AM43x devices: Sitara™ ARM® Cortex®-A9 processors

Texas Instruments

Device/Family description

The Sitara™ AM43x devices are a scalable, highly integrated processor family with flexible peripherals, connectivity and security features; all built around pin-to-pin compatible hardware and a common software platform that accelerates time to market and reduces overall system cost.

At the heart of the AM43x processor is an ARM® Cortex®-A9 core with speeds of up to 1 GHz. The AM43x device has multiple 32-bit memory options, dual-camera support, dual CAN, dual Gigabit Ethernet, enhanced 3D graphics acceleration core, quad-core programmable real time unit (PRU) for industrial communications protocols, and much more. AM43x devices share the same TI Processor SDK, which is the common software development kit platform allowing for easy migration between all of TI's Sitara processors.

TI Embedded Security Portfolio –

Security is hard, we make it easier

Security problem targeted: Typical threats / security measures

Security threats are always present. The security of an embedded system should not be an afterthought, an after-the-fact add-on or a nice-to-have feature. If hackers tamper with boot code, they could insert malware that could hijack a system, download intellectual property (IP), snoop on unsuspecting users or take any number of nefarious actions.

Security is either designed into the embedded processor so that the device operates as intended from the time power is first supplied, or it's not. Building a powerful security foundation begins when the system boots. Security features in embedded systems can help developers reduce the risk of a security breach. Establishing a root-of-trust through a secure boot process helps to ensure the integrity of the system and guards against hackers taking over any part of the system. This helps protect customer's software in the system and acts as an anti-cloning barrier so the system or any part of it, cannot be copied.

The AM43x processor family offers a comprehensive package for evaluation and development of secure boot and software signing/encryption; including software, image signing tool, OTP key provisioning tool, user guides and a secure boot reference hardware EVM containing an AM43x development device.

Security features details:

What is secure boot? The prime function of secure boot is to provide takeover protection, that when properly configured can assist customers in designing their systems such that the device only executes authentic code and rejects code that is not signed by authorized keys. The first possible point where the security of the system might be compromised is during the boot process when the system is becoming operational. If this process is not secure, there is no root-of-trust established in the system. So, to secure the boot process, the boot firmware stored in memory must be certifiably secure and authentic.

What role does cryptography play? One of the fundamental technologies used to secure the boot process is cryptography, which can be used to limit access to boot code to only authorized users, to secure code as it is transferred from memory to the processor and to certify the authenticity of boot code as it arrives to be processed. Asymmetric and symmetric cryptography are the two most common key-processing techniques employed in embedded systems which rely on other elements of cryptography, such as random number generators and hashing.

Additional security information:

TI Sitara AM43x processors have been designed with security in mind. Secure boot as well as its supporting security infrastructure provides the root-of-trust upon which developers can begin to build security subsystems to meet their desired security objectives. Secure boot, when properly configured, is the foundation for providing root-of-trust and is a requisite for any system's security.

Additional resources

- **Embedded processor security white paper**
- For more information about TI's secure boot feature on AM43x processors, or to purchase a high-secure EVM or obtain SEC-DEV software, please fill out the request form on **TI.com**.

Security enablers:

Device	Security enablers	Detailed security features
AM4372S, AM4376S, AM4377S, AM4378S, AM4379S	Debug security	JTAG access can be disabled: control of chip debug, test and trace capabilities
	Secure storage	Keys or data can be protected from outside access in ROM and RAM
	Cryptographic acceleration	Hardware crypto accelerators: DES/3DES, AES, SHA, MD5, Fast PKA and TRNG
	Initial secure programming	Secure boot, cryptographic accelerator
	Trusted execution environment	ARM Trustzone, secure DMA, secure storage, secure WDG Interconnect security firewalls
	Secure boot	Secure flashing and booting: IP protection, takeover, anti-cloning; on-chip one-time-programmable (OTP) keys
	IP protection	External contents of Flash are encrypted
	Device identity	Unique device ID based on part number features and manufacturing data

For more information about the TI Security Solutions, visit the TI security web site at **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