Getting Started Guide
SLAU697 – December 2016

MSP432™ Security Overview

The security environment facing the embedded developer is a daunting one. New threats are constantly appearing that pose risks at various points in the product life cycle from development and manufacturing to secure operation and maintenance in the field. Defining security goals for an application in this environment requires multiple considerations including:

- The assets to be secured (code, keys, communication data, and so forth)
- The security attributes to be maintained (confidentiality, integrity, authenticity, and so forth)
- The threat access levels applicable to the system (remote access, local access)
- The Impact of a security failure for each function or aspect of design

In addition to the above concerns, other constraints must often be considered such as the security impact on cost, maintenance, and power. To assist in addressing these security goals, TI's MSP432 32-bit ARM® Cortex®-M4F microcontroller (MCU) platform offers a variety of security features, which may be embedded within the device hardware, programmed during device manufacture, or implemented as part of the users' program code.

Trademarks

MSP432 is a trademark of Texas Instruments.
ARM, Cortex are registered trademarks of ARM Limited.
All other trademarks are the property of their respective owners.

1 MSP432 Security Features

Table 1. MSP432 Security Features

Asset	Security Feature	Description	Learn More
Credentials	JTAG and SWD Lock	Assists in preventing unauthorized access to the device through the debug interface	For more information, see the JTAG and SWD Lock Based Security chapter in the *MSP432P4xx Technical Reference Manual*.
Data Communications	AES Accelerator	256-bit AES hardware accelerator assists in enabling secure communications without sacrificing performance or low power	For more information, see the *AES Accelerator* chapter in the *MSP432P4xx Technical Reference Manual*.
	Random Number Seed	Generate random keys using a 128-bit true random number programmed per device with a software PRNG (pseudo random number generator) or DRBG (deterministic random bit generator)	For more information, see the *MSP432P4xx Technical Reference Manual* and *MSP432P401R, MSP432P401M Mixed-Signal Microcontrollers*.
Software IP	IP Protection	Assists in enabling software IP to be isolated from the rest of your application through read, write, or execute-only permissions	For more information, see *Software IP Protection on MSP432P4xx MCUs* and the *MSP432™ Security and Update Tool*.
Device Firmware Update	Bootloader Password Protection	Password protected bootloader commands to increase security against unauthorized device access	For more information, see *Configuring Security and Bootloader (BSL) on MSP432P4xx*.
	Encrypted Firmware Updates	Can offer increased security against critical threats to field firmware update mechanisms with encryption and password based verification of new firmware image	For more information, see *Secure In-Field Firmware Updates for MSP MCUs*.

2 Security Features Description

- JTAG or SWD Lock (Secure Debug Access)

  MSP432 MCUs provide the means to secure debug access (JTAG or SWD) through user configuration to assist in enhancing system integrity and the confidentiality of software IP. When debug access is disabled, access to the device is possible using a bootloader.

- AES Accelerator and Random Number Seed

  MSP432 MCUs include a powerful yet efficient hardware accelerator designed for AES encryption and decryption (128-, 192-, and 256-bit key length) of communication data. This accelerator offers greater than 40 times cycle reduction compared to regular C implementations, which yields faster and lower-power crypto operations. Software crypto libraries for MSP432 MCUs for commonly used crypto algorithms like AES, DES, 3-DES, SHA-1, SHA-2 are also available. The MSP432 MCUs also include a random number stored within the memory of the device which can be used as a seed for a deterministic random number generator. This read-only random number is generated by a cryptographic random number generator and permanently programmed into the device during the manufacturing cycle of the device.

- Software IP Protection (IPP)

  Additionally, MSP432 MCUs offer an IP protection (IPP) feature that allows for incremental debug and code read lock-out of up to four IP protected zones to provide regional security for IPs on-chip. This feature can enable code confidentiality benefits in a host of multi-party software development scenarios.

- Encrypted Firmware Update Mechanism

  With Debug access disabled, the TI-provided bootloader requires a password to program new firmware. Additionally, MSP432 MCUs can enable an encrypted firmware update mechanism wherein the MCU decrypts and verifies a password in the new firmware image before programming it onto the Flash memory. When enabled properly, this feature can assist in preventing an outside party from either viewing the firmware or tampering with it.

  Furthermore, developers can leverage the bootloader infrastructure available on MSP432 MCUs to implement their own customized secure firmware update functionality. For more information, see *Configuring Security and Bootloader (BSL) on MSP432P4xx*.

3 References

- *MSP432P401R, MSP432P401M Mixed-Signal Microcontrollers*
- *MSP432P4xx Technical Reference Manual*
- *Software IP Protection on MSP432P4xx MCUs*
- *MSP432™ Security and Update Tool*
- *Configuring Security and Bootloader (BSL) on MSP432P4xx*
- *Secure In-Field Firmware Updates for MSP MCUs*
- *C Implementation of Cryptographic Algorithms*
- *System-Level Tamper Protection Using MSP MCUs*
- MSP Security Training Module

Products		**Applications**	
Audio	www.ti.com/audio	Automotive and Transportation	www.ti.com/automotive
Amplifiers	amplifier.ti.com	Communications and Telecom	www.ti.com/communications
Data Converters	dataconverter.ti.com	Computers and Peripherals	www.ti.com/computers
DLP® Products	www.dlp.com	Consumer Electronics	www.ti.com/consumer-apps
DSP	dsp.ti.com	Energy and Lighting	www.ti.com/energy
Clocks and Timers	www.ti.com/clocks	Industrial	www.ti.com/industrial
Interface	interface.ti.com	Medical	www.ti.com/medical
Logic	logic.ti.com	Security	www.ti.com/security
Power Mgmt	power.ti.com	Space, Avionics and Defense	www.ti.com/space-avionics-defense
Microcontrollers	microcontroller.ti.com	Video and Imaging	www.ti.com/video
RFID	www.ti-rfid.com		
OMAP Applications Processors	www.ti.com/omap	**TI E2E Community**	e2e.ti.com
Wireless Connectivity	www.ti.com/wirelessconnectivity		

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