Understanding security features for DRA7xx “Jacinto 6” automotive processors

Texas Instruments

Device/Family description

The “Jacinto 6” family of automotive processors enables digital cockpit applications including infotainment and digital instrument clusters.

TI Embedded Security Portfolio –

Security is hard, TI makes it easier

Security problem targeted: Typical threats / security measures

With the increasing amount of electronic components and features in cars also comes an increasing number of threats to assets like sensitive data and intellectual property. In automotive applications, protecting these assets can be critical to ensuring the integrity and correct functioning of infotainment and cluster systems. To help automotive engineers protect these assets, the DRA7xx “Jacinto 6” family of automotive processors is available in a High-Security (HS) version, in addition to the standard general-purpose (GP) device variant. The high security versions of the “Jacinto 6” processors come with features that provide a foundation for automotive OEMs and Tier 1 manufacturers to implement more robust security in their systems.

Security features details:

Secure boot

To prevent booting of an unauthenticated firmware or kernel that could compromise important system functions, “Jacinto 6” HS processors have a secure boot feature, enforced via a “root-of-trust” key embedded in the device. Any software booted must be verified against the “root-of-trust”, or an extension to it. In this way, OEMs and Tier 1 manufacturers can design systems so that only authorized software and applications (those signed by the OEM or system integrator) can be loaded and run on the processor.

Trusted execution environment

The “Jacinto 6” processors are also equipped with features to help the user extend their security implementation beyond initial boot time authentication. DRA7xx processors support the industry-standard ARM® TrustZone®

Security enablers:

Device	Security enablers	Detailed security features
DRA7xx “Jacinto 6”	Secure boot	“Root-of-trust” key
	Trusted execution environment	Secure-execution-capable CPU Support for OP-TEE Secure infrastructure—Firewalls
	Cryptographic acceleration	AES, DES3DES, DES, TRNG
	Device identity	Unique public ID per device
	Debug security	JTAG lock Per-device debug token
	Secure storage	Enabled via secure ROM APIs and OP-TEE

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

technology, which allows the ARM Cortex®-A15 cores within the system-on-chip (SoC) to execute code in a separate secure world, isolated from the public world. This technology enables segregating functions that require isolation and security from other code, such as third-party applications or drivers that could be considered untrusted. The hardware within the ARM Cortex-A15 cores enables separation and helps to prevent the leakage of information between the secure and public domains.

The idea of separation within the core is important, but it also needs to be extended beyond the processor's cores and into the remainder of the system-on-chip. The bus infrastructure of the "Jacinto 6" processors carries the state of each transaction, including whether they are secure or non-secure. Firewalls throughout the SoC enable the system designer to setup hardware-enforced access controls to bus targets such as external memory and peripheral interfaces and ensure separation between different core operating modes (secure and non-secure, privileged and non-privileged), other device cores (DSP, multiple Cortex-M4 auxiliary CPUs) and the various bus initiators.

The flexible and programmable firewall features of "Jacinto 6", along with the heterogeneous multi-core architecture, enable hardware enforced isolation of various sub-systems to fit the product requirements. For example, in digital instrument cluster applications, auxiliary processing cores can be used to manage the overall display functions to ensure proper display content is maintained, as well as provide monitoring functionality. Furthermore, the aux core and display functions and can be isolated with firewalls so that the primary system cannot interfere with the auxiliary core operations.

Additional security information

The "Jacinto 6" family also supports the Open Portable Trusted Execution Environment (OP-TEE), an open-source TEE maintained by Linaro. OP-TEE provides a secure environment with support for GlobalPlatform APIs and crypto abstraction layer to add support for hardware crypto acceleration to enable portable runtime security applications.

Resources

- **Blog**
- **Video**
- **Jacinto overview**

Security is hard, TI makes it easier

For more information about TI's Embedded Security Solutions, visit **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