Hello and welcome to this on-line training module dedicated to the advanced security features of the STM32H7: the Root Security Services (RSS).
It is strongly advised to have already viewed the on-line training module “Memory protections”.

STM32H7 - RSS
Root Security Services
Rev 1.0
Root Secure Services (RSS) are ST ROM code that are part of the STM32H7’s security features. These firmware services are available in Secure access mode, the new security device configuration introduced with the STM32H7 series.
For a definition and how to set the Secure Access mode, please refer to the on-line training module “STM32H7 Memory Protections”.

The main secure service provided by RSS is the Secure Firmware Install (SFI).
This service ensures firmware confidentiality when transferring data to the Flash and prevents overproduction in unsecure manufacturing environments.

To achieve a high level of protection, ST’s solution relies on asymmetric cryptography with a private and unique key for each STM32H7 device. The SFI procedure is detailed in the coming slides.

RSS is also used to manage protected areas such as the
PCROP or Secure User Memory. These protection features are also detailed in the on-line training module “STM32H7 Memory Protections”.


RSS relies on a specific memory protection mechanism presented in this slide. As with all other STM32 products, STM32H7 embeds a read-only area within the Flash memory. This area, called System Flash Memory, embeds ST firmware such as a bootloader and the RSS functions. Note that only the Cortex M7 core has access to the System Flash Memory. The Cortex M4 core can never access it, neither read nor execute access. Sensitive RSS functions with confidential algorithm and cryptographic keys are embedded in a specific part of the System Flash Memory: the Secure System Memory. This memory has specific access rules that grant a very high level of protection to the device. It is only available in Secure Access mode. The device must be set in this mode before any RSS services can be accessed. Access to most RSS services are granted after a system
reset. The Cortex M7 core can then safely execute the service required by preempting all other processes running on either one of the cores. When RSS execution is completed, the device jumps to the User application and the Secure System Memory is no longer accessible until the next system reset.
RSS services can be called either by direct application programming interface (API) functions or by specific bootloader commands. RSS functions and bootloader commands set are given for reference in the next slide. RSS services can be split into two kinds depending on the confidential data or code they manipulate.

Critical services are the ones that manipulate confidential data, such as cryptographic keys, or that require a safe execution from other processes. A system reset is triggered before execution of these services.

Critical RSS services include:
- Secure firmware or module install
- Initialization of Secure User memory and PCROP areas removal

Uncritical services do not require access to confidential data and can be executed without any reset.

Critical services:
- Manipulate confidential data and protected code
- Require a system reset to be executed from Secure System memory
  - Secure Firmware Install
  - Secure Module Install
  - Initialize Secure User memory
  - Destroy PCROP areas

Uncritical services:
- Access to non-secret data or status (certificate, RSS version, …)
- Manipulate encrypted data only
- Does not require reset to be executed
This slide lists the RSS services available and how they can be called. Services called by direct API are the ones that can be called by device administration firmware. These services allow secure area management or secure module install. Certain RSS services can be seen as a bootloader extension for secure commands. These commands allow the SFI procedure to be driven by external flasher tools such as the STM32CubeProgrammer or any other flasher tool.
This slide presents the RSS services that are used to manage the protected areas of the device. These services allow the setting and the management of the Secure User Memory. This memory is for critical user firmware that will be executed in a safe environment. Typical applications of such critical firmware are “Secure Firmware update” (SFU) and Secure bootloader.

For a detailed description of the Secure User Memory functionality, please refer to the STM32H7 training module “Memory protections” and to application note AN4925.

An RSS service is available for managing the PCROP areas. It can be used in the case of software update to remove protected areas without triggering a Flash Mass Erase.
This slide describes the main RSS service which is the Secure Firmware Install (SFI). SFI is used to securely transfer firmware to the device in an unsafe manufacturing stage. Firmware is protected against copy and overproduction by cryptographic algorithms. Each STM32H7 device is provisioned by STMicroelectronics with chip asymmetric key pairs and certificates for device authentication and firmware confidentiality. The device’s private key is embedded in the Secure System Flash and only the ST RSS service can access it. The SFI cryptographic flow is described in this image.

First, the firmware is encrypted with Advance Encryption Standard in Galois Counter Mode (AES-GCM). Then, a firmware license for the device is generated from the firmware encryption key and the device’s public key. This license can only be used by the targeted device. Finally, the encrypted firmware is transferred to the device and decrypted before being stored in the user Flash.
memory.
The cryptographic data flow presented in the previous slide requires specific tools: an encryption tool for the firmware, a license server to generate the firmware license associated to a device and a Flasher tool to execute the SFI sequence through the device bootloader.
STM32 Trusted Package Creator implements the AES-GCM algorithm and generates the encrypted firmware image with the correct header and option byte descriptions. It can also be used for third-party modules for firmware update applications.

The secure license server is required to generate the license from the device certificate and the firmware key. This server is under the product owner’s responsibility and is accessed by the product manufacturer.
The flasher tool drives the SFI sequence by using the device bootloader with its RSS extension. It fetches the device certificate, gets the firmware license from the license server and transfers the encrypted firmware to the device. You can get ST’s flasher tool “STM32CubeProgrammer” on ST.com or use one of our partners’.
Related peripherals

- Refer to the training related to this peripheral:
  - Memory protections

Please refer to the Flash memory protection training to learn more about the memory architecture, option bytes and Flash operations.
You will find detailed descriptions and explanations of the RSS concept in the following application notes and user manuals.
• Application note AN2606 describes the bootloader feature.
• Application note AN4992 describes the SFI procedure in detail.
• Application note AN4925 gives an example of the secure user memory.
User manuals for STM32CubeProgrammer and STM32 Trusted Package Creator are also available on the ST website.

References

• For more details, please refer to following resources
  • Application note AN2606: STM32 microcontroller system memory boot mode
  • Application note AN4992: STM32H753xl secure firmware install (SFI) overview.
  • Application note AN4925: STM32H753xl secure user memory and example of secure firmware update
  • User Manual UM2237: STM32CubeProgrammer software description
  • User Manual UM2238: STM32 Trusted Package Creator software description