Understanding security features for SimpleLink™ MSP432P4xx MCUs

Texas Instruments

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**

Texas Instruments

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