

## **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 <a href="#">MSP432P4xx Technical Reference Manual</a> .
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 <a href="#">MSP432P4xx Technical Reference Manual</a> .
	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 <a href="#">MSP432P4xx Technical Reference Manual</a> and <a href="#">MSP432P401R, MSP432P401M Mixed-Signal Microcontrollers</a> .
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 <a href="#">Software IP Protection on MSP432P4xx MCUs</a> and the <a href="#">MSP432™ Security and Update Tool</a> .
Device Firmware Update	Bootloader Password Protection	Password protected bootloader commands to increase security against unauthorized device access	For more information, see <a href="#">Configuring Security and Bootloader (BSL) on MSP432P4xx</a> .
	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 <a href="#">Secure In-Field Firmware Updates for MSP MCUs</a> .

## 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](#)

## IMPORTANT NOTICE

Texas Instruments Incorporated and its subsidiaries (TI) reserve the right to make corrections, enhancements, improvements and other changes to its semiconductor products and services per JESD46, latest issue, and to discontinue any product or service per JESD48, latest issue. Buyers should obtain the latest relevant information before placing orders and should verify that such information is current and complete. All semiconductor products (also referred to herein as "components") are sold subject to TI's terms and conditions of sale supplied at the time of order acknowledgment.

TI warrants performance of its components to the specifications applicable at the time of sale, in accordance with the warranty in TI's terms and conditions of sale of semiconductor products. Testing and other quality control techniques are used to the extent TI deems necessary to support this warranty. Except where mandated by applicable law, testing of all parameters of each component is not necessarily performed.

TI assumes no liability for applications assistance or the design of Buyers' products. Buyers are responsible for their products and applications using TI components. To minimize the risks associated with Buyers' products and applications, Buyers should provide adequate design and operating safeguards.

TI does not warrant or represent that any license, either express or implied, is granted under any patent right, copyright, mask work right, or other intellectual property right relating to any combination, machine, or process in which TI components or services are used. Information published by TI regarding third-party products or services does not constitute a license to use such products or services or a warranty or endorsement thereof. Use of such information 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.

Reproduction of significant portions of TI information in TI data books or data sheets is permissible only if reproduction is without alteration and is accompanied by all associated warranties, conditions, limitations, and notices. TI is not responsible or liable for such altered documentation. Information of third parties may be subject to additional restrictions.

Resale of TI components or services with statements different from or beyond the parameters stated by TI for that component or service voids all express and any implied warranties for the associated TI component or service and is an unfair and deceptive business practice. TI is not responsible or liable for any such statements.

Buyer acknowledges and agrees that it is solely responsible for compliance with all legal, regulatory and safety-related requirements concerning its products, and any use of TI components in its applications, notwithstanding any applications-related information or support that may be provided by TI. Buyer represents and agrees that it has all the necessary expertise to create and implement safeguards which anticipate dangerous consequences of failures, monitor failures and their consequences, lessen the likelihood of failures that might cause harm and take appropriate remedial actions. Buyer will fully indemnify TI and its representatives against any damages arising out of the use of any TI components in safety-critical applications.

In some cases, TI components may be promoted specifically to facilitate safety-related applications. With such components, TI's goal is to help enable customers to design and create their own end-product solutions that meet applicable functional safety standards and requirements. Nonetheless, such components are subject to these terms.

No TI components are authorized for use in FDA Class III (or similar life-critical medical equipment) unless authorized officers of the parties have executed a special agreement specifically governing such use.

Only those TI components which TI has specifically designated as military grade or "enhanced plastic" are designed and intended for use in military/aerospace applications or environments. Buyer acknowledges and agrees that any military or aerospace use of TI components which have **not** been so designated is solely at the Buyer's risk, and that Buyer is solely responsible for compliance with all legal and regulatory requirements in connection with such use.

TI has specifically designated certain components as meeting ISO/TS16949 requirements, mainly for automotive use. In any case of use of non-designated products, TI will not be responsible for any failure to meet ISO/TS16949.

### Products

Audio	<a href="http://www.ti.com/audio">www.ti.com/audio</a>
Amplifiers	<a href="http://amplifier.ti.com">amplifier.ti.com</a>
Data Converters	<a href="http://dataconverter.ti.com">dataconverter.ti.com</a>
DLP® Products	<a href="http://www.dlp.com">www.dlp.com</a>
DSP	<a href="http://dsp.ti.com">dsp.ti.com</a>
Clocks and Timers	<a href="http://www.ti.com/clocks">www.ti.com/clocks</a>
Interface	<a href="http://interface.ti.com">interface.ti.com</a>
Logic	<a href="http://logic.ti.com">logic.ti.com</a>
Power Mgmt	<a href="http://power.ti.com">power.ti.com</a>
Microcontrollers	<a href="http://microcontroller.ti.com">microcontroller.ti.com</a>
RFID	<a href="http://www.ti-rfid.com">www.ti-rfid.com</a>
OMAP Applications Processors	<a href="http://www.ti.com/omap">www.ti.com/omap</a>
Wireless Connectivity	<a href="http://www.ti.com/wirelessconnectivity">www.ti.com/wirelessconnectivity</a>

### Applications

Automotive and Transportation	<a href="http://www.ti.com/automotive">www.ti.com/automotive</a>
Communications and Telecom	<a href="http://www.ti.com/communications">www.ti.com/communications</a>
Computers and Peripherals	<a href="http://www.ti.com/computers">www.ti.com/computers</a>
Consumer Electronics	<a href="http://www.ti.com/consumer-apps">www.ti.com/consumer-apps</a>
Energy and Lighting	<a href="http://www.ti.com/energy">www.ti.com/energy</a>
Industrial	<a href="http://www.ti.com/industrial">www.ti.com/industrial</a>
Medical	<a href="http://www.ti.com/medical">www.ti.com/medical</a>
Security	<a href="http://www.ti.com/security">www.ti.com/security</a>
Space, Avionics and Defense	<a href="http://www.ti.com/space-avionics-defense">www.ti.com/space-avionics-defense</a>
Video and Imaging	<a href="http://www.ti.com/video">www.ti.com/video</a>

### TI E2E Community

[e2e.ti.com](http://e2e.ti.com)