In-Field Firmware Updates for MSP MCUs**
- **Software IP Protection on MSP432P4xx Microcontrollers Application Note**
- **MSP432 Security and Update Tool**
- **System-Level Tamper Protection Using MSP MCUs**
- **C Implementation of Cryptographic Algorithms**
- **SimpleLink MSP432 Software Development Kit (SDK)**
- **SimpleLink MSP432 SDK Bluetooth Plugin**
- **SimpleLink MSP432 SDK Wi-Fi Plugin**

Security is hard, TI makes it easier

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

The platform bar, MSP432 and SimpleLink are trademarks of Texas Instruments. All other trademarks are the property of their respective owners.

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/sampterm.htm) (<http://www.ti.com/sc/docs/sampterm.htm>).

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265
Copyright © 2017, Texas Instruments Incorporated