Product Overview

F29-TIFS-SDK 产品简介

软件产品概述

F29 器件中的硬件安全管理器包含多个旨在实现系统安全目标的元件块。其中包括各种存储器、安全管理器、加密加速器引擎、外设模块和安全邮箱。主机 C29 子系统与 HSM 子系统连接，以执行代码身份验证、安全启动、安全固件升级和加密运行时通信所需的加密操作。

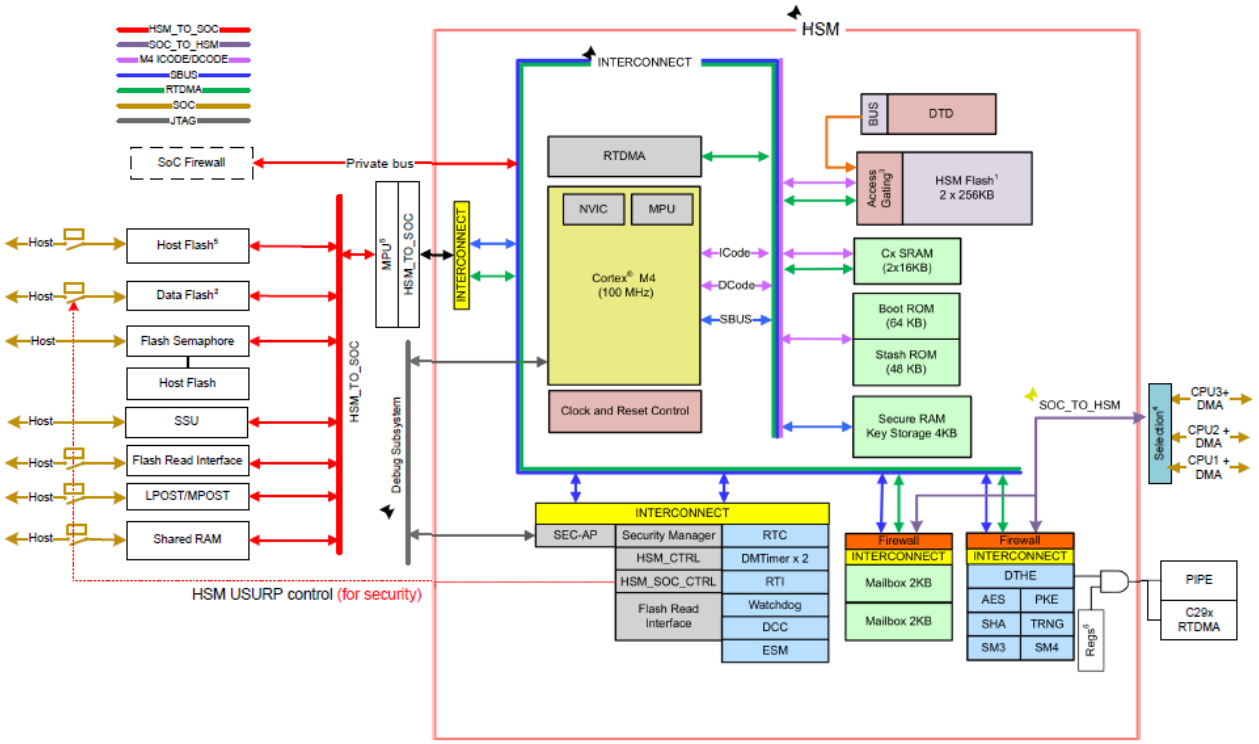

图 1. HSM 方框图

F29 器件的安全目标

- 模块和平台保护：
  - 保护模块（硬件和软件）并防止平台被接管和受到未经授权的修改。
  - 保护关键资产和资源免受硬件和软件攻击
- 限制关键资产的攻击面 -
  - 将关键资产隔离在访问受严格限制的受保护空间中。重点防范基于类的攻击。
  - 假设系统的其余部分受到入侵，以保护关键资产。
- 沙盒安全性：
  - 安全功能在隔离的环境中运行。
  - 应用模块和任务相互安全隔离，即使它们在同一个 CPU 上也是如此。
- 分层安全性：
  - 多层方法，使入侵不会扩散并破坏整个系统的安全性。

  - 每一层与其他层隔离运行。
- 安全功能开发的可追溯性、责任性和隔离：
  - 必须在隔离的环境中开发安全功能以避免意外问题。
  - 也需要这样做以向认证实体和客户证明安全性。

器件生命周期和配置流程

《为高性能实时控制系统实现网络安全 *sprado0*》中也介绍了该流程。

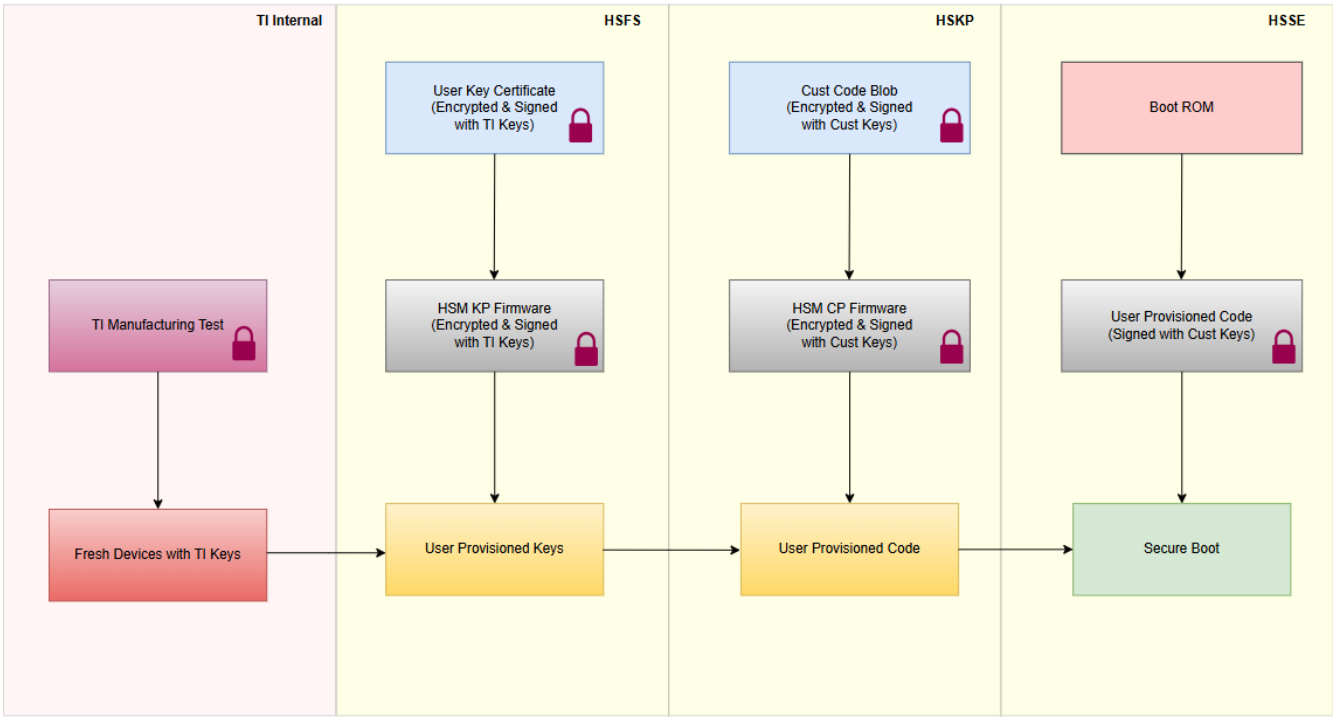

图 2. F29x 器件配置流程

阶段 1：

用户获得 HSFS（字段安全）状态的器件。该器件包含已配置 TI 密钥。在此状态下，HSM 内核仅执行使用 TI 密钥进行加密和签名的代码。

阶段 2：

TI 支持使用密钥配置包（在可信环境中）配置用户密钥，并使用 TI 密钥对用户密钥进行加密和签名。然后，使用闪存内核示例和主机编程器工具安全地传输此密钥证书。在整个过程中保持用户密钥的机密性，使用户即使在非安全环境中也能复制该过程。配置用户加密密钥后，器件的生命周期将更改为 HSKP（密钥已配置）状态。

阶段 3：

现在，由于器件处于 HSKP 状态，因此可以将应用代码编程到器件中。然后使用用户密钥对代码配置进行加密和签名。还使用闪存内核和主机编程器安全传输代码配置。使用器件安全存储中可用的用户密钥对应配置到 HSM 或 C29 闪存中的用户代码进行加密和签名。配置 HSM Code、C29 Code 和 Secure Config (SecCfg) 等所有必需的映像后，器件将转换为 HSSE 状态。HSSE（已加强安全性）器件的生命周期保持代码始终是安全引导。

TI 安全软件组件

TI 可作为 TIFS-SDK 的 2 个主要软件组件：

- 一次性可编程 (OTP) 密钥配置包
- MCU 器件附加包的 TI 基础安全

TI 的 F29x OTP 密钥编写器包

TI 提供的 OTP 密钥编写器包支持将安全器件生命周期从 HS-FS（不具有强制安全功能的开发型号）过渡到 HS-KP（具有强制安全功能的量产型号）。这些配置流程是端到端安全的，可用于不安全的工厂车间配置。

密钥配置流程支持的功能列表

F29x-TIFS-SDK 的 1.01.00 版本可提供此类支持。

- HSM 的已签名密钥写入器固件可接受 x.509 客户密钥证书，且所有闪存 OTP 字段都已配置。
- 支持按一次性客户密钥证书对密钥进行编程。
- 支持基于 RSA-4K、ECDSA secp256R1、secp384R1、secp521r1 和 brainpool512r1 的密钥预置。
- 支持密钥编程的 UART 模式。
- 支持 OpenSSL v3.0.2 及更高版本。
- 加密密钥（SMEK 和 BMEK）是选填字段。公钥（SMPK 和 BMPK）是必填字段。
- 使用 Python 脚本生成 x.509 证书的选项。
- 以下密钥可编程：
  - MSV
  - SMPK、SMEK
  - BMPK、BMEK
  - 外部 OTP
  - 密钥计数
  - SWREV-HSM、SWREV-APP、SWREV-SBL、SWREV-SSU
  - 密钥修订版本

MCU 器件的 TI 基础软件

什么是 TIFS-MCU？

TIFS 表示德州仪器 (TI) F29x SoC 基础安全。其能提供器件信任根和基础安全服务。HSM（即硬件安全模块）由基于安全内核的安全子系统组成。TIFS-MCU 是 F29-SDK 之上的一个附加包，适用于 F29x 器件，例如 F29H85x。TIFS-MCU 在安全 CPU 上启用了裸机安全栈，用户也可以使用该栈。

1. 开发设备信任根并提供基础安全服务
2. 与 3P Auto-HSM 堆栈集成时，TIFS-MCU 并非 AUTOSAR-HSM 堆栈的替代方案。

TIFS-MCU 支持基础安全软件（其具备器件内信任根所需的所有构建块）并且可利用各种服务。AUTOSAR-HSM 栈供应商可以轻松集成 TIFS-MCU，以便开发符合 SHE/EVITA 标准的 HSM 栈。

什么是 TIFS-MCU 中的代码配置固件？

代码配置固件是 TI 交付的软件（包括源代码），可以将软件安全配置到器件的内部闪存中。这样一来，即使在不安全的环境中，用户也可以对 HSM 和 C29 应用程序进行安全编程。

表 1. 代码配置流程支持的特性列表

代码配置流程的特性	映像完整性	存储体模式
HSM 运行时间固件配置	• RSA-4K 与 SHA512 • 采用 SHA512 的 ECDSA secp256R1 • 采用 SHA512 的 ECDSA secp384R1 • 采用 SHA512 的 ECDSA secp521R1 • 采用 SHA512 的 ECDSA brainpool512R1	所有存储体模式
C29 CPU1 配置	• RSA-4K 与 SHA512 • 采用 SHA512 的 ECDSA secp256R1 • 采用 SHA512 的 ECDSA secp384R1 • 采用 SHA512 的 ECDSA secp521R1 • 采用 SHA512 的 ECDSA brainpool512R1	所有存储体模式
安全设置配置	• RSA-4K 与 SHA512 • 采用 SHA512 的 ECDSA secp256R1 • 采用 SHA512 的 ECDSA secp384R1 • 采用 SHA512 的 ECDSA secp521R1 • 采用 SHA512 的 ECDSA brainpool512R1	所有存储体模式

表 2. 安全代码配置流程的软件可交付结果列表

软件组件列表	软件类型	OPN	交付位置	源位于 1.01.00
UART 闪存内核	示例	F29H85x-SDK	ti.com	是
主机编程器	面向如下系统的工具： • Windows • Linux • MacOS	F29H85x-SDK	ti.com	是
OTP 密钥编写器证书生成	Python 工具	F29H85x-TIFS-SDK	安全资源	是
HSM KP 固件	加密固件	F29H85x-TIFS-SDK	安全资源	否
HSM CP 固件	示例	F29H85x-TIFS-SDK	安全资源	是
代码签名工具	Python 工具	F29H85x-TIFS-SDK	安全资源	是

TIFS-MCU SDK 提供哪些功能？

TIFS-MCU SDK 提供开箱即用的服务和 HSM 固件示例，展示了可在 HSM 子系统中执行的用例。

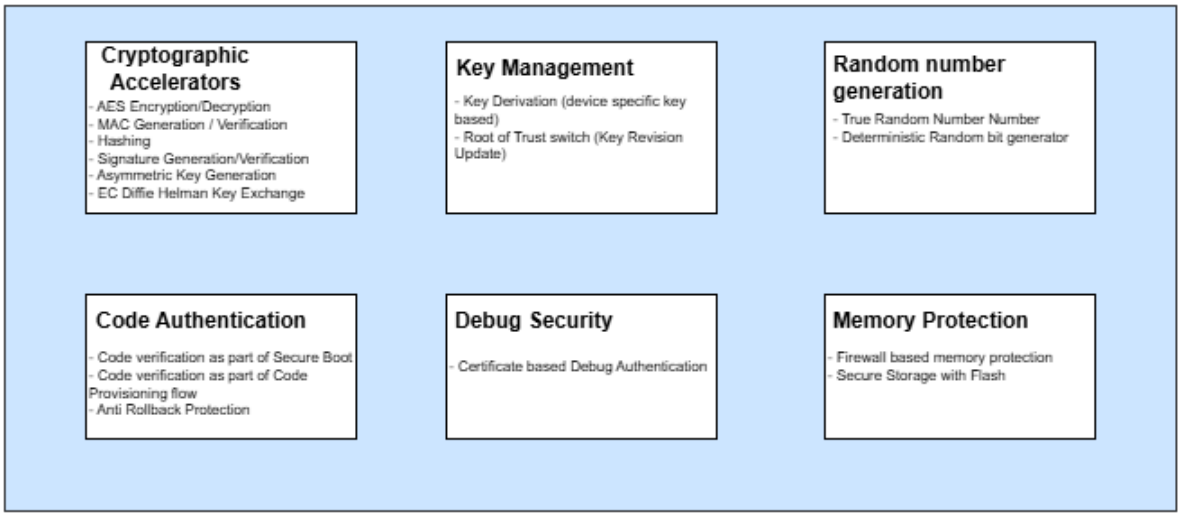

图 3. TIFS-MCU 提供的本机服务

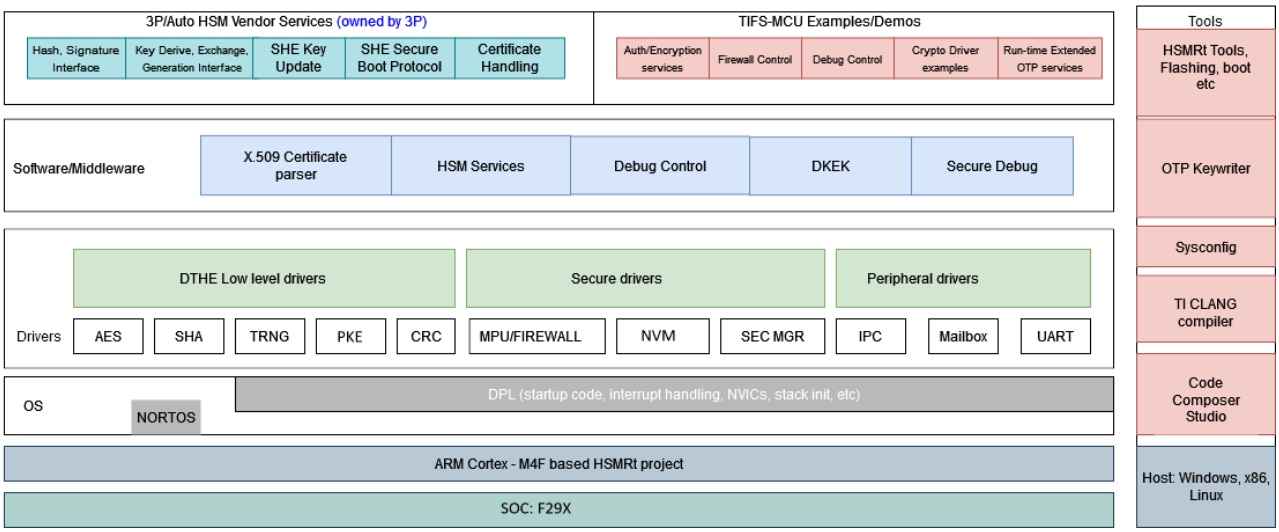

图 4. TIFS-MCU 的软件架构方框图

表 3. TIFS-MCU 软件组件

TIFS-MCU 软件组件	说明
操作系统内核	
无 RTOS	包含可实现由计时器、ISR、主线程组成的非 RTOS 执行环境的模块。允许顶部软件以裸机模式运行。**注 — 仅 NORTOS 支持 HSM 服务器。**
驱动程序移植层 (DPL)	驱动程序用于提取象操作系统环境的 API。示例包括信标、硬件中断、互斥、时钟。
安全性器件驱动程序和模块	
TIFS-MCU 外设驱动程序	HSM 的器件驱动程序库和 API。 *SOC 外设驱动程序列表：* • HSM MBOX 和 Secure IPC • 加密驱动程序 • HSM 闪存、HSM FRI • 安全管理器 • 防火墙
TIFS-MCU 中间件	TIFS-MCU 封装支持的 TIFS-MCU 中间件 *中间件列表：* • HSM 服务器 • HSM 存储器日志 • ASN1 解析器和证书解析器 • 密钥导出 • 加密接口
TIFS-MCU 服务	TIFS-MCU 封装支持的 TIFS-MCU 中间件 *HSM 服务列表：* • HSM 获取版本服务 • HSM 获取 UID 服务 • HSM 运行时间调试验证服务 • HSM 导出 KEK 服务 • HSM 随机数生成服务 • HSM 扩展 OTP 服务 • HSM 防回滚服务 • HSM 信任根切换服务 • HSM 安全固件更新服务
TIFS-MCU 固件	TIFS-MCU 固件的开箱即用示例实现（启用所有上述服务）
示例和演示	
示例和演示	*HSM 示例列表：* • 显示所有 HSM 服务的组合服务演示 • Boot Manager 演示了闪存引导模式下的固件更新 • 加密/解密密码学示例 • 哈希加密示例 • 非对称加密示例
工具（在主机上使用）	
Code Composer Studio (CCS)	构建项目和调试程序的 IDE
TI CLANG 编译器工具链	TI 基于 CLANG 的 ARM 编译器，适用于 ARM M4F
TI C29-CGT 工具链	TI 基于 CLANG 的 C29 编译器，适用于 C29 CPU
SysConfig	系统配置工具，用于配置外设、引脚多路复用和时钟，并生成系统初始化代码
SDK 工具和实用程序	其他工具和实用程序，如闪存工具、引导工具、与 SDK 开发流程配合使用的 CCS 加载脚本

表 3. TIFS-MCU 软件组件（续）

TIFS-MCU 软件组件	说明
OTP Keywriter	OTP Keywriter 用于将客户密钥融合到器件中，并将 HS-FS 转换为 HS-KP 以建立客户信任根。
TIFS-MCU 工具	利用通过 TIFS-MCU 提供的服务的工具和脚本。

表 4. 支持 HSM 服务

服务	说明	现有示例
HSM 获取版本服务	HSM 获取版本服务是为了获取当前 TIFS-MCU 固件版本	是
HSM 获取 UID 服务	当 TIFS-MCU 固件收到 HSM 服务器的获取 UID 请求时，UID 将从安全存储器复制到用户请求的输出存储器位置。	是
HSM 运行时间调试验证服务	要在运行期间解锁调试端口，您需要使用私钥签名的 X509 证书。此服务用于向 TIFS-MCU 固件提供已签名的证书以进行处理。	是
HSM 导出 KEK 服务	TIFS-MCU 提供该服务，以获取基于某些输入常数的导出 KEK。 • 该密钥对于每个器件都是唯一的，并保密。 • 不能以任何方式从硬件获取该密钥。	是
HSM 随机数生成服务	TIFS-MCU 提供该服务，以便从给定的输入常量中获取随机数。	是
HSM 扩展 OTP 服务	TIFS-MCU 为通用 OTP 区域编程提供服务，该区域是由 OTP 闪存位组成的阵列，可供用户自定义使用模型。	是
HSM 防回滚服务	TIFS-MCU 提供防回滚服务，可防止引导旧版软件映像。该器件有 OTP 字段，用于保存 SBL、HSMRt、SECCFG 和应用程序映像的软件版本。	是
HSM 信任交换机服务根	TIFS-MCU 提供安全 RoT 切换，可从辅助密钥切换到备份密钥。SoC 中存在两个信任根密钥：辅助 (SMPK/SMEK) 和备份 (BMPK/BMEK)。如果辅助密钥受损，攻击者可以控制整个 SoC。	是
HSM 固件更新服务	TIFS-MCU 提供安全固件更新服务，包括证书身份验证流程、信任根密钥验证以及在整个流程中保持映像的完整性。	是

表 5. 支持加密硬件加速器和模式

加密核心	软件驱动程序提供支持	现有示例	规格
AES 加密和解密	• 128,192 和 256 位密钥 • ECB、CBC、CCM、CTR、CFB • 单次 + 流模式 • CPU 轮询模式	是	
AESMAC 生成和验证	• 128,192 和 256 位密钥 • CCM、CBC-MAC、CMAC • 单次 + 流模式 • CPU 轮询模式	是	
SHAHasing 算法	• SHA256、SHA512 • HMAC SHA-256、HMAC SHA-512 • 单次 + 流模式 • CPU 轮询模式	是	
RSA 加密和解密签名和验证	• RSA 2048、3072、4096 位 • RSA PKCS1_5，PSS2_1 • CPU 轮询模式	仅限 4K 的 RSA PKCS1_5	

表 5. 支持加密硬件加速器和模式（续）

加密核心	软件驱动程序提供支持	现有示例	规格
ECDSA 签名和验证	• SECP256、SECP384、SECP521 • BRAINPOOL-P512 • CPU 轮询模式	是	
EDDSA 签名和验证	• ED25519 • CPU 轮询模式	是	
ECDH Diffie Helman 密钥交换	• SECP256、SECP384、SECP521 • BRAINPOOL-P512 • CPU 轮询模式	是	

有效器件列表

- F29H85x

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、某特定用途方面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功能安全、信息安全、监管或其他要求。

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。您应全额赔偿因在这些资源的使用中对 TI 及其代表造成的任何索赔、损害、成本、损失和债务，TI 对此概不负责。

TI 提供的产品受 TI 的销售条款或 ti.com 上其他适用条款/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。

TI 反对并拒绝您可能提出的任何其他或不同的条款。

邮寄地址：Texas Instruments, Post Office Box 655303, Dallas, Texas 75265