Technical White Paper

守护未来安全：通过 TI 的 Jacinto 和 Sitara 处理器实现《网络弹性法案》(EU-CRA) 合规

摘要

本文档简要概述了欧盟 (EU) 的《网络弹性法案》(CRA)。文中首先讨论了 EU-CRA 的主要特性和要求，然后说明了 TI 的 Jacinto™ 和 Sitara™ 处理器如何满足即将实施的 EU-CRA 要求。

内容

1 简介

数字产品和服务如今已是日常生活中不可或缺的一部分。联网设备数量预计将呈指数级增长，在这一增长过程中，网络攻击的接触面和潜在风险也随之增加。2024 年，欧洲议会通过了《网络弹性法案》(CRA)，以加强欧盟 (EU) 内部的网络弹性。CRA 旨在减少数字产品中的漏洞，并将全面的安全防护嵌入这些产品的整个生命周期。CRA 要求含有数字元素的产品在整个生命周期内（涵盖硬件和软件）遵守强制性设计即安全原则。

本文档阐释了德州仪器 (TI) 的处理器及其配套特性如何帮助原始设备制造商 (OEM) 实现 CRA 合规。文中首先概述了 CRA 对重要 1 类产品（主要是微处理器）的关键要求，然后将这些要求映射到 TI 处理器产品组合的各项功能。

2 CRA 的范围

EU CRA 法规适用于在欧盟市场投放的含有数字元素的产品和组件（例如所有处理数字数据的硬件或软件产品），只要其设计目的或预期是要与其他器件或网络相连，就会纳入法规监管范围。

表 2-1. 该范围包含和不包含的产品和组件示例

含有数字元素的产品和组件示例	含有以下欧盟现行法规适用的数字元素的产品
• 网络管理系统 • 智能电器 • 手机 • 微处理器和微控制器 • 操作系统 • 开源软件 • 启动管理器	• 机动车辆和机动车辆系统 — 法规 (EU) 2019/2144 • 医疗设备 — 法规 (EU) 2017/745 • 体外诊断设备 — 法规 (EU) 2017/746 • 信息技术服务、云服务、软件即服务 (SaaS) 等 — 指令 (EU) 2022/2555 • 船用设备 -— 指令 2014/90/EU • 民航 — 法规 (EU) 2018/1139 • 国家安全与国防

3 产品要求

CRA 要求产品具有适当的安全级别，并且不存在*已知*漏洞。根据产品的网络安全风险概况，适用的防护措施必须包含默认安全，实现充分的安全更新并防止未经授权的访问。CRA 还涵盖对数据机密性和完整性的额外要求，包括：

- 命令与程序
- 最大限度减少存储数据
- 提供基本功能
- 减少对其他器件的负面影响
- 限制攻击面
- 减轻事故影响
- 记录和监控安全相关事件
- 确保数据及设置得到永久擦除或安全转移

4 漏洞处理流程

CRA 要求制造商识别并记录所有依赖项和漏洞，提供软件物料清单 (SBOM) 并持续跟踪这些物料，同时确认不存在已知漏洞，且任何发现的依赖项和漏洞必须及时处理。制造商必须测试数字产品的安全性，公开披露已修复漏洞的信息，维持协调漏洞披露策略，促进潜在漏洞数据共享，并及时免费提供补丁及通告消息。

5 信息和标记

要遵守 CRA，要求产品加贴 CE (Conformité Européenne) 标志，提供欧盟符合性声明，指定授权代表，设立安全联系人，并对产品进行明确标识。CRA 要求技术文档必须包含：

- 网络安全风险评估
- 安全更新的可用性信息
- 涵盖顶级依赖项的 SBOM
- 支持的定义及其持续时间
- 通过公开软件存档访问修订版

- 用户指令集

6 TI 处理器符合 CRA 要求

Jacinto™ （TDA4x 和 DRA8x）和 Sitara™ (AM6x) 处理器系列专为满足默认安全要求而设计。在这些系列的每个微处理器中，都将专用的公钥硬接线到芯片中。只有使用了对应私钥签名的固件才能通过启动校验。该密钥建立了一个硬件信任根，用于验证平台上运行的所有软件的真实性和完整性，确保只有经过身份验证的软件才能在处理器上运行。

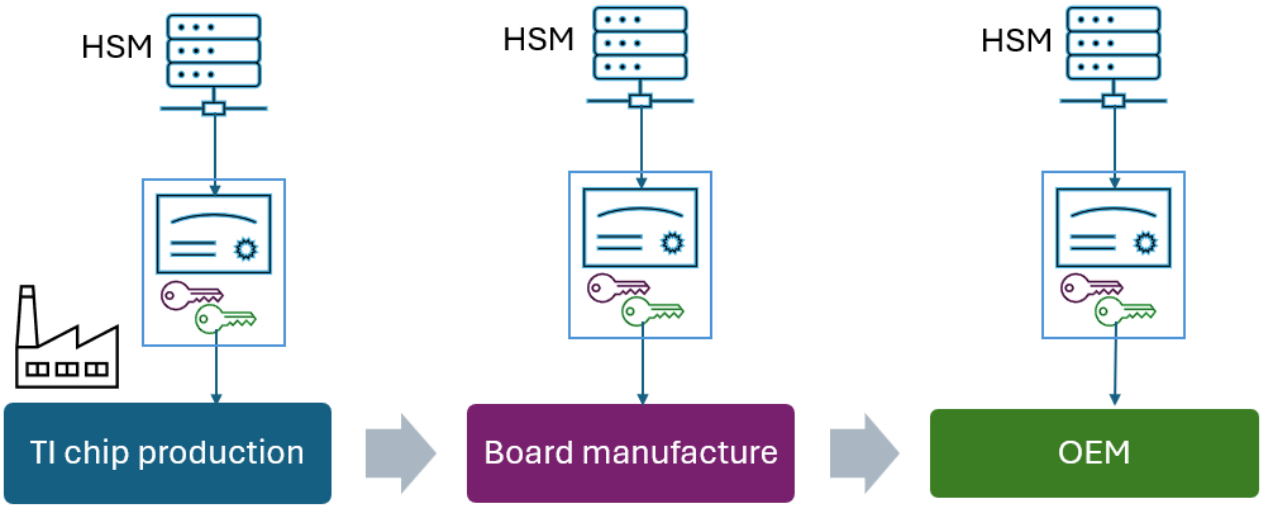

图 6-1. 信任根 (RoT) 密钥配置

TI 处理器内嵌了硬件访问控制功能，可将片上存储器划分为相互隔离的区域，保护关键存储器区域免受未经授权的读写操作。该平台通过为每个应用程序（通常在同一器件内的不同 CPU 核心上运行）分配单独的受保护代码和数据区域，实现并发工作负载间的隔离，从而防止意外泄露或恶意干扰。除了这些存储器保护措施外，这些处理器还提供了对调试端口的访问控制功能。可以对生产单元永久禁用调试接口，或者仅在请求通过了签名证书的验证后才开放调试接口，从而关闭利用调试工具进行攻击的常见攻击向量。

每个封装均提供全面的文档，且首先会对为 TI 处理器发布的固件和软件进行已知漏洞扫描。这些控制措施共同实现了《网络弹性法案》所要求的适当安全级别。

TI 致力于发布不存在已知漏洞的软件。多年来，TI 一直通过其产品安全事件响应团队 (PSIRT) 积极执行漏洞处理流程。TI 的漏洞处理流程包括以下示例：

- 生成 SBOM
- 跟踪 TI 作为处理器一部分提供的各种软件中的漏洞
- 修复关键漏洞
- 漏洞修复后公开披露

TI 正在积极关注协调漏洞披露 (CVD) 的要求，并建立漏洞披露系统。

TI 的处理器提供了一系列合规工件，可简单直接地满足《网络弹性法案》的要求。每个芯片系列都随附有详细的数据表，TI 还发布了清晰的更新策略，会告知客户固件补丁的交付时间和方式。对于每个软件栈（例如引导加载程序、SDK 和中间件），SBOM 列出了所有顶级许可证、组件和依赖项，使漏洞追踪变得轻松易行。作为新 SDK 版本的一部分，TI 会为每个处理器生成并提供 SBOM。产品的生命周期指南概述了每个器件的支持期限、停产日期和保修范围。全面的用户指南则解释了如何配置安全功能，例如安全引导和调试端口控制；同时，每颗芯片拥有唯一的器件型号和裸片 ID，使最终用户能够核实确切的产品型号。所有这些文档、更新、SBOM 和标识符，为 OEM 提供了证明 TI 处理器符合 CRA 要求所需的证据。

7 结论

《网络弹性法案》为像 TI 这样的供应商在设计和制造具备网络安全特性的微处理器以及提供相应支持方面指明了方向。通过遵循 CRA 的标准化要求，TI 实现了开发流程的透明化。TI 的客户可以充分利用 TI 在设计、交付和支持具备网络安全功能的微处理器方面所积累的知识与专长。TI 正在积极关注网络安全形势、CRA 及其他类似标准的发展，以落实相应的功能和法规要求，助力客户满足网络安全要求。TI 在业界以打造内置网络安全功能的微处理器、集成先进安全特性以及建立相关流程而备受信赖，这些流程有助于客户在要求与法规不断演变的网络安全环境中取得长期成功。

8 参考资料

1. 欧洲委员会，《网络弹性法案》，网页。
2. 德州仪器 (TI)，微控制器 (MCU) 和处理器，网页。
3. 德州仪器 (TI)，《网络弹性法案》(CRA)，网页。
4. 德州仪器 (TI)，TI PSIRT，网页。

重要通知和免责声明

TI“按原样”提供技术和可靠性数据（包括数据表）、设计资源（包括参考设计）、应用或其他设计建议、网络工具、安全信息和其他资源，不保证没有瑕疵且不做出任何明示或暗示的担保，包括但不限于对适销性、与某特定用途的适用性或不侵犯任何第三方知识产权的暗示担保。

这些资源可供使用 TI 产品进行设计的熟练开发人员使用。您将自行承担以下全部责任：(1) 针对您的应用选择合适的 TI 产品，(2) 设计、验证并测试您的应用，(3) 确保您的应用满足相应标准以及任何其他安全、安保法规或其他要求。

这些资源如有变更，恕不另行通知。TI 授权您仅可将这些资源用于研发本资源所述的 TI 产品的相关应用。严禁以其他方式对这些资源进行复制或展示。您无权使用任何其他 TI 知识产权或任何第三方知识产权。对于因您对这些资源的使用而对 TI 及其代表造成的任何索赔、损害、成本、损失和债务，您将全额赔偿，TI 对此概不负责。

TI 提供的产品受 TI 销售条款)、TI 通用质量指南 或 ti.com 上其他适用条款或 TI 产品随附的其他适用条款的约束。TI 提供这些资源并不会扩展或以其他方式更改 TI 针对 TI 产品发布的适用的担保或担保免责声明。 除非德州仪器 (TI) 明确将某产品指定为定制产品或客户特定产品，否则其产品均为按确定价格收入目录的标准通用器件。

TI 反对并拒绝您可能提出的任何其他或不同的条款。

最后更新日期：2025 年 10 月