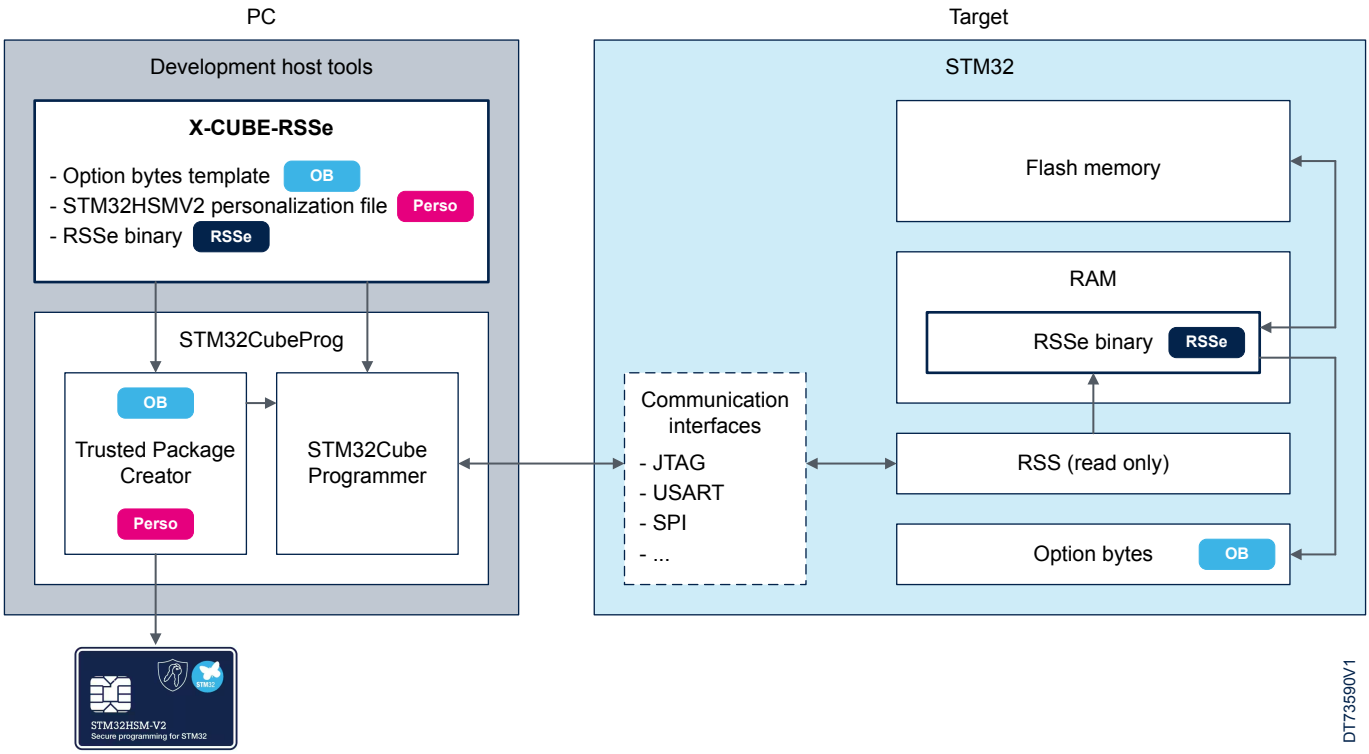
X-CUBE-RSSe

Data brief

Root security services extension (RSSe) software expansion for STM32Cube



Product status link
X-CUBE-RSSe

Features

- Support for various services and API functions to integrate in the user's secure programming tool
  - RSSe binaries for compatible STM32 microcontrollers
  - STM32HSM-V2 personalization data files
  - Option bytes templates
- Compatible with STM32CubeProgrammer and STM32 Trusted Package Creator (STM32CubeProg) v2.18.0 and above
- RSSe-SFI:
  - Secure firmware install (SFI)
- RSSe-KW:
  - Secure key wrapping (KW) service for the protection of private keys

Description

The X-CUBE-RSSe STM32Cube Expansion Package provides STM32 RSSe extension binaries to the root security services (RSS), personalization data files to the STM32HSM-V2 secure application module, and option bytes templates.

In STM32 microcontrollers, the system memory is a read-only part of the embedded flash memory. It is dedicated to the STMicroelectronics bootloader. Some devices might include an RSS library in this area. This RSS library is immutable. It consolidates functionalities and APIs to perform the security functions provided by the STM32 device.

Part of the RSS provides runtime services and functions, which are exposed to the user within the CMSIS device header file of the STM32Cube MCU Package firmware.

Part of the RSS is provided as external RSS extension binaries (RSSe) that extend the security services supported by the STM32. They are authenticated and encrypted libraries delivered in a binary format that only dedicated STM32 devices can execute. RSSe libraries are used by the STMicroelectronics ecosystem tools and by STMicroelectronics programming tool partners to support secure manufacturing processes:

- To use the RSSe-SFI secure firmware install binary, refer to the *STM32 MCUs secure firmware install (SFI) overview* application note (AN4992) and visit the *SFI overview* page of the STM32 MCU wiki at wiki.st.com/stm32mcu.
- The RSSe-KW secure key wrapping service ensures the protection of private keys. Once wrapped, the private keys are not accessible by the user application or by the CPU. The secure key wrapping service uses the coupling and chaining bridge peripheral (CCB) to manage the wrapped keys.

At first, the RSSe binaries, STM32HSM-V2 personalization data files, and option bytes templates were integrated and distributed via the STM32CubeProgrammer tool (STM32CubeProg). From STM32CubeProgrammer version v2.18.0 onwards, all these files are delivered separately in the dedicated X-CUBE-RSSe Expansion Package. They must be installed manually into the STM32 tools. X-CUBE-RSSe is regularly maintained, updated, and made available on *www.st.com*. It is the integrator's responsibility to use the latest version to limit vulnerability exposures.

Table 1. Applicable products

Type	Products
Microcontrollers	• STM32H5 series • STM32H7R3/7S3 line • STM32H7R7/7S7 line • STM32L5 series • STM32U5 series • STM32WBA5xxx (in the STM32WBA series) • STM32WL5x line
Software development tool	STM32CubeProgrammer and STM32 Trusted Package Creator (STM32CubeProg)
Hardware tool	STM32HSM-V2 secure application module

1 General information

X-CUBE-RSSe runs on STM32 microcontrollers based on the Arm® Cortex®-M processor.

Note: Arm is a registered trademark of Arm Limited (or its subsidiaries) in the US and/or elsewhere.

1.1 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 STM32CubeU5 for the STM32U5 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, touch library, network library, mbed-crypto, TFM, 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

2 License

X-CUBE-RSSe is delivered under the SLA0048 software license agreement and its Additional License Terms.

Revision history

Table 2. **Document revision history**

Date	Revision	Changes
18-Oct-2024	1	Initial release.

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.