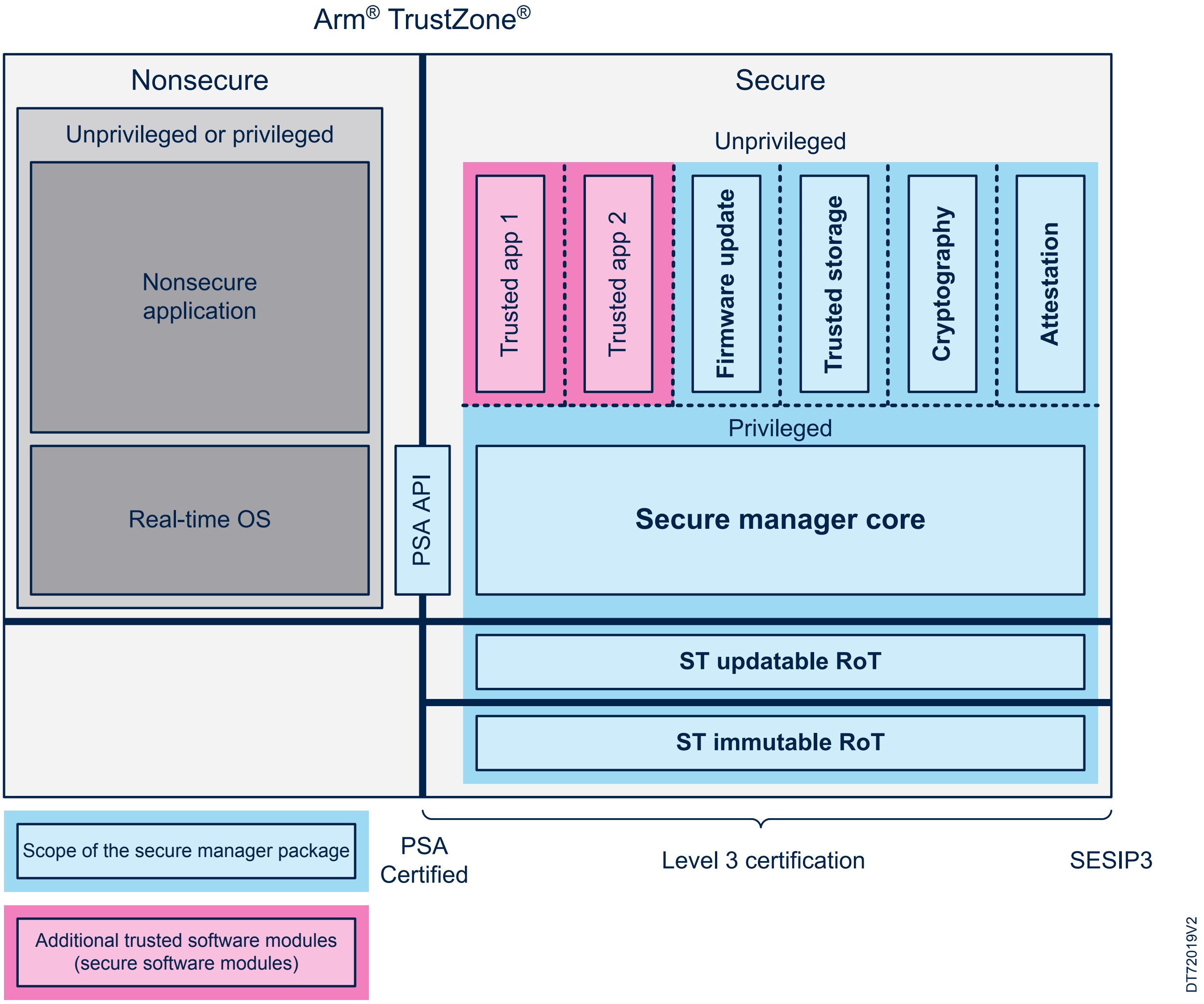
STM32TRUSTEE-SM

Data brief

Secure manager embedded software for STM32Cube



Product status link
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 (STiRoT, STuRoT, and attestation keys)
  - Side-channel-resistant cryptographic accelerators SAES and SPKA
  - Internal and external event tampers detections
  - TRNG NIST SP800-90B
  - Debug authentication with certificate
- 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 the STM32CubeMX initialization code generator, 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 wiki.st.com. The reference of the STM32Trust TEE secure manager access kit (SMAK) binary software package for STM32H573xx microcontrollers is X-CUBE-SEC-M-H5. 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.

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

1 General information

The STM32 32-bit microcontrollers compatible with the STM32Trust TEE secure manager (STM32TRUSTEE-SM) are based on Arm® Cortex®-M processors 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* website.

Note: X-CUBE-SEC-M-H5 is under export control conditions. Read the Get Software description before downloading from 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[1]	STM32H573xx	STM32CubeH5 X-CUBE-SEC-M-H5

1. *Detailed information is available from the security section of the STMicroelectronics wiki at wiki.st.com.*

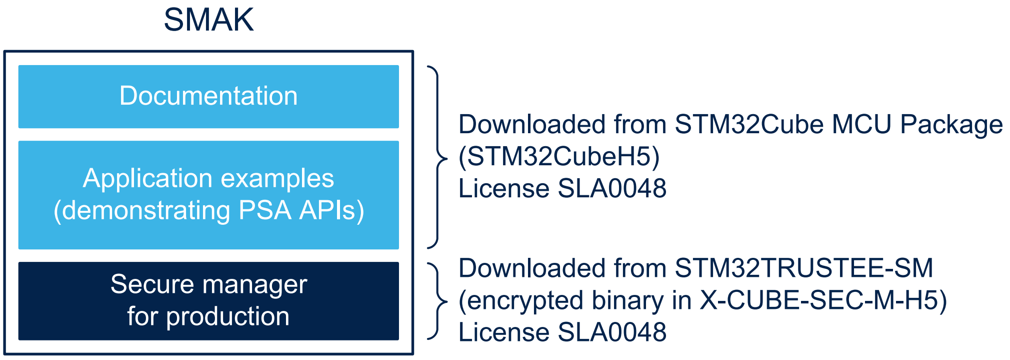
1.3 License

The STM32Trust TEE secure manager access kit X-CUBE-SEC-M-H5 package is delivered under the SLA0048 software license agreement. The secure manager binary is delivered under the SLA0044 software license agreement.

1.4 Development kits

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

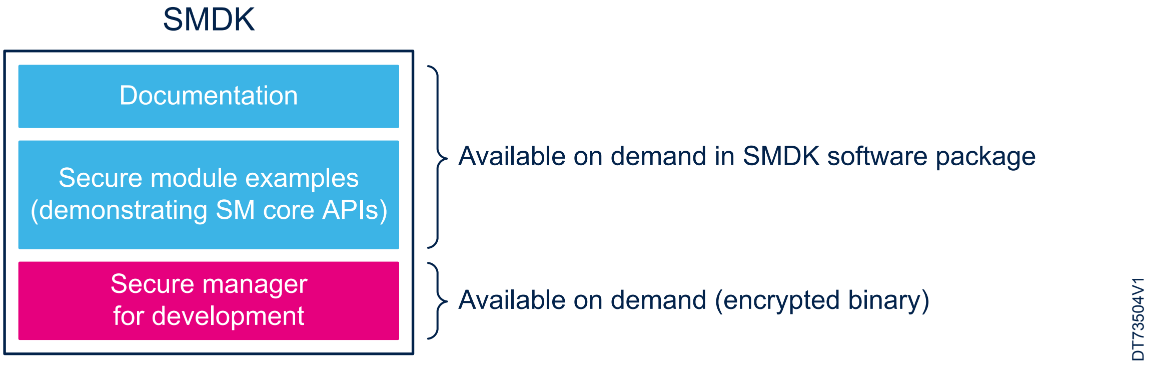
Figure 1. **Secure manager access kit for nonsecure applications**



DT73503V1

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

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


SMDK
Documentation
Secure module examples (demonstrating SM core APIs)
Secure manager for development
Available on demand in SMDK software package
Available on demand (encrypted binary)
DT73504V1

1.5 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, secure manager API, 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 2. **Document revision history**

Date	Revision	Changes
6-Mar-2023	1	Initial release.
22-Aug-2023	2	Updated the cover picture, Description, Applicable products, and License. Added Development kits.

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. 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.

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 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.

ST and the ST logo are trademarks of ST. For additional information about ST trademarks, refer to 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.