Product Overview

F29-TIFS-SDK 產品簡介

軟體產品概覽

F29 裝置中的硬體安全管理器包含多個元件區塊，旨在實現系統安全目標。這類區塊包括各種記憶體、安全管理器、加密加速器引擎、週邊設備模組和安全郵箱。主機 C29 子系統與 HSM 子系統介接，以執行程式碼驗證、安全開機、安全韌體升級和加密運作階段通訊所需的密碼作業。

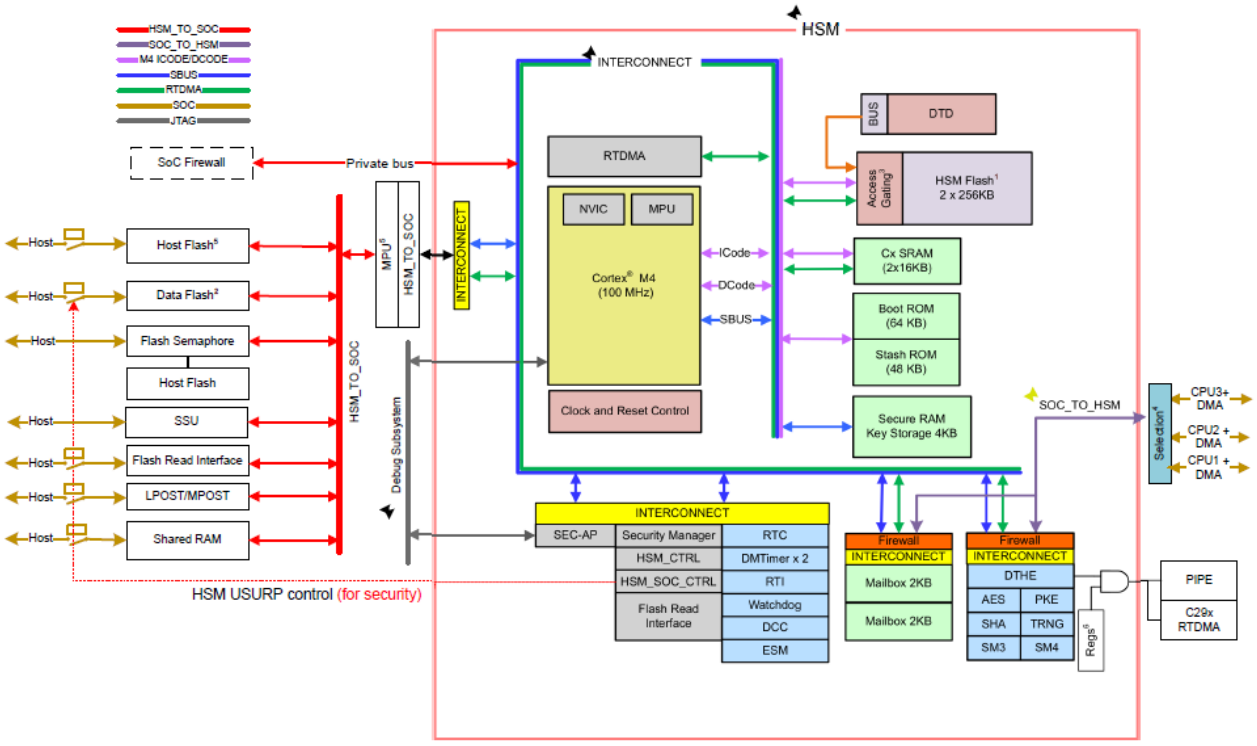


图 1. HSM 原理圖

F29 裝置的安全目標

- 模組和平台保護機制：
  - 保護模組（硬體和軟體），並防止平台被接管或遭到未經授權的修改。
  - 保護關鍵資產和資源免遭硬體和軟體攻擊
- 限制關鍵資產的攻擊面 -
  - 將關鍵資產隔離在受保護的空間中，並嚴格限制存取權限。重點防範特定類別的攻擊。
  - 假設系統的其餘部分遭到入侵，以保護關鍵資產。
- 沙箱安全性：
  - 安全機制在隔離式環境中運作。
  - 即使應用程式模組和任務在同一個 CPU 上執行，也必須彼此安全隔離。
- 分層安全性：
  - 採用多層方法，這樣做不會分散和破壞整個系統的安全性。
  - 各層之間彼此獨立執行。

English Document: SPRT789
Copyright © 2026 Texas Instruments Incorporated

- 安全開發的可追溯性、問責性和隔離性：
  - 必須在隔離式環境中發展安全功能，以避免發生意外問題。
  - 這也是向認證機構和客戶證明安全性所必需的條件。

裝置生命週期和配置流程

*啟用高性能即時控制系統網路安全*中也對該流程進行了說明。

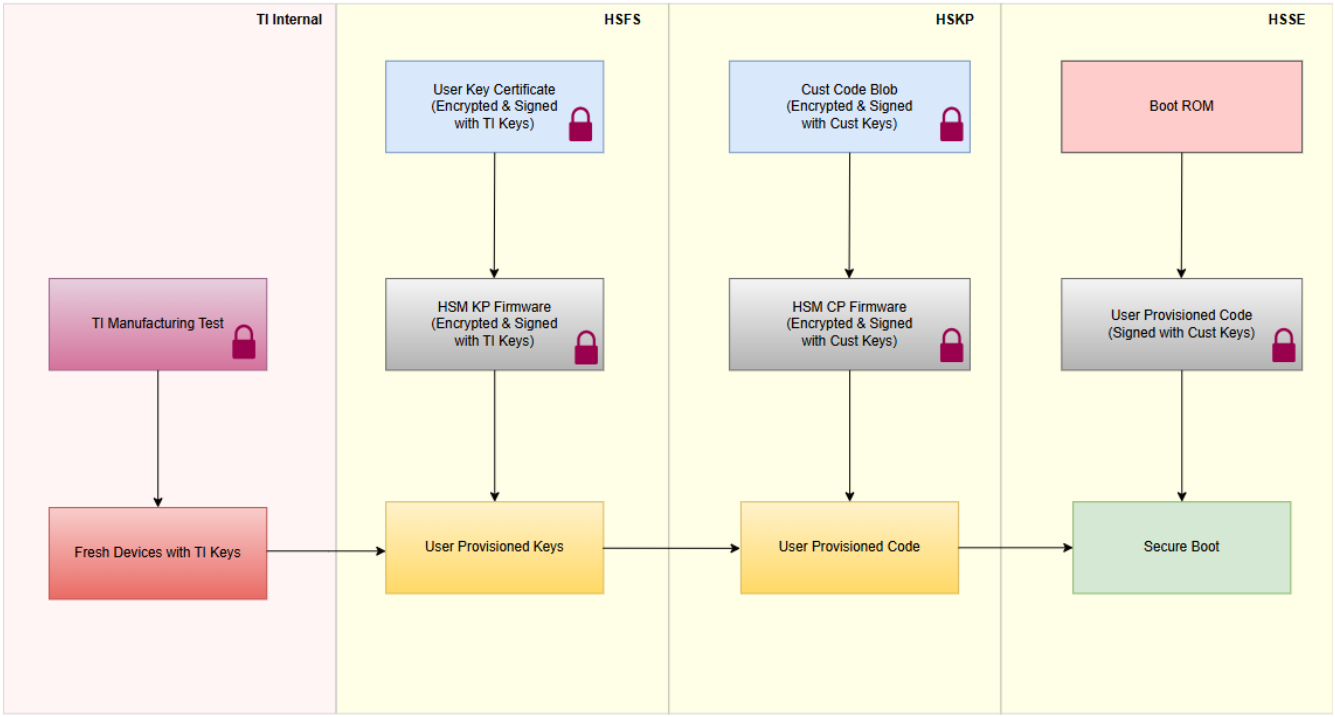


图 2. F29x 裝置配置流程

階段 1：

使用者收到裝置時，裝置處於 HSFS（現場安全）狀態。本裝置包含預先配置的 TI 金鑰。在此狀態下，HSM 核心只會執行使用 TI 金鑰加密並簽名的程式碼。

階段 2：

TI 透過使用金鑰配置套件（在受信任的環境中）來支援使用者金鑰配置，並且使用者金鑰會以 TI 金鑰加密並簽名。接著，透過快閃記憶體核心範例和主機編程工具安全地傳輸此金鑰憑證。使用者金鑰的機密性在整個過程中都會受到保護，即使在不安全的環境中，使用者也可以重複執行此流程。配置使用者加密金鑰後，裝置的生命週期將變更為 HSKP（金鑰已配置）狀態。

English Document: SPRT789
Copyright © 2026 Texas Instruments Incorporated

階段 3：

由於裝置處於 HSKP 狀態，應用程式碼可編程至裝置中。然後，程式碼配置資料會使用使用者金鑰進行加密及簽名。這些資料亦可透過快閃記憶體核心和主機編程工具安全傳輸。預計配置至 HSM 或 C29 快閃記憶體的使用者程式碼，會使用儲存在裝置安全儲存區內的使用者金鑰進行加密及簽名。所有必要影像（例如 HSM 程式碼、C29 程式碼和安全配置 (SecCfg)）配置完畢後，裝置將轉換為 HSSE 狀態。處於 HSSE（安全機制強制執行）狀態的裝置之生命週期，會確保程式碼一律透過安全開機機制啟動。

TI 安全軟體元件

TI 在 TIFS-SDK 中提供 2 種主要軟體元件：

- 一次性可編程 (OTP) 金鑰配置套件
- TI MCU 裝置基礎安全附加套件

TI 的 F29x OTP 金鑰寫入器套件

TI 提供 OTP 金鑰寫入器套件，可將安全裝置的生命週期從 HS-FS（開發變體，未強制執行安全機制）轉換為 HS-KP（臨時生命週期，已配置金鑰）。這些配置流程採用端對端安全保護機制，因此可用於在不安全的工廠車間配置環境佈建。

金鑰配置流程支援的功能清單

以下是 F29x-TIFS-SDK 的 26.01.00LTS 版本支援的功能。

- 提供經簽名的 HSM 金鑰寫入器韌體，可接受 x.509 客戶金鑰憑證並已配置所有快閃記憶體 OTP 欄位。
- 支援透過單次配置的客戶金鑰憑證進行金鑰編程。
- 支援 RSA-4K、ECDSA secp256R1、secp384R1、secp521r1 和基於 brainpool512r1 的金鑰配置。
- 支援透過 UART 模式進行金鑰編程。
- 支援透過 JTAG 模式進行金鑰編程。
- 支援 OpenSSL v3.0.2 及更新版本。
- 加密金鑰（SMEK 和 BMEK）為可選欄位。公共金鑰（SMPK 和 BMPK）為是必填欄位。
- 可選用 Python 指令碼產生 x.509 憑證。
- 以下為是可編程的金鑰：
  - MSV
  - SMPK、SMEK
  - BMPK、BMEK
  - EXT OTP
  - KEY COUNT
  - SWREV-HSM、SWREV-APP、SWREV-SBL、SWREV-SSU
  - KEY REV

English Document: SPRT789
Copyright © 2026 Texas Instruments Incorporated

適用於 MCU 裝置的 TI 基礎軟體

什麼是 TIFS-MCU？

TIFS 是指德州儀器針對 F29x SoC 提供的基礎安全技術。TIFS 提供裝置信任根和基礎安全服務。HSM 即硬體安全模組，由以安全核心為基礎的安全子系統組成。TIFS-MCU 可作為 F29-SDK 產品的附加套件，適用於 F29H85x 和 F29P32x 等 F29x 裝置。TIFS-MCU 可在安全的 CPU 上提供裸機安全堆疊，使用者也能運用此堆疊。

1. 開發裝置信任根並提供基礎安全服務
2. 與第三方 Auto-HSM 堆疊整合。TIFS-MCU 無法替代 AUTOSAR-HSM 堆疊。

TIFS-MCU 可提供基礎安全軟體及在裝置內建立信任根所需的所有基本元件，並利用各種服務。TIFS-MCU 可由 AUTOSAR-HSM 堆疊廠商輕鬆整合，以開發符合 SHE/EVITA 標準的 HSM 堆疊。

TIFS-MCU 中的程式碼配置韌體是什麼？

程式碼配置韌體是 TI 提供的軟體（包括原始碼），可將軟體安全佈建至裝置的內部快閃記憶體中。借助此韌體，即使在不安全的環境中，使用者亦可安全地對 HSM 和 C29 應用程式進行編程。

表 1. 程式碼配置流程支援的功能清單

程式碼配置流程的特點	影像完整性	組模式
HSM 執行時間韌體配置	• RSA-4K 搭配 SHA512 • ECDSA secp256R1 搭配 SHA512 • ECDSA secp384R1 搭配 SHA512 • ECDSA secp521R1 搭配 SHA512 • ECDSA brainpool512R1 搭配 SHA512	所有組模式
C29 CPU1 配置	• RSA-4K 搭配 SHA512 • ECDSA secp256R1 搭配 SHA512 • ECDSA secp384R1 搭配 SHA512 • ECDSA secp521R1 搭配 SHA512 • ECDSA brainpool512R1 搭配 SHA512	所有組模式
安全配置佈建	• RSA-4K 搭配 SHA512 • ECDSA secp256R1 搭配 SHA512 • ECDSA secp384R1 搭配 SHA512 • ECDSA secp521R1 搭配 SHA512 • ECDSA brainpool512R1 搭配 SHA512	所有組模式

English Document: SPRT789
Copyright © 2026 Texas Instruments Incorporated

表 2. 安全程式碼配置流程的軟體交付內容清單

軟體元件清單	軟體類型	OPN	交付位置	26.01.00 LTS 中提供的來源
UART 快閃記憶體核心	範例	F29H85x-SDK	ti.com	是
JTAG 快閃記憶體核心	範例	F29H85x-SDK	ti.com	是
CAN 快閃記憶體核心	範例	F29H85x-SDK	ti.com	是
主機編程工具	適用於以下系統的工具： • Windows • Linux • MacOS	F29H85x-SDK	ti.com	是
OTP Key Writer 憑證產生	Python 工具	F29H85x-TIFS-SDK	安全資源	是
HSM KP 韌體	加密韌體	F29H85x-TIFS-SDK	安全資源	否
HSM CP 韌體	範例	F29H85x-TIFS-SDK	安全資源	是
Cyber Shield 工具套件	Python 工具	Cyber Shield 工具套件	GitHub	是

English Document: SPRT789
Copyright © 2026 Texas Instruments Incorporated

TIFS-MCU SDK 提供哪些功能？

TIFS-MCU SDK 提供開箱即用的服務和範例 HSM 韌體，展示在 HSM 子系統中執行的使用案例。

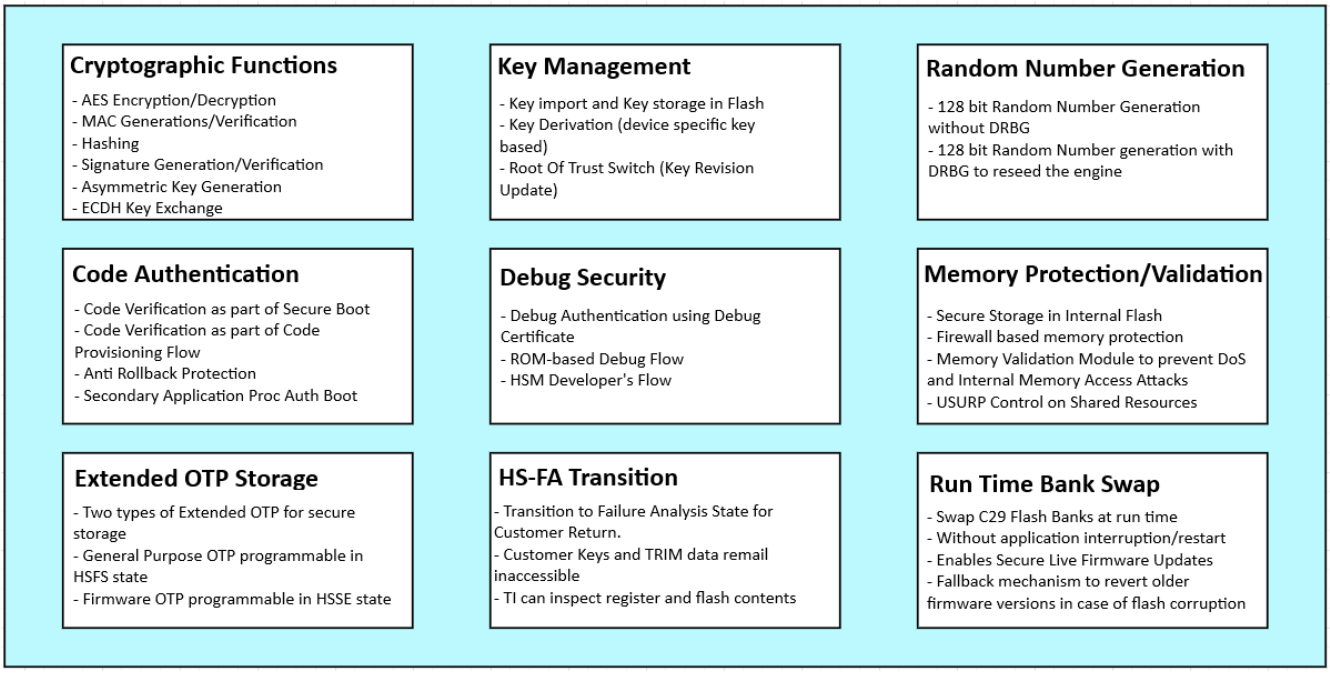


图 3. TIFS-MCU 提供的原生服務

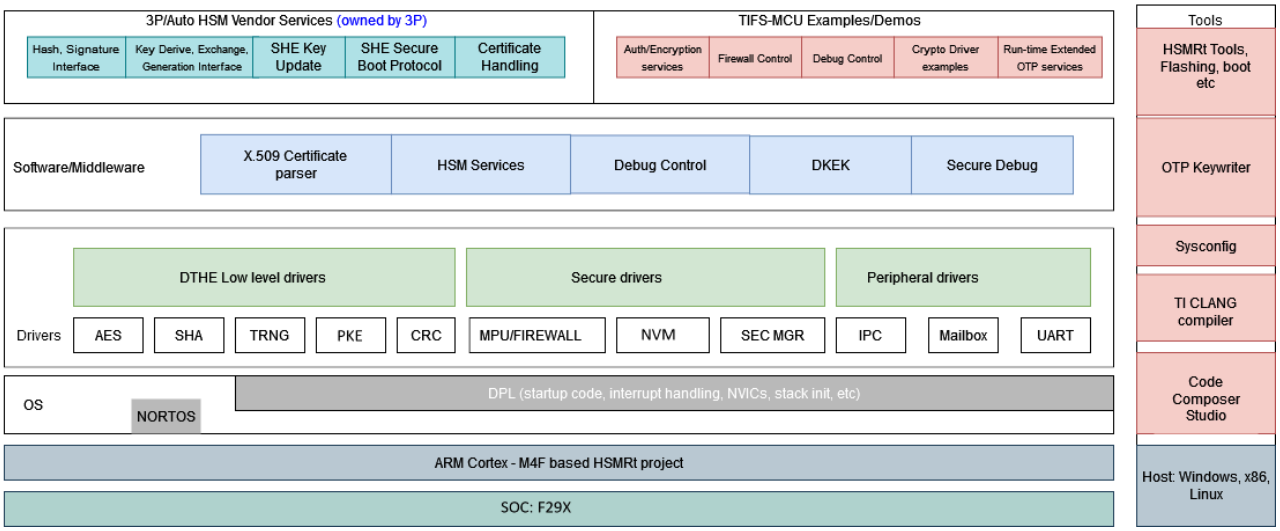


图 4. TIFS-MCU 的軟體架構原理圖

English Document: SPRT789
Copyright © 2026 Texas Instruments Incorporated

表 3. TIFS-MCU 軟體元件

TIFS-MCU 軟體元件	說明
OS 核心	
無 RTOS	包含實作非 RTOS 執行環境的模組，此環境由計時器、ISR、主執行緒組成。允許上層軟體以裸機模式執行。**注：HSM 伺服器僅在 NORTOS 中受支援。**
驅動程式移植層 (DPL)	驅動器用來抽象化作業系統環境的 API。例如：旗號、硬體中斷、互斥鎖、時鐘。
安全裝置驅動器和模組	
TIFS-MCU 週邊設備驅動器	適用於 HSM 的裝置驅動器函式庫和 API。 *SOC 週邊設備驅動器清單：* • HSM MBOX 和安全 IPC • 加密驅動器 • HSM 快閃記憶體、HSM FRI • 安全管理器 • MPU 防火牆 • USURP • 記憶體驗證模組 • HSM RTI • HSM 看門狗
TIFS-MCU 中間件	TIFS-MCU 套件支援的 TIFS-MCU 中間件 *中間件清單：* • HSM 伺服器 • HSM 記憶體日誌 • ASN1 剖析器和憑證剖析器 • 金鑰衍生 • 加密介面
TIFS-MCU 服務	TIFS-MCU 套件中支援的 HSM 服務 *HSM 服務清單：* • HSM 獲取版本服務 • HSM GET UID 服務 • HSM 執行時間偵錯驗證服務 • HSM 派生 KEK 服務 • HSM 隨機數產生服務 • HSM 擴展 OTP 服務 • HSM 防回復服務 • HSM 信任根交換服務 • HSM 安全韌體更新服務 • HSM 獲取裝置配置服務 • HSM 加密服務 • HSM 處理器驗證開機服務 • HSM 活動到休眠快閃記憶體組復制服務 • HSM 執行時間組交換服務 • HSM 金鑰環匯入服務 • HSM HS-FA 轉換服務
TIFS-MCU 韌體	已啟用所有上述服務的 TIFS-MCU 韌體開箱即用範例實作

English Document: SPRT789
Copyright © 2026 Texas Instruments Incorporated

表 3. TIFS-MCU 軟體元件（續）

TIFS-MCU 軟體元件	說明
範例與示範	
範例與示範	*HSM 範例清單：* • 組合服務演示，用於展示所有 HSM 服務 • 開機管理器，用於演示快閃記憶體開機模式下的安全韌體固件更新 • 加密/解密加密範例 • 雜湊加密範例 • 不對稱加密範例 • CPU3 安全開機範例 • 安全即時韌體更新範例 • HS-FA 轉換示例
工具（在主機上使用）	
Code Composer Studio (CCS)	用於建立專案、對程序偵錯的 IDE
TI CLANG 編譯器工具鏈	TI 適用於 ARM M4F 的 Clang 型 ARM 編譯器
TI C29-CGT 工具鏈	TI 適用於 C29 編譯器的 Clang 型 C29 架構
SysConfig	系統配置工具，用於配置週邊設備、PinMux、時鐘，以及產生系統初始化程式碼
SDK 工具和公用程式	其他工具和公用程式，例如快閃記憶體工具、開機工具、SDK 開發流程使用的 CCS 載入指令碼
OTP Keywriter	OTP Keywriter 用於將客戶金鑰整合至裝置中，並將 HS-FS 轉換為 HS-KP，以建立客戶信任根。
TIFS-MCU 工具	可利用透過 TIFS-MCU 所提供服務的工具和指令碼。

表 4. 支援的 HSM 服務

服務	說明	可用範例
HSM 獲取版本服務	HSM GetVersion 服務旨在取得當前的 TIFS-MCU 韌體版本	是
HSM GET UID 服務	當 TIFS-MCU 韌體收到來自 HSM 伺服器的 GetUID 要求時，UID 會從安全記憶體復制到使用者所要求的輸出記憶體位置。	是
HSM 執行時間偵錯驗證服務	如要在執行時解鎖偵錯埠，您需要使用活動信任根私密金鑰簽名的 X509 憑證。此服務用於為 TIFS-MCU 韌體提供簽名憑證以進行處理。	是
HSM 派生 KEK 服務	TIFS-MCU 提供此服務，以根據某些輸入常數獲取派生的 KEK。 • 此金鑰對於每部裝置均為唯一，並被保密。 • 此金鑰不能以任何方式從硬體中擷取。	是
HSM 隨機數產生服務	TIFS-MCU 提供此服務，以從給定的輸入常數中獲取隨機數。	是
HSM 擴展 OTP 服務	TIFS-MCU 提供對通用 OTP 區域進行編程的服務，這些區域是可針對使用者使用模型定義的 OTP 快閃記憶體位元陣列。	是
HSM 防回復服務	TIFS-MCU 提供防回復服務，有助防止啟動較舊的軟體影像。該裝置具有 OTP 欄位，用於儲存 SBL、HSMRt、SECCFG 和應用程式影像的軟體修訂版。	是
HSM 信任根交換服務	TIFS-MCU 提供安全的 RoT 切換功能，可從次要金鑰切換至備用金鑰。 SoC 中存在兩個信任根金鑰：次要金鑰 (SMPK/SMEK) 和備用金鑰 (BMPK/BMEK)。如果次要金鑰遭洩露，攻擊者即可控制整個 SoC。	是
HSM 韌體更新服務	TIFS-MCU 提供安全的韌體更新服務，內容包含憑證驗證流程、針對信任根金鑰進行驗證，以及在整個流程中維護影像的完整性。	是
HSM 獲取裝置配置服務	TIFS-MCU 提供獲取裝置配置服務，可讀取開機期間由 HSM-ROM 載入至資產（安全 RAM）的裝置配置，以及其他僅限 HSM CPU 存取的硬體配置。	是
HSM 加密服務	TIFS-MCU 提供加密服務，可安全地產生並驗證加密消息驗證程式碼，以進行身份驗證並確保資料完整性。支援 CMAC、HMAC 和 GMAC。	是
HSM 處理器驗證開機服務	TIFS-MCU 使用金鑰環中提供的客戶信任根金鑰，為應用程式二進位和 Sec-Cfg 影像提供驗證服務。	是
HSM 活動到休眠快閃記憶體組復制服務	TIFS-MCU 提供用於將活動快閃記憶體組內容複製到休眠快閃記憶體組的服務，該服務可用於將主快閃記憶體組的內容從活動快閃記憶體組複製到 C29 CPU1、C29 CPU3 和 HSM CPU 的休眠快閃記憶體組	是

English Document: SPRT789
Copyright © 2026 Texas Instruments Incorporated

表 4. 支援的 HSM 服務（續）

服務	說明	可用範例
HSM 執行時間組交換服務	TIFS-MCU 提供執行階段切換 C29 快閃記憶體組的服務，無須重新啟動裝置即可完成切換。此功能可用於安全即時韌體更新，也可作為備援機制，在快閃記憶體資料損毀時回復至較舊版本的韌體	是
HSM 金鑰環匯入服務	TIFS-MCU 提供不對稱和對稱金鑰儲存服務，使用者可藉此擴展信任根。該服務可匯入公共金鑰、私密金鑰、對稱金鑰和自訂資料，而這些資料皆包含於由目前活動的信任根簽名的 x509 憑證中。	是
HSM HS-FA 轉換服務	TIFS-MCU 提供裝置生命週期狀態轉換服務，可將裝置從 HS-SE（安全機制強制執行）狀態永久轉換為 HS-FA（故障分析）狀態。此轉換不可逆，並在裝置 OTP 中永久設定故障分析啟用位元。	是

表 5. 受支援的加密硬體加速器和模式

加密核心	軟體驅動器中提供的支援	可用範例	技術規格
AES 加密和解密	• 128,192 和 256 位元金鑰 • ECB、CBC、CCM、CTR、CFB、GCM、OFB、XTS • 單次 + 串流模式 • CPU 輪詢模式 • RTDMA 模式	是	
AES-MAC 產生和驗證	• 128,192 和 256 位元金鑰 • CCM、CBC-MAC、CMAC、GCM • 單次 + 串流模式 • CPU 輪詢模式 • RTDMA 模式	是	
SHA 雜湊演算法	• MD5、SHA-1、SHA2-224、SHA2-256、SHA2-384、SHA2-512 • HMAC SHA-256、HMAC SHA-512 • 單次 + 串流模式 • CPU 輪詢模式 • RTDMA 模式	是	
SM3 雜湊演算法散列算法	• SM3-512 • CPU 輪詢模式 • RTDMA 模式	是	
SM4 加密和解密	• CBC、CFB、CTR、ECB、OFB • CPU 輪詢模式 • RTDMA 模式	是	
RSA 加密和解密簽名和驗證	• RSA 2048、3072、4096 位元 • RSA PKCS1_5、PSS2_1 • CPU 輪詢模式	是	
ECDSA 簽名和驗證	• SECP256、SECP384、SECP521 • BRAINPOOL-P512 • CPU 輪詢模式	是	
EDDSA 簽名和驗證	• ED25519 • CPU 輪詢模式	是	
ECDH Diffie Helman 金鑰交換	• SECP256、SECP384、SECP521 • BRAINPOOL-P512 • CPU 輪詢模式	是	

English Document: SPRT789
Copyright © 2026 Texas Instruments Incorporated

有效裝置清單

- F29H85x
- F29P32x

English Document: SPRT789
Copyright © 2026 Texas Instruments Incorporated

重要聲明與免責聲明

TI 以「現狀」及所含一切錯誤提供技術與可靠數據 (包含產品規格書)、設計資源 (包含參考設計)、應用或其他設計建議、網頁工具、安全資訊和其他資源，且不承擔所有明示或默示保證，包括但不限於適銷性或用於特定用途之適用性的任何默示保證，或不侵害第三方智慧財產的任何默示保證。

所述資源可供專業開發人員應用 TI 產品進行設計使用。您應自行負責 (1) 選擇適合您應用的 TI 產品，(2) 設計、驗證與測試您的應用，與 (3) 確保應用符合適用標準，以及任何其他安全、安保、法規或其他要求。

這些資源得進行修改且無需通知。TI 對您使用所述資源的授權僅限於開發資源所涉及 TI 產品的相關應用。除此之外不得複製或展示所述資源，也不提供其它 TI 或任何第三方的智慧財產權授權許可。如因使用所述資源而產生任何索賠、賠償、成本、損失及債務等，TI 對此概不負責，並且您須賠償由此對 TI 及其代表造成的損害。

TI 的產品均受 TI 的銷售條款 、TI 的通用品質指南 或 ti.com 上其他適用條款，或連同這類 TI 產品提供之適用條款所約束。TI 提供此等資源並不會擴大或以其他方式改變 TI 對於 TI 產品的適用保證或保證免責聲明。 除非 TI 明確將某產品指定為自訂或客戶指定型號，否則 TI 產品均為標準、類比、通用裝置。

TI 反對並拒絕您可能提出的任何附加或不同條款。

Copyright © 2026, Texas Instruments Incorporated

上次更新 10/2025

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.

Copyright © 2026, Texas Instruments Incorporated

Last updated 10/2025