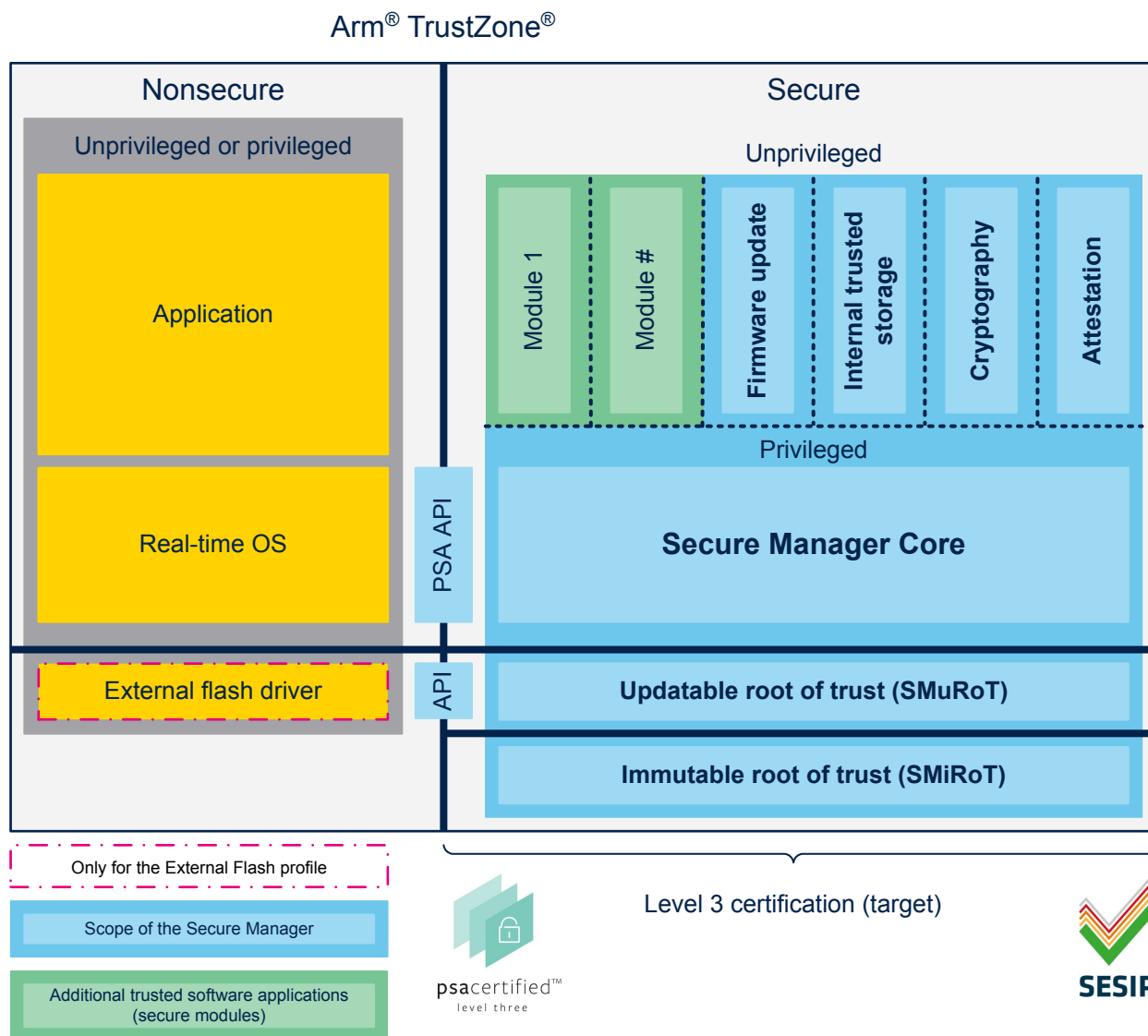


## Secure Manager embedded software for STM32Cube



DT72019v6

### Product status

STM32TRUSTEE-SM

## Features

- Arm® PSA standard and API compliancy
- Arm® PSA services
  - Secure Boot
  - Root of trust (RoT) with chip diversified keys
  - Cryptography functions
  - Internal trusted storage (ITS)
  - Initial attestation (IAT)
  - Firmware update (FWU)
- Software IP protection (PSA isolation level 3)
  - Sandboxed secure services
- Security hardware
  - Arm® Cortex®-M33 with Arm® TrustZone®
  - Option bytes OB-Key secure system key storage (SMiRoT, SMuRoT, and attestation keys)
  - Side-channel-resistant cryptographic accelerators SAES and SPKA
  - Internal and external event tamper detections
  - TRNG NIST SP800-90B
  - Debug authentication with certificate
- Support for external flash memory
  - Application size up to 1.5 Mbytes, enabled by dedicated download slots in the external flash memory
- Security certification (target)
  - PSA Certified™ Level 3
  - GlobalPlatform SESIP3

## Description

Security is a key driver for the microcontroller market, often perceived as complex by the users.

The STM32Trust TEE Secure Manager ([STM32TRUSTEE-SM](#)) is a suite of system-on-chip security solutions that simplifies the development of embedded applications to ensure ready to use security services. With the STM32 microcontroller, the STM32Trust TEE Secure Manager relieves the developers of writing and validating their own code while providing security services developed according to the best practices.

The STM32Trust TEE Secure Manager encompasses two types of packages: the STM32Trust TEE Secure Manager access kit (SMAK) and the STM32Trust TEE secure module development kit (SMDK).

The STM32Trust TEE Secure Manager access kit (SMAK) is installed easily into STM32 products by the customers on their production lines. It offers a ready to use, high performance, and certified solution to support the Secure Boot, root of trust, cryptographic, internal trusted storage, initial attestation, and firmware update functions as defined by the Arm® PSA specifications.

The STM32Trust TEE SMAK binary code is isolated by the Arm® TrustZone® hardware, which protects its capabilities and all the OEM applicative secure credentials it manages and stores. OEMs develop, debug, and protect their applicative firmware as usual, and call STM32Trust TEE SMAK secure functionalities as defined in the STM32Trust TEE SMAK nonsecure reference source code provided by STMicroelectronics (refer to the [Development kits](#) section of the data brief).

The STM32Trust TEE Secure Manager solution is supported by the global STM32 ecosystem tools with [STM32CubeMX](#), the [STM32CubeIDE](#) integrated development environment, and the STM32CubeProgrammer ([STM32CubeProg](#)) ST-LINK programmer.

The STM32H573xx microcontrollers are the first products to support the STM32Trust TEE Secure Manager solution. Download the documentation and software package from the [STM32TRUSTEE-SM](#) web page. Retrieve additional operational and functional descriptions from the STMicroelectronics wiki security pages at [How to start with Secure Manager](#). The reference of the STM32Trust TEE Secure Manager access kit (SMAK) binary software package for STM32H573xx microcontrollers is [X-CUBE-SEC-M-H5](#). Its cryptographic algorithms are CAVP certified (refer to the [NIST CSRC validation](#) section of the data brief). This software package is under export control conditions. Read the [Get Software](#) description before downloading it.

The STM32Trust TEE SMAK binary can be complemented by new secure functions, called secure software modules, developed by STMicroelectronics, OEMs, or ST Partners who want to sell and protect their software intellectual property.

The STM32Trust TEE secure module development kit (SMDK) is dedicated to the development of these new secure software modules. A software module is a simple or a complex function, which has access to the STM32 peripherals and interfaces and is limited in code size. The STM32Trust TEE SMDK allows OEMs and ST Partners to develop, debug with traces, and distribute their own software module to be installed, updated, and executed under the STM32Trust TEE SMAK rules and isolation (refer to the [Development kits](#) section of the data brief).

The STM32Trust TEE secure module development kit (SMDK) for STM32H573xx microcontrollers is not available to mass market usage. It is provided under a specific license agreement. Contact STMicroelectronics sales office for additional information. For usage information, refer to the security section of the STMicroelectronics wiki at [wiki.st.com](http://wiki.st.com).

The list of applicable products is provided in the corresponding section of the data brief.

## 1 General information

The STM32H573xx 32-bit microcontrollers compatible with the STM32Trust TEE Secure Manager (STM32TRUSTEE-SM) are based on Arm® Cortex®-M processor with Arm® TrustZone®.

*Note:* Arm and TrustZone are registered trademarks of Arm Limited (or its subsidiaries) in the US and/or elsewhere.



### 1.1 Ordering information

The STM32Trust TEE Secure Manager access kit (SMAK) for STM32H573xx microcontrollers (X-CUBE-SEC-M-H5) is available for free download from the STM32TRUSTEE-SM web page at the [www.st.com](http://www.st.com) website.

*Note:* X-CUBE-SEC-M-H5 is under export control conditions. Read the Get Software description before downloading from [www.st.com](http://www.st.com).

The STM32Trust TEE secure module development kit (SMDK) for STM32H573xx microcontrollers is not available to mass market usage. It is provided under a specific license agreement. Contact STMicroelectronics sales office for additional information.

### 1.2 Applicable products

**Table 1. Applicable products**

Secure Manager	Microcontrollers	Embedded software
STM32Trust TEE SMAK package <sup>(1)</sup>	STM32H573xx	X-CUBE-SEC-M-H5 (Self-sufficient package including all the required components from STM32CubeH5)

1. Detailed information is available from the security section of the STMicroelectronics wiki at [How to start with Secure Manager](#).

### 1.3 NIST CSRC validation

Refer to Table 2 for access to the Secure Manager CAVP page on the National Institute of Standards and Technology (NIST) portal.

**Table 2. NIST CSRC validation**

Reference	CAVP link
A6437	<a href="https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?product=19163">csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?product=19163</a>

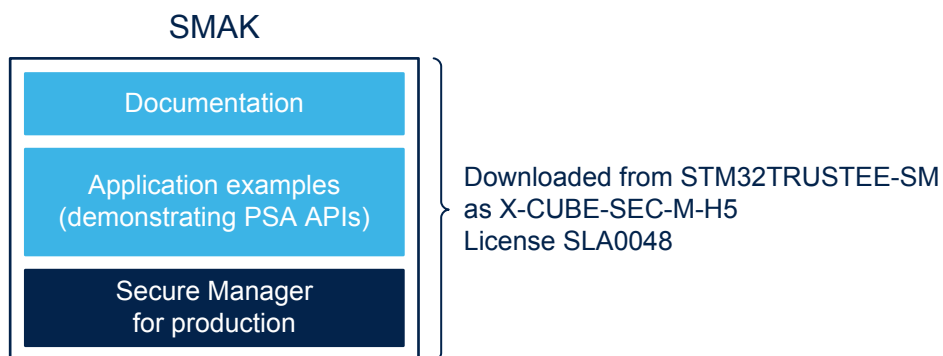
### 1.4 License

The STM32Trust TEE Secure Manager access kit X-CUBE-SEC-M-H5 package is delivered under the SLA0048 software license agreement.

## 1.5 Development kits

Figure 1 presents the Secure Manager access kit to develop nonsecure applications using secure services.

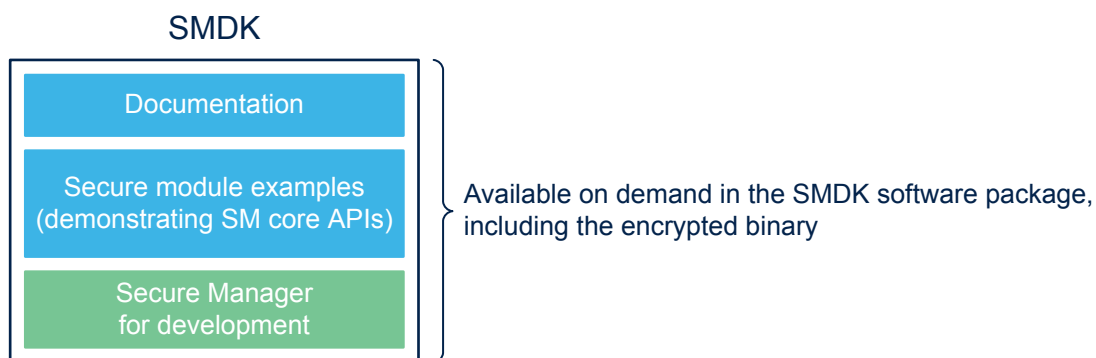
**Figure 1. Secure Manager access kit for nonsecure applications**



DT73503V3

Figure 2 presents the secure module development kit to develop trusted applications.

**Figure 2. Secure module development kit for trusted applications**



DT73504V3

## 1.6 What is STM32Cube?

STM32Cube is an STMicroelectronics original initiative to improve designer productivity significantly by reducing development effort, time, and cost. STM32Cube covers the whole STM32 portfolio.

STM32Cube includes:

- A set of user-friendly software development tools to cover project development from conception to realization, among which are:
  - [STM32CubeMX](#), a graphical software configuration tool that allows the automatic generation of C initialization code using graphical wizards
  - [STM32CubeIDE](#), an all-in-one development tool with peripheral configuration, code generation, code compilation, and debug features
  - [STM32CubeCLT](#), an all-in-one command-line development toolset with code compilation, board programming, and debug features
  - STM32CubeProgrammer ([STM32CubeProg](#)), a programming tool available in graphical and command-line versions
  - STM32CubeMonitor ([STM32CubeMonitor](#), [STM32CubeMonPwr](#), [STM32CubeMonRF](#), [STM32CubeMonUCPD](#)), powerful monitoring tools to fine-tune the behavior and performance of STM32 applications in real time
- [STM32Cube MCU and MPU Packages](#), comprehensive embedded-software platforms specific to each microcontroller and microprocessor series (such as STM32CubeH5 for the STM32H5 series), which include:
  - STM32Cube hardware abstraction layer (HAL), ensuring maximized portability across the STM32 portfolio
  - STM32Cube low-layer APIs, ensuring the best performance and footprints with a high degree of user control over hardware
  - A consistent set of middleware components such as ThreadX, FileX, LevelX, NetX Duo, USBX, USB PD, mbed-crypto, MCUboot, and OpenBL
  - All embedded software utilities with full sets of peripheral and applicative examples
- [STM32Cube Expansion Packages](#), which contain embedded software components that complement the functionalities of the STM32Cube MCU and MPU Packages with:
  - Middleware extensions and applicative layers
  - Examples running on some specific STMicroelectronics development boards

## Revision history

**Table 3. Document revision history**

Date	Revision	Changes
06-Mar-2023	1	Initial release.
22-Aug-2023	2	Updated the cover picture, <i>Description</i> , <i>Applicable products</i> , and <i>License</i> . Added <i>Development kits</i> .
11-Apr-2025	3	Used the SMiRoT and SMuRoT root of trust terms specific to the Secure Manager: <ul style="list-style-type: none"> <li>Updated the cover picture</li> <li>Updated <i>Features</i></li> </ul> Added a reference to the CAVP certification: <ul style="list-style-type: none"> <li>Updated <i>Description</i></li> <li>Added <i>NIST CSRC validation</i></li> </ul> Updated the embedded software package organization in <i>Applicable products</i> , <i>License</i> , and <i>Development kits</i> .
27-Oct-2025	4	Added the External Flash profile: <ul style="list-style-type: none"> <li>Updated the cover picture</li> <li>Updated <a href="#">Features</a></li> </ul>

**IMPORTANT NOTICE – READ CAREFULLY**

STMicroelectronics NV and its subsidiaries ("ST") reserve the right to make changes, corrections, enhancements, modifications, and improvements to ST products and/or to this document at any time without notice.

In the event of any conflict between the provisions of this document and the provisions of any contractual arrangement in force between the purchasers and ST, the provisions of such contractual arrangement shall prevail.

The purchasers should obtain the latest relevant information on ST products before placing orders. ST products are sold pursuant to ST's terms and conditions of sale in place at the time of order acknowledgment.

The purchasers are solely responsible for the choice, selection, and use of ST products and ST assumes no liability for application assistance or the design of the purchasers' products.

No license, express or implied, to any intellectual property right is granted by ST herein.

Resale of ST products with provisions different from the information set forth herein shall void any warranty granted by ST for such product.

If the purchasers identify an ST product that meets their functional and performance requirements but that is not designated for the purchasers' market segment, the purchasers shall contact ST for more information.

ST and the ST logo are trademarks of ST. For additional information about ST trademarks, refer to [www.st.com/trademarks](http://www.st.com/trademarks). All other product or service names are the property of their respective owners.

Information in this document supersedes and replaces information previously supplied in any prior versions of this document.

© 2025 STMicroelectronics – All rights reserved