Product Overview

AM26xx 系列 TIFS-SDK 产品简介

1 AM26x 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/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泄露的情况。
  - 也需要这样做以向认证实体和客户证明安全性。

2 TI 提供的软件组件

TI 可作为 TIFS-SDK 的 2 个主要软件组件：

- OTP 密钥配置包
- TIFS-MCU（TI 的基础安全）附加包

3 器件生命周期和配置流程

在 MCU+ Academy 中介绍了该流程。

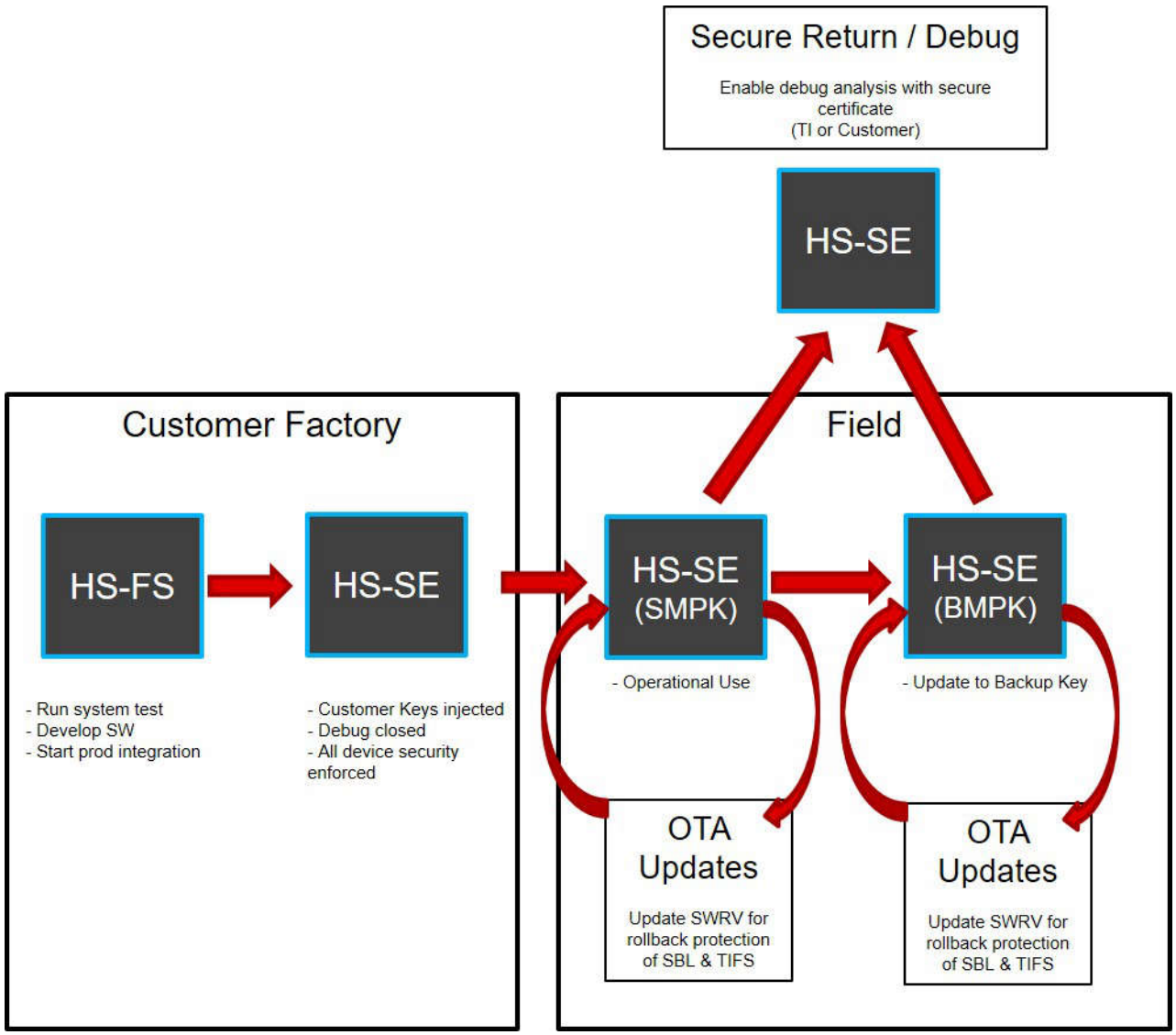

图 1. AM26x 器件系列的安全生命周期

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，使用在器件上执行的 SBL 密钥编写器示例安全地传输此密钥证书，该示例作为 OTP 密钥配置包的一部分提供。使用 SBL 密钥编写器的方法有多种，例如 UART 引导模式，闪存引导模式（QSPI 或 OSPI 引导模式）等。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 HSSE 状态。

阶段 3：

现在，由于器件处于 HSSE 状态，例如通过为器件配置密钥、强制执行安全启动和锁定调试接口，可以将应用代码编程到外部闪存中（如需要，使用器件）。作为 MCU+ SDK 的一部分提供的 uniflash 可用于将引导加载程序以及应用程序映像编程到外部闪存中。请注意，因器件转换为 HSSE，uniflash 映像执行的配置过程也会在器件上安全地启动。由于该器件支持加密的安全启动，因此可以通过通信介质和外部闪存对数据进行加密，从而保持机密性。

使用器件安全存储中可用的用户密钥，对 HSM Run Time 固件和 SBL 的用户代码进行加密和签名。一旦配置了所有必需的映像（例如 HSM Run Time 软件、SBL 软件和应用程序映像），代码就始终是安全启动。

4 TI 的 AM26xx OTP 密钥编写器包

TI 提供的 OTP 密钥写入器封装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）转换到 HS-SE（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。

4.1 OTP 密钥编写器流程支持的功能列表

- 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 eFuse 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。
- 支持以下引导模式- UART、JTAG、USB（仅适用于 AM261x）和闪存（QSPI/OSPI）模式，在该等模式下，可引导密钥编程。
- 支持 RSA 以及基于 ECDSA 的 OTP 编程。
- 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
  - 密钥修订版本

5 MCU 器件的 TI 基础软件

什么是 TIFS-MCU？

TIFS 表示德州仪器 (TI) AM26xx SoC 基础安全。其能提供设备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 用作 MCU+ SDK 产品之上的附加包，适用于 AM26xx 器件，例如 AM263x/AM263Px/AM261x。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 自动 HSM 栈集成

TIFS-MCU 不是 AUTOSAR-HSM 栈的替代产品。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。

表 1. 基于 HSSE 的安全启动支持的特性列表（由 ROM 支持）

安全引导的特性	支持的算法 (AM263x/AM263Px)	支持的算法 (AM261x)	在 10.02.00 能提供支持
HSM Run Time 固件引导	• 证书验证 • RSA-4K • 解密支持 • AES-CBC-256	• 证书验证 • RSA-4K • ECDSA (secp256r1) • ECDSA (secp384r1) • ECDSA (secp521r1) • ECDSA (brainpool512r1) • 解密支持 • AES-CBC-256	是
SBL 引导	• 证书验证 • RSA-4K • 解密支持 • AES-CBC-256	• 证书验证 • RSA-4K • ECDSA (secp256r1) • ECDSA (secp384r1) • ECDSA (secp521r1) • ECDSA (brainpool512r1) • 解密支持 • AES-CBC-256	是

表 2. 基于 HSSE 的安全启动支持的特性列表（TIFS-MCU 支持）

安全引导的特性	支持的算法 (AM263x)	支持的算法 (AM263Px)	支持的算法 (AM261x)	在 10.02.00 能提供支持
基于 RAM 的多核应用程序通过根密钥引导	• 证书验证 • RSA-4K • 解密支持 • AES-CBC-256	• 证书验证 • RSA-4K • 解密支持 • AES-CBC-256	• 证书验证 • RSA-4K • ECDSA (secp256r1) • ECDSA (secp384r1) • ECDSA (secp521r1) • ECDSA (brainpool512r1) • 解密支持 • AES-CBC-256	是
基于 XiP 的多核应用程序通过根密钥引导	• AM263x 上不支持 XiP	• 通过根密钥支持 MAC • AES-GCM-128 • 通过根密钥支持解密 • AES-CTR-128	• 通过根密钥支持 MAC • AES-GCM-128 • 通过根密钥支持解密 • AES-CTR-128	是
基于 RAM 的多核应用程序通过辅助密钥引导	• 证书验证（使用不同的 SHA 选项） • RSA-4K • ECDSA (secp256r1) • ECDSA (secp384r1) • ECDSA (secp521r1) • ECDSA (brainpool512r1) • 解密支持 • AES-CBC-256	• 证书验证（使用不同的 SHA 选项） • RSA-4K • ECDSA (secp256r1) • ECDSA (secp384r1) • ECDSA (secp521r1) • ECDSA (brainpool512r1) • 解密支持 • AES-CBC-256	• 证书验证（使用不同的 SHA 选项） • RSA-4K • ECDSA (secp256r1) • ECDSA (secp384r1) • ECDSA (secp521r1) • ECDSA (brainpool512r1) • 解密支持 • AES-CBC-256	是

表 2. 基于 HSSE 的安全启动支持的特性列表（TIFS-MCU 支持）（续）

安全引导的特性	支持的算法 (AM263x)	支持的算法 (AM263Px)	支持的算法 (AM261x)	在 10.02.00 能提供支持
基于 XiP 的多核应用程序通过辅助密钥引导	• AM263x 上不支持 XiP	• 通过辅助密钥支持 MAC • AES-GCM-128 • 通过辅助密钥支持解密 • AES-CTR-128	• 通过辅助密钥支持 MAC • AES-GCM-128 • 通过辅助密钥支持解密 • AES-CTR-128	是

有关 AM26x 器件安全启动时间的更多详细信息、请参阅链接列表。

表 3. 安全编程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 10.02.00
SBL Keywriter	示例	AM263X_RESTRICTED_SECURITY	安全资源	是
		AM263PX_RESTRICTED_SECURITY		
		AM261x-TIFS-SDK		
Uart 引导加载程序	面向如下系统的工具 - • Windows • Linux • MacOS	MCU_PLUS_SDK	ti.com	是
Uart Uniflash	面向如下系统的工具 - • Windows • Linux • MacOS	MCU_PLUS_SDK	ti.com	是
OTP 密钥编写器证书生成	Python 工具	AM263X_RESTRICTED_SECURITY	安全资源	是
		AM263PX_RESTRICTED_SECURITY		
		AM261x-TIFS-SDK		
OTP KW HSM 固件	使用 TI 密钥进行加密和签名	AM263X_RESTRICTED_SECURITY	安全资源	否
		AM263PX_RESTRICTED_SECURITY		
		AM261x-TIFS-SDK		
SBL 和 HSM 签名工具	Python 工具	MCU_PLUS_SDK	安全资源	是
应用程序签名工具	Python 工具	MCU_PLUS_SDK	安全资源	是

TIFS-MCU 提供的本机服务

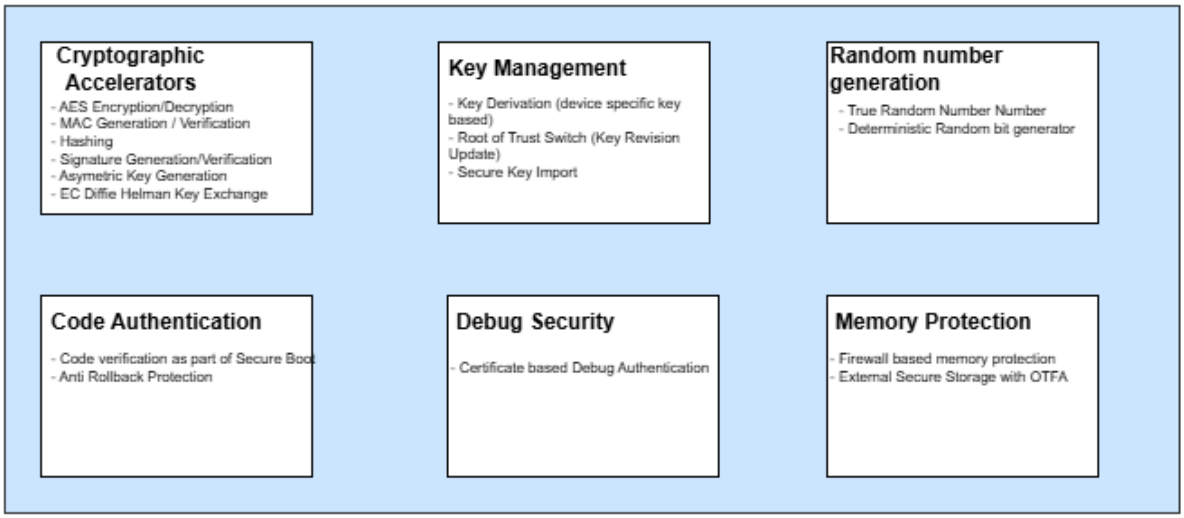

图 2. AM26x 器件 TIFS-SDK 的顶级安全特性

TIFS-MCU 的软件方框图

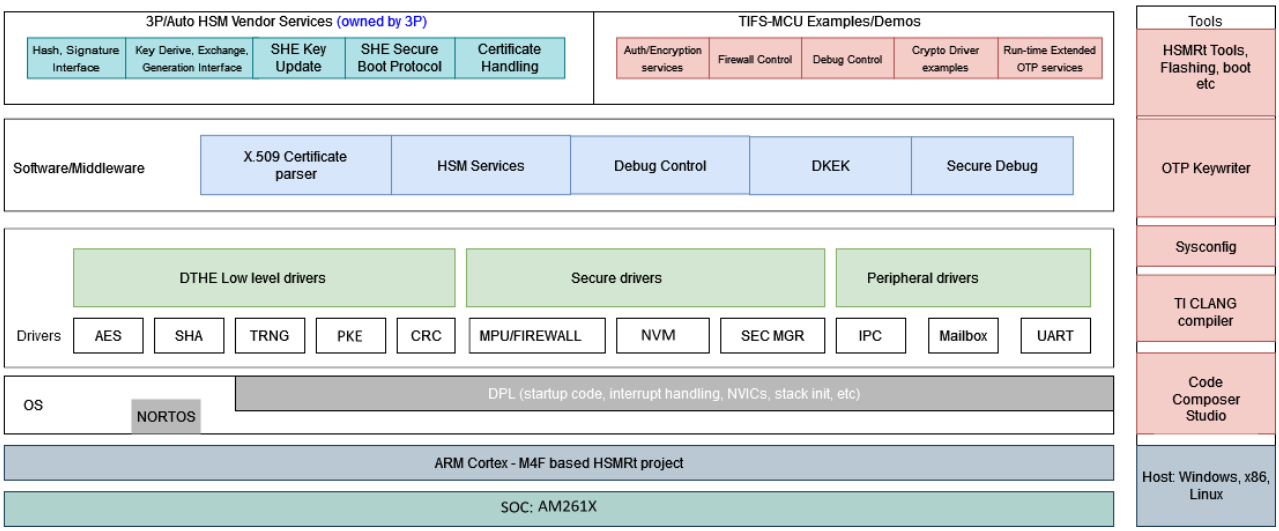

图 3. AM261x SW 方框图

表 4. 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。

表 4. TIFS-MCU 软件组件（续）

TIFS-MCU 软件组件	说明
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 • 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 运行时防火墙服务 • HSM 扩展 OTP 服务 • HSM 防回滚服务 • HSM 信任交换机服务根 • HSM 处理器认证启动服务（单个/流式） • HSM 密钥导入服务 • HSM OTFA 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）

表 4. TIFS-MCU 软件组件（续）

TIFS-MCU 软件组件	说明
示例和演示	
示例和演示	*HSM 示例列表：* • HSM 获取版本示例 • 调试身份验证示例 • 扩展 OTP 示例 • 运行时间防火墙示例 • 防火墙中断服务示例 • 防回滚示例 • 推导出的 KEK 示例 • RNG 示例 • 加密/解密加密示例 • 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，R5F
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
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-SE 以建立客户信任根。
TIFS-MCU 工具	为了能使用所提供的服务而需要的工具和脚本

表 5. 10.02 版支持 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 运行时防火墙服务	TIFS-MCU 提供该服务以便仅对由 HSM 控制的系统防火墙进行编程以实现保护、隔离等	是
HSM 扩展 OTP 服务	TIFS-MCU 提供该服务以便对通用或用户定义的 OTP 行编程进行编程。	是
HSM 防回滚服务	TIFS-MCU 提供此服务以对 eFuse 中的软件版本进行编程，以防止系统中以前的软件反回滚。	是
HSM 信任交换机服务根	TIFS-MCU 提供此服务以将信任根交换机从主密钥更改为备份密钥。	是
HSM 处理器授权启动服务	TIFS-MCU 提供 Proc Auth 启动服务以对使用根密钥或辅助密钥签名的应用程序映像进行身份验证和解密。	是（*MCU+ SDK 中 SBL 的一部分*）
HSM 密钥导入服务	TIFS-MCU 提供密钥导入服务以将辅助密钥导入系统。	是（*MCU+ SDK 中 SBL 的一部分*）
HSM OTFA 服务	TIFS-MCU 提供 OTFA 服务，以基于根密钥和辅助密钥配置 OTFA 区域。	是（*MCU+ SDK 中 SBL 的一部分*）

表 6. 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 • EDMA 模式（轮询）	是	
AES MAC 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 • EDMA 模式（轮询）	是	
SHA Hasing 算法	• SHA256，SHA512 • HMAC SHA-256、HMAC SHA-512 • 单次 + 流模式 • CPU 轮询模式 • EDMA 模式（轮询）	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 6. 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
RSA 密钥生成服务	• RSA 2048、3072、4096 位 • CPU 轮询模式	示例仅包含 4096 位密钥 *（仅适用于 AM261x）*	
ECDSA 签名和验证	• SECP256、SECP384、SECP521 • BRAINPOOL-P512 • CPU 轮询模式	是	
ECDSA 密钥生成服务	• 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	• SECP256、SECP384、SECP521 • BRAINPOOL-P512 • CPU 轮询模式	是 *（仅适用于 AM261x）*	

5.1 NIST 标准和参考列表

- *AM263x、AM263Px、AM261x 的引导时间计算器*
- *FIPS Pub. 197：“发布高级加密标准 (AES)”*
- *[NIST-SP800-38A] “块密码运行模式建议：方法和技巧”*
- *[GCM] 伽罗瓦/计数器操作模式 (GCM)，2005 年 5 月 31 日*
- *[CCM] “具有 CBC-MAC (CCM) 的计数器- AES 运行模式”*
- *FIPS Pub. 180-4: 安全散列标准，NIST*
- *FIPS Pub. 198-1: 锁定哈希消息验证码 (HMAC)，2008 年 7 月*

6 有效器件列表

- AM2631
- AM2631-Q1
- AM2632
- AM2632-Q1
- AM2634
- AM2634-Q1
- AM263P2
- AM263P4
- AM263P4-Q1
- AM2612

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