Technical White Paper

Securing the Future: Cyber Resilience Act (EU-CRA) Compliance With TI's Jacinto and Sitara Processors

ABSTRACT

This document provides a brief overview of the Cyber Resilience Act (CRA) from the European Union (EU). This document first discusses the key features and requirements of EU-CRA, followed by a description of how the Jacinto™ and Sitara™ processors from TI meet the upcoming EU-CRA requirements.

Table of Contents

1 Introduction

Digital products and services are now integral to daily life. The number of connected devices is expected to rise exponentially, increasing the surface and potential for cyber attacks during this growth. In 2024, the European Parliament adopted the Cyber Resilience Act (CRA) to strengthen cyber resilience across the European Union (EU). The CRA aims to reduce vulnerabilities in digitally-enabled products and embed comprehensive security throughout the life cycle of these products. The CRA requires that products containing digital elements incorporate mandatory security-by-design principles throughout the entire lifecycle that encompasses both hardware and software.

This document explains how processors from Texas Instruments, and the accompanying features of these processors, can help original equipment manufacturers (OEMs) achieve compliance with the CRA. This document first outlines the key requirements of the CRA for important Class-1 products, mainly microprocessors, and then maps those requirements to the capabilities of TI's processor portfolio.

2 Scope of CRA

The EU CRA regulation applies to products and components with digital elements made available on the EU market, such as any hardware or software product processing digital data which is intended or is expected to be connected to another device or to a network.

Table 2-1. Examples of Products and Components That are Included and Excluded in Scope

Examples of Products and Components With Digital Elements	Products With Digital Elements to which the Following Existing EU Regulations Apply
• Network management systems • Smart appliances • Mobile phones • Microprocessors and microcontrollers • Operating systems • Open-source software • Boot manager	• Motor vehicles, and motor vehicle systems – Regulation (EU) 2019/2144 • Medical devices – Regulation (EU) 2017/745 • In vitro diagnostic devices – Regulation (EU) 2017/746 • Information technology services, cloud services, software as a service (SaaS), and so forth – Directive (EU) 2022/2555 • Marine equipment – Directive 2014/90/EU • Civil aviation – Regulation (EU) 2018/1139 • National security and defense

3 Product Requirements

The CRA requires that the product delivers an appropriate level of security and is free from *known* vulnerabilities. Based on the cybersecurity risk profile of the product, the applicable safeguards must include security by default —enabling adequate security updates and protecting against unauthorized access. The CRA covers additional requirements for the confidentiality and integrity of data, including requirements for:

- Commands and programs
- The minimization of stored data
- The availability of essential functions
- Reducing negative impacts on other devices
- Limiting attack surfaces
- Mitigating incident impacts
- Recording and monitoring security-relevant events
- Securing permanent erasure or transfers of data and settings

4 Vulnerability Handling Process

The CRA requires that manufacturers identify and document all dependencies and vulnerabilities, provide a software bill of materials (SBOM), and track these items continuously, while verifying that no known vulnerabilities remain and any dependencies and vulnerabilities which surface must be addressed without delay. Manufacturers must test the security of the digital product, publicly disclose information about fixed vulnerabilities, maintain a coordinated vulnerability disclosure policy, facilitate sharing of potential vulnerability data, and deliver patches promptly, free of charge, with advisory messages.

5 Information and Labeling

Compliance to the CRA demands a CE (Conformité Européenne) marking on the product and an EU Declaration of Conformity, the appointment of an authorized representative, designation of a security point-of-contact, and clear identification of the product. The CRA requires technical documentation that must contain:

- A cybersecurity risk assessment
- Information on the availability of security updates
- An SBOM covering top-level dependencies
- Definitions of support and the duration of that support
- Access to revisions through a public software archive
- A user instruction set

6 TI Processors Meeting the Requirements of the CRA

The Jacinto™ (TDA4x and DRA8x) and Sitara™ (AM6x) processor families are engineered to satisfy security by default requirements. In every microprocessor in these families, a dedicated public key is hardwired into the silicon. Only firmware signed with the corresponding private key can pass the boot check. This key establishes a hardware root-of-trust that verifies both authenticity and integrity for all software running on the platform, so that only authenticated software runs on the processor.

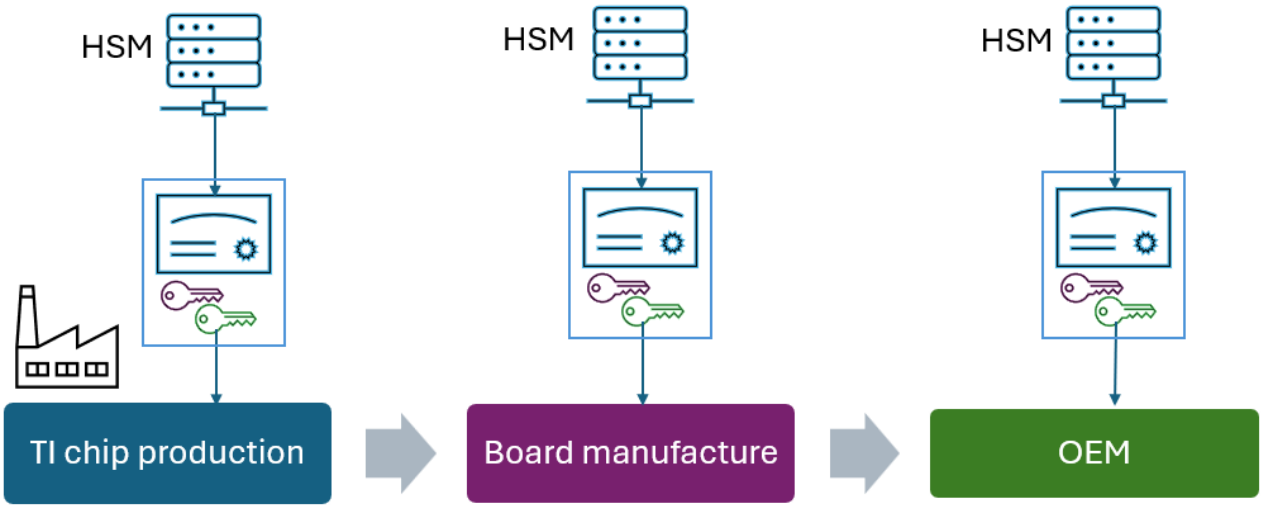

Figure 6-1. Root of Trust (RoT) Key Provisioning

TI processors embed hardware access control that segment the on-chip memory into isolated zones, shielding critical memory sections from unauthorized read or write operations. The platform enables separation between concurrent workloads by assigning each application (which often runs on a distinct CPU core within the same device) an individual protected code and data region; thereby, preventing accidental leakage or malicious interference. In addition to these memory safeguards, the processors offer features to access control the debug port. A debug interface can be permanently disabled for production units, or the debug interface can be exposed only after a request is authenticated through a signed certificate, thus closing common attack vectors that exploit debugging tools.

Comprehensive documentation is supplied for each package and the firmware and software released for TI processors is first scanned for known vulnerabilities. Together, these controls meet the appropriate level of security required by the Cyber Resilience Act.

TI aims to release software with no known vulnerabilities. TI has had an active vulnerability handling process for many years through TI's Product Security Incident Response Team (PSIRT). The vulnerability handling process at TI includes the following examples:

- The generation of an SBOM

- Tracking vulnerabilities across various software that TI provides as part of the processors
- Providing fixes to critical vulnerabilities
- Public disclosure when the vulnerabilities are fixed

TI is actively monitoring the requirements of the coordinated vulnerability disclosure (CVD) and putting a system in place for vulnerability disclosures.

Processors from TI provide a set of compliance artifacts that satisfy the requirements of the Cyber Resilience Act in a straightforward way. Each silicon family is shipped with a detailed datasheet, and TI publishes a clear update policy that informs customers when and how firmware patches are delivered. For every software stack (for example, bootloaders, SDKs, and middleware) an SBOM lists all top-level licenses, components, and the dependencies, making vulnerability tracking easy. TI generates and provides an SBOM as part of newer SDK releases for each processor. The lifecycle guide for the product outlines the support period, end-of-life dates, and the scope of warranty for each device. The comprehensive user guides explain how to configure security features, such as secure boot and debug port control; while every chip carries a unique part number and die ID that allows end users to verify the exact product variant. All together, these documents, updates, SBOMs, and identifiers give OEMs the evidence required to prove CRA compliance of TI processors.

7 Conclusions

The Cyber Resilience Act gives direction to vendors like TI regarding the design, manufacture, and support of microprocessors with cybersecurity features. In following the standardized requirements of the CRA, TI brings transparency to the development process. TI's customers can leverage the knowledge and expertise of TI in designing, delivering, and supporting cybersecurity capable microprocessors. TI is actively monitoring the cybersecurity landscape, the developments of the CRA, and other similar standards to implement the features and regulatory requirements that enable customers to comply with cybersecurity requirements. TI is trusted in the industry for building microprocessors with cybersecurity enablers, incorporating advanced security features, and creating processes that help customers achieve long-term success in a cybersecurity environment of constantly evolving requirements and regulations.

8 References

1. European Commission, Cyber Resilience Act, webpage.
2. Texas, Instruments, Microcontrollers (MCUs) & processors, webpage.
3. Texas Instruments, Cyber Resilience Act (CRA), webpage.
4. Texas Instruments, TI PSIRT, webpage.

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, regulatory 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 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, TI’s General Quality Guidelines, 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. Unless TI explicitly designates a product as custom or customer-specified, TI products are standard, catalog, general purpose devices.

TI objects to and rejects any additional or different terms you may propose.

Last updated 10/2025