*Product Overview*

# *F29-TIFS-SDK Product Brief*

## Software Product Overview

The Hardware Security Manager in F29 devices contains several component blocks designed to achieve system security objectives. These include various memories, the Security Manager, cryptographic accelerator engines, peripheral modules, and the secure mailbox. The host C29 subsystem interfaces with the HSM subsystem to perform the cryptographic operations required for code authentication, secure boot, secure firmware upgrades and encrypted run-time communications.

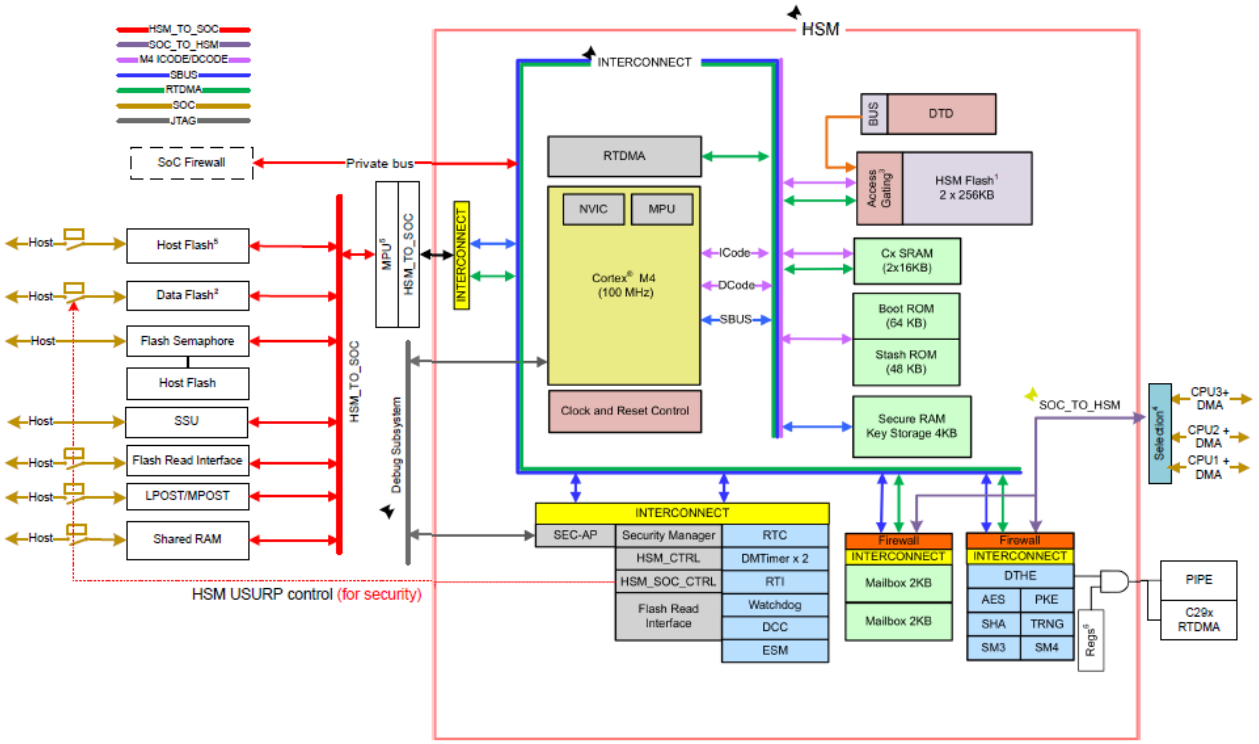


**Figure 1. HSM Block Diagram**

### Security Goals of F29 devices

- Modules and platform protection:
  - Protect modules (hardware and software) and defend platform from takeover and unauthorized modifications.
  - Protect critical assets and resources from hardware and software attacks
- Limit the attack surface for critical assets -
  - Isolate critical assets in protected space with heavily restricted access. Focus on protection against class-based attacks.
  - Assume rest of system is compromised to protect critical assets.
- Sand-box security:
  - Security operates in isolated environment.
  - Application modules and tasks are securely isolated from each other, even on the same CPU.



Copyright © 2026 Texas Instruments Incorporated

- Layered security:
  - Multi-tier approach, such that compromises do not spread and break the entire system security.
  - Each tier operates in isolation with other tiers.
- Traceability, accountability and isolation for security development:
  - Security must be developed in isolated environment so that unexpected issues can be avoided.
  - This is also required to prove security to certification entities and customers.

## Device Lifecycle and Provisioning Flow

The flow is also explained in *Enabling Cybersecurity for High Performance Real-Time Control Systems*.

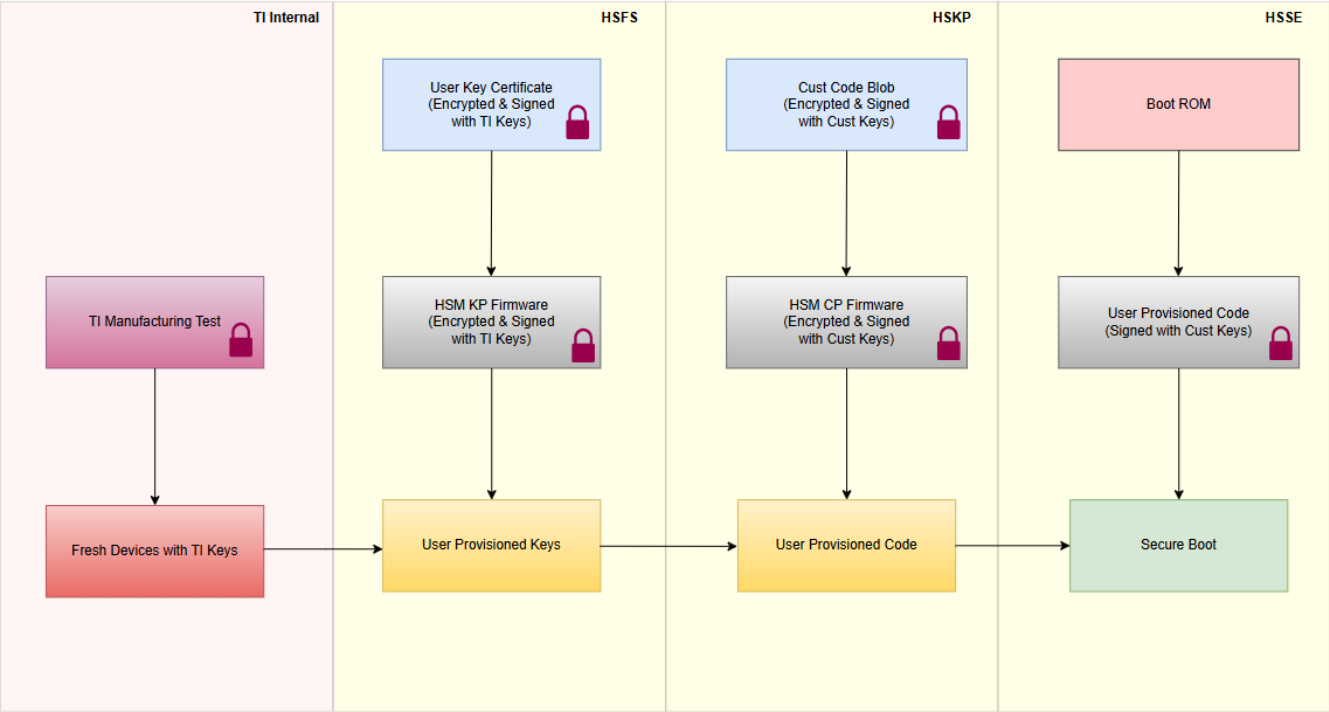


**Figure 2. F29x Device Provisioning Flow**

*Stage 1:*

User is delivered the device in HSFS (Field Secure) state. The device contains TI keys provisioned. In this state, the HSM core only executes a code which is encrypted and signed with TI keys.

*Stage 2:*

TI supports provisioning of user keys by using a key provisioning package (in a trusted environment), with user keys encrypted and signed using the TI keys. This key certificate is then securely transmitted using the flash kernel example and host programmer tool. Confidentiality of the user keys is maintained throughout the process that allows users to replicate the process even in a non-secure environment. Once user encryption keys are provisioned, the life-cycle of the device is changed to HSKP (Key Provisioned) state.



Copyright © 2026 Texas Instruments Incorporated

*Stage 3:*

Now as the device is in HSKP state, the application code can be programmed into the device. The code provisioning is then encrypted and signed with user keys. This is also securely transmitted using the flash kernel and the host programmer. The user code which is supposed to be provisioned into the HSM or C29 flash is encrypted and signed using the user keys that are available in the device secure storage. Once all the required images for example HSM Code, C29 Code, and Secure Config (SecCfg) are provisioned, the device is converted to HSSE state. HSSE (Security Enforced) life-cyle of device maintains that the code is always a secure boot.

### TI Security software components

TI delivers 2 primary software components as part of TIFS-SDK:

- One-Time Programmable (OTP) Key Provisioning Package
- TI-Foundational Security for MCU devices Add-on Package

## TI's F29x OTP Key Writer Package

TI provides a OTP Key Writer package which enables the transitioning of the Secure device life cycle from HS-FS (development variant without security enforcement) to HS-KP (temporary lifecycle with key provisioned). These provisioning flows are end-to-end secured and can be utilized for non-secure factory floor provisioning.

### List of Features Supported by Key Provisioning Flow

*This is the support available in 26.01.00LTS release of F29x-TIFS-SDK.*

- Signed Key writer firmware for HSM which accepts x.509 customer keys certificate with all Flash OTP fields configured.
- Supports programming keys at one-pass customer key certificates.
- Supports RSA-4K, ECDSA secp256R1, secp384R1, secp521r1, brainpool512r1 based Key Provisioning.
- Supports UART mode for key programming.
- Supports JTAG mode for key programming.
- Supports OpenSSL v3.0.2 and above.
- Encryption keys (SMEK and BMEK) are made optional. Public keys (SMPK and BMPK) are mandatory fields.
- Option of using Python script for generating x.509 certificate.
- Following are the keys programmable:
  - MSV
  - SMPK, SMEK
  - BMPK, BMEK
  - EXT OTP
  - KEY COUNT
  - SWREV-HSM, SWREV-APP, SWREV-SBL, SWREV-SSU
  - KEY REV


Copyright © 2026 Texas Instruments Incorporated

# TI Foundational Software for MCU Devices

## What is TIFS-MCU ?

TIFS stands for Texas Instruments Foundational Security for F29x SoCs. TIFS provides device root of trust and foundational security services. The HSM or hardware security module consists of a secure core based secure subsystem. TIFS-MCU serves as an add-on package on top of F29-SDK offering for F29x devices like F29H85x and F29P32x. TIFS-MCU enables a bare metal security stack on secure CPU that can be leveraged by the user too.

1. Develop device root of trust and provide foundational security services
2. Integrate with 3P Auto-HSM stacks TIFS-MCU is not a replacement for AUTOSAR-HSM stack.

TIFS-MCU enables foundational security SW with all the building blocks required for root-of-trust within the device and utilizes various services. TIFS-MCU can be easily integrated by AUTOSAR-HSM stack vendors to develop HSM stacks that adhere to SHE/EVITA standards.

## What is Code Provisioning Firmware in TIFS-MCU ?

Code Provisioning firmware is TI delivered software (including source) which enables secure provisioning of software into the internal flash of the device. This allows users to program HSM as well as C29 applications securely even in non-secure environment.

**Table 1. List of Features Supported by Code Provisioning Flow**

| Features of Code Provisioning Flow | Image Integrity | Bank Mode |
|---|---|---|
| HSM Run Time Firmware Provisioning | • RSA-4K with SHA512<br>• ECDSA secp256R1 with SHA512<br>• ECDSA secp384R1 with SHA512<br>• ECDSA secp521R1 with SHA512<br>• ECDSA brainpool512R1 with SHA512 | All Bank Modes |
| C29 CPU1 Provisioning | • RSA-4K with SHA512<br>• ECDSA secp256R1 with SHA512<br>• ECDSA secp384R1 with SHA512<br>• ECDSA secp521R1 with SHA512<br>• ECDSA brainpool512R1 with SHA512 | All Bank Modes |
| Secure Config Provisioning | • RSA-4K with SHA512<br>• ECDSA secp256R1 with SHA512<br>• ECDSA secp384R1 with SHA512<br>• ECDSA secp521R1 with SHA512<br>• ECDSA brainpool512R1 with SHA512 | All Bank Modes |



Copyright © 2026 Texas Instruments Incorporated

**Table 2. List of Software Deliverables for Secure Code Provisioning Flow**

| List of Software Components | Software Type | OPN | Delivery Location | Source Available in 26.01.00 LTS |
|---|---|---|---|---|
| UART Flash Kernel | Example | F29H85x-SDK | ti.com | Yes |
| JTAG Flash Kernel | Example | F29H85x-SDK | ti.com | Yes |
| CAN Flash Kernel | Example | F29H85x-SDK | ti.com | Yes |
| Host Programmer | Tool for:<br>• Windows<br>• Linux<br>• MacOS | F29H85x-SDK | ti.com | Yes |
| OTP Key Writer Certificate Generation | Python tool | F29H85x-TIFS-SDK | Secure Resources | Yes |
| HSM KP firmware | Encrypted Firmware | F29H85x-TIFS-SDK | Secure Resources | No |
| HSM CP firmware | Example | F29H85x-TIFS-SDK | Secure Resources | Yes |
| Cyber Shield Toolkit | Python tool | Cyber Shield Toolkit | GitHub | Yes |


Copyright © 2026 Texas Instruments Incorporated

## What is available in the TIFS-MCU SDK ?

TIFS-MCU SDK offers out-of-box services and example HSM firmware showcasing use cases which execute in HSM subsystem.

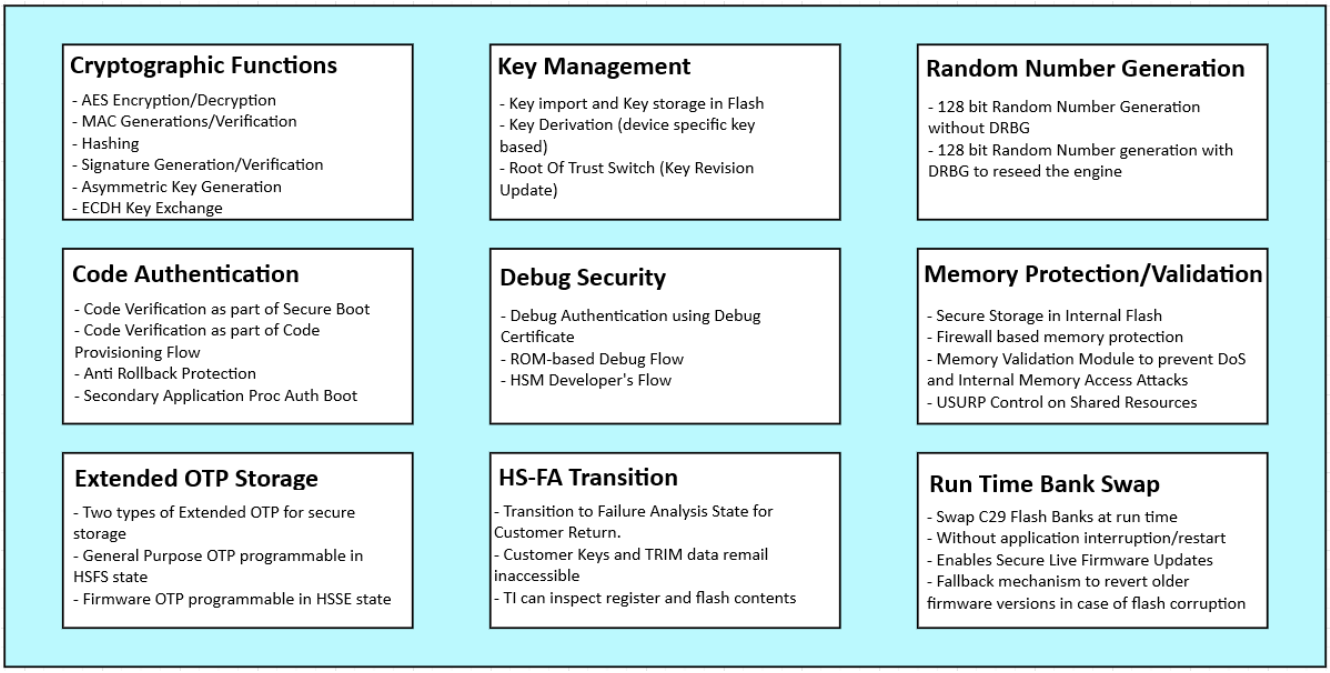


**Figure 3. Native Services Provided by TIFS-MCU**

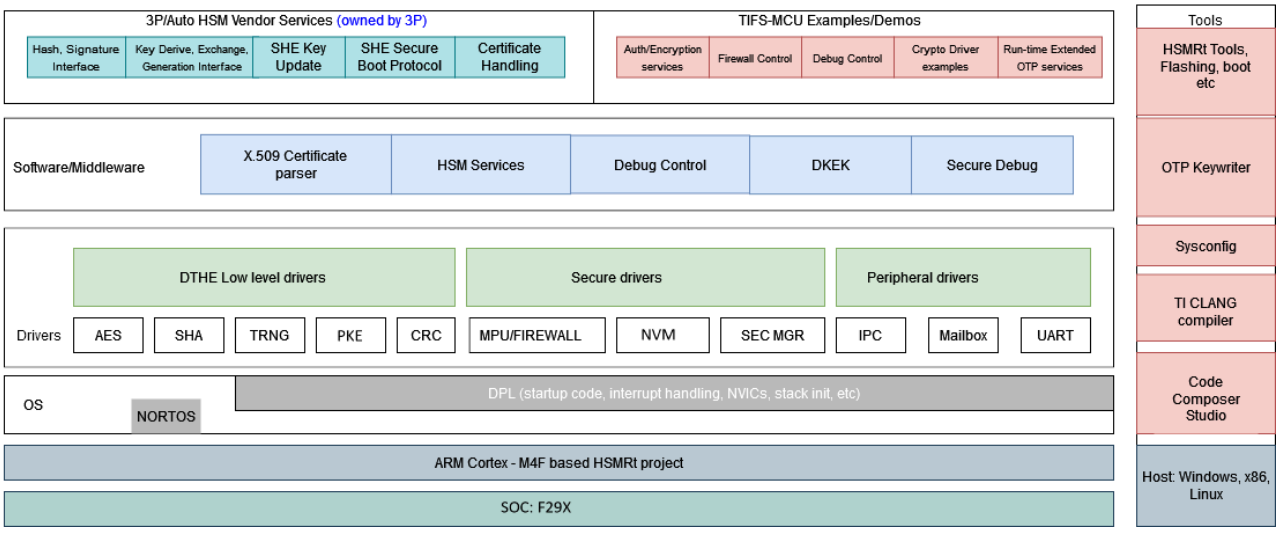


**Figure 4. Software Architecture Block Diagram of TIFS-MCU**



Copyright © 2026 Texas Instruments Incorporated

**Table 3. TIFS-MCU Software Components**

| TIFS-MCU Software Components | Description |
|---|---|
| **OS Kernel** | |
| No RTOS | Contains modules which implement no-RTOS execution environment consisting of timers, ISR, main thread. Allows software on top to run in bare metal mode. **Note - HSM Server is only supported in NORTOS.** |
| Driver Porting Layer (DPL) | APIs used by drivers to abstract the OS environment. Example, Semaphore, HW interrupts, mutex, clock. |
| **Security Device Drivers and Modules** | |
| TIFS-MCU Peripheral Drivers | Device Drivers library and APIs for HSM.<br>*List of SOC Peripheral Driver:*<br>• HSM MBOX and Secure IPC<br>• Crypto Drivers<br>• HSM Flash, HSM FRI<br>• Security Manager<br>• MPU Firewall<br>• USURP<br>• Memory Validation Module<br>• HSM RTI<br>• HSM Watchdog |
| TIFS-MCU Middle-ware | TIFS-MCU middle-ware that are supported in TIFS-MCU package<br>*List of Middle-ware:*<br>• HSM Server<br>• HSM Memory Log<br>• ASN1 Parser and Certificate Parser<br>• Key Derivation<br>• Crypto Interface |
| TIFS-MCU Services | HSM Services that are supported in TIFS-MCU package<br>*List of HSM Services:*<br>• HSM Get Version Service<br>• HSM Get UID Service<br>• HSM Run Time Debug Authentication Service<br>• HSM Derived KEK Service<br>• HSM Random Number Generate Service<br>• HSM Extended OTP Services<br>• HSM Anti Rollback Services<br>• HSM Root of Trust Switching Services<br>• HSM Secure Firmware Update Services<br>• HSM Get Device Config Service<br>• HSM Crypto Services<br>• HSM Proc Auth Boot Service<br>• HSM Active to Dormant Flash Bank Copy Service<br>• HSM Run Time Bank Swap Service<br>• HSM Keyring Import Service<br>• HSM HS-FA Transition Service |
| TIFS-MCU Firmware | Out of Box Example implementation of TIFS-MCU firmware with all the mentioned services enabled |


Copyright © 2026 Texas Instruments Incorporated

**Table 3. TIFS-MCU Software Components (continued)**

| TIFS-MCU Software Components | Description |
|---|---|
| **Examples and Demos** | |
| Examples and Demos | *List of HSM Examples:*<br>• Combined Services Demo showcasing all the HSM services<br>• Boot Manager demonstrating Secure Firmware Update in Flash Boot Mode<br>• Encryption/Decryption Cryptographic Examples<br>• Hashing Cryptographic Examples<br>• Asymmetric Cryptographic Examples<br>• CPU3 Secure Boot Example<br>• Secure Live Firmware Update Example<br>• HS-FA Transition Example |
| *Tools (used on host machine)* | |
| Code Composer Studio (CCS) | IDE used to build projects, debug programs |
| TI CLANG Compiler Toolchain | CLANG based ARM compiler from TI for ARM M4F |
| TI C29-CGT Toolchain | CLANG based C29 compiler from TI for C29 CPU |
| SysConfig | System configuration tool, used to configure peripherals, pinmux, clocks and generate system initialization code |
| SDK Tools and Utilities | Additional tools and utilities, like flashing tools, booting tools, CCS loading scripts used with the SDK development flow |
| OTP Keywriter | OTP Keywriter is used to fuse customer keys into the device and convert HS-FS to HS-KP to establish customer root-of-trust. |
| TIFS-MCU tools | Tools and scripts to leverage the services provided via TIFS-MCU. |

**Table 4. HSM Services Supported**

| Services | Description | Examples Available |
|---|---|---|
| HSM Get Version Service | HSM GetVersion service is to get the current TIFS-MCU Firmware version | Yes |
| HSM Get UID Service | When TIFS-MCU Firmware receives a request to GetUID from HSM Server, the UID is copied from secure memory to the output memory location requested by the user. | Yes |
| HSM Run Time Debug Authentication Service | To unlock the debug port during the run-time, you need an X509 certificate signed with active Root of Trust private keys. This service is used to provide the signed certificate to TIFS-MCU Firmware for processing. | Yes |
| HSM Derived KEK Service | TIFS-MCU provides this service to get a derived KEK based on some input constants.<br>• This key is unique for every unit device and is kept secret.<br>• This key cannot be fetched from hardware in any manner. | Yes |
| HSM Random Number Generate Service | TIFS-MCU provides this service to get a random number from the given input constants. | Yes |
| HSM Extended OTP Service | TIFS-MCU provides services to program General Purpose OTP regions which are an array of otp flash bits that can be defined for user usage models. | Yes |
| HSM Anti Rollback Service | TIFS-MCU provides anti-rollback services that help prevent booting older software images. The device has OTP fields to hold software revision for SBL, HSMRt, SECCFG and Application Images. | Yes |
| HSM Root of Trust Switch Service | TIFS-MCU provides Secure RoT Switching to switch to backup keys from the secondary keys.<br>There are two Root of Trust Keys that are present in the SoC: Secondary (SMPK/SMEK) and Backup (BMPK/BMEK). If the secondary key is compromised, the attacker can take the control of the entire SoC. | Yes |
| HSM Firmware Update Service | TIFS-MCU provides secure firmware update service which consists of certificate authentication flow, verification against the root of trust keys and maintain the image integrity of the image throughout the flow. | Yes |
| HSM Get Device Config Service | TIFS-MCU provides get device config service to read device configurations populated by HSM-ROM in Assets (Secure RAM) during boot and also additional hardware configurations which are restricted to HSM CPU. | Yes |



Copyright © 2026 Texas Instruments Incorporated

**Table 4. HSM Services Supported (continued)**

| Services | Description | Examples Available |
|---|---|---|
| HSM Crypto Services | TIFS-MCU provides crypto services allowing secure cryptographic Message Authentication Code (MAC) Generation and Verification for authenticated data integrity. CMAC, HMAC and GMAC are supported. | Yes |
| HSM Proc Auth Boot Service | TIFS-MCU provides authentication service for application binary as well as Sec-Cfg images using customer root-of-trust keys available in keyring. | Yes |
| HSM Active to Dormant Flash Bank Copy Service | TIFS-MCU provides a service for copying active flash bank contents to dormant flash bank which can be used to copy contents of MAIN flash region from active flash bank to dormant flash bank for C29 CPU1, C29 CPU3 an HSM CPU | Yes |
| HSM Run Time Bank Swap Service | TIFS-MCU provides a service for swapping C29 flash banks at run time without restarting the device which can be used for Secure Live firmware Updates and as a fallback mechanism to revert older firmware versions in case of flash corruption | Yes |
| HSM Keyring Import Service | TIFS-MCU provides a service for the storage of asymmetric and symmetric keys, allowing an extension of the root of trust. The service imports public keys, private keys, symmetric keys and custom data which are a part of x509 certificate signed by the active root of trust. | Yes |
| HSM HS-FA Transition Service | TIFS-MCU provides a service which allows permanent transitioning of a device from HS-SE (Security Enforced) state to HS-FA (Failure Analysis) state. This transition is irreversible and permanently sets the Failure Analysis Enable bit in the device OTP. | Yes |

**Table 5. Crypto HW Accelerators and Modes Supported**

| Crypto Core | Support Available in SW Driver | Examples Available | Specification |
|---|---|---|---|
| AES Encryption and Decryption | • 128,192 and 256 bits Keys<br>• ECB, CBC, CCM, CTR, CFB, GCM, OFB, XTS<br>• One-Shot + Streaming Mode<br>• CPU Polling Mode<br>• RTDMA Mode | Yes | |
| AES-MAC Generation and Verification | • 128,192 and 256 bits Keys<br>• CCM, CBC-MAC, CMAC, GCM<br>• One-Shot + Streaming Mode<br>• CPU Polling Mode<br>• RTDMA Mode | Yes | |
| SHA Hashing Algorithm | • MD5, SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512<br>• HMAC SHA-256, HMAC SHA-512<br>• One-Shot + Streaming Mode<br>• CPU Polling Mode<br>• RTDMA Mode | Yes | |
| SM3 Hashing Algorithm | • SM3-512<br>• CPU Polling Mode<br>• RTDMA Mode | Yes | |
| SM4 Encryption and Decryption | • CBC, CFB, CTR, ECB, OFB<br>• CPU Polling Mode<br>• RTDMA Mode | Yes | |
| RSA<br>Encryption and Decryption<br>Signing and Verification | • RSA 2048, 3072, 4096 bit<br>• RSA PKCS1_5, PSS2_1<br>• CPU Polling Mode | Yes | |
| ECDSA<br>Signing and Verification | • SECP256, SECP384, SECP521<br>• BRAINPOOL-P512<br>• CPU Polling Mode | Yes | |


Copyright © 2026 Texas Instruments Incorporated

**Table 5. Crypto HW Accelerators and Modes Supported (continued)**

| Crypto Core | Support Available in SW Driver | Examples Available | Specification |
|---|---|---|---|
| EDDSA<br>Signing and Verification | • ED25519<br>• CPU Polling Mode | Yes | |
| ECDH<br>Diffie Helman Key Exchange | • SECP256, SECP384, SECP521<br>• BRAINPOOL-P512<br>• CPU Polling Mode | Yes | |

## List of Valid Devices

- F29H85x
- F29P32x



Copyright © 2026 Texas Instruments Incorporated

# 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