STM32WL5 security - RSS

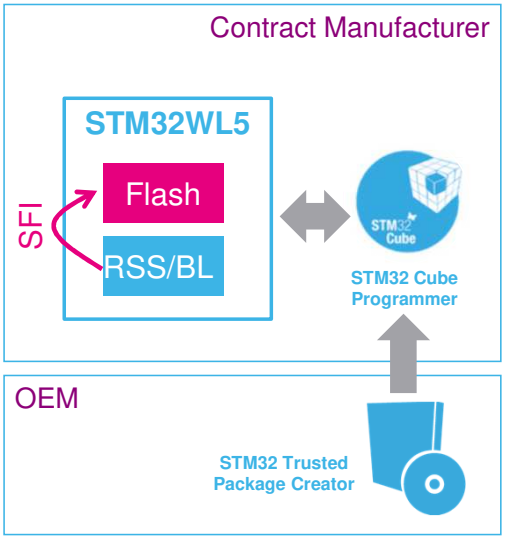
Root Security Services

Revision 1.0

Hello and welcome to this on-line training module dedicated to the advanced security features of the STM32WL5: Root Security Services (RSS).

Overview

- RSS provide services for secure firmware install solutions (SFI) to the bootloader and the user firmware.



Application benefits

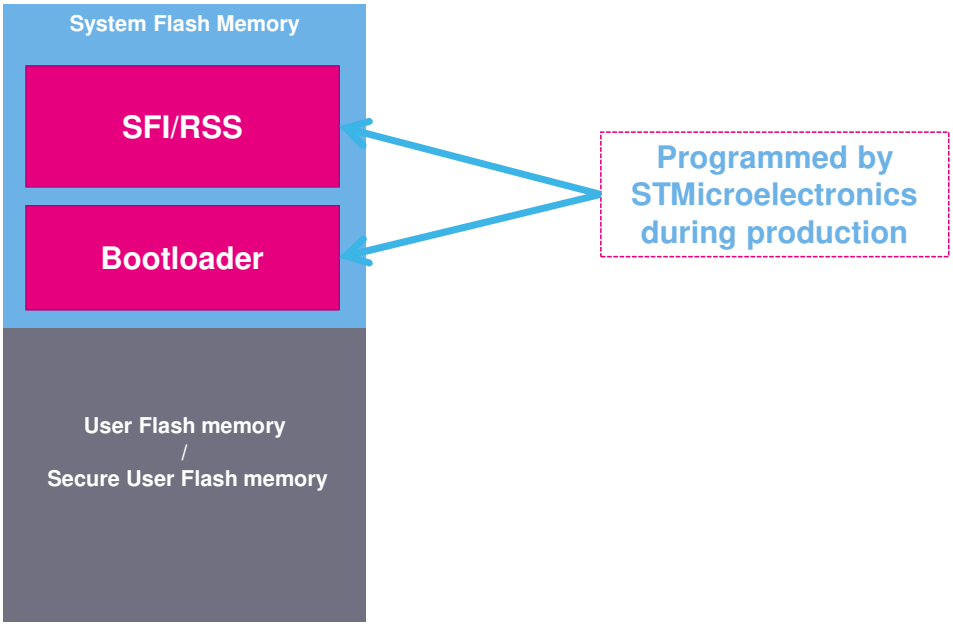
- Enables Secure Firmware Install (SFI)

life.augmented

2

RSS is used to load content in the secure or non secure flash memory.
The RSS provides runtime root security services used by the STM32 secure firmware install solution (SFI).
For more information on protected memories please refer to the on-line training module “STM32WL5-Security-Memories Protection”.

Flash memory organisation

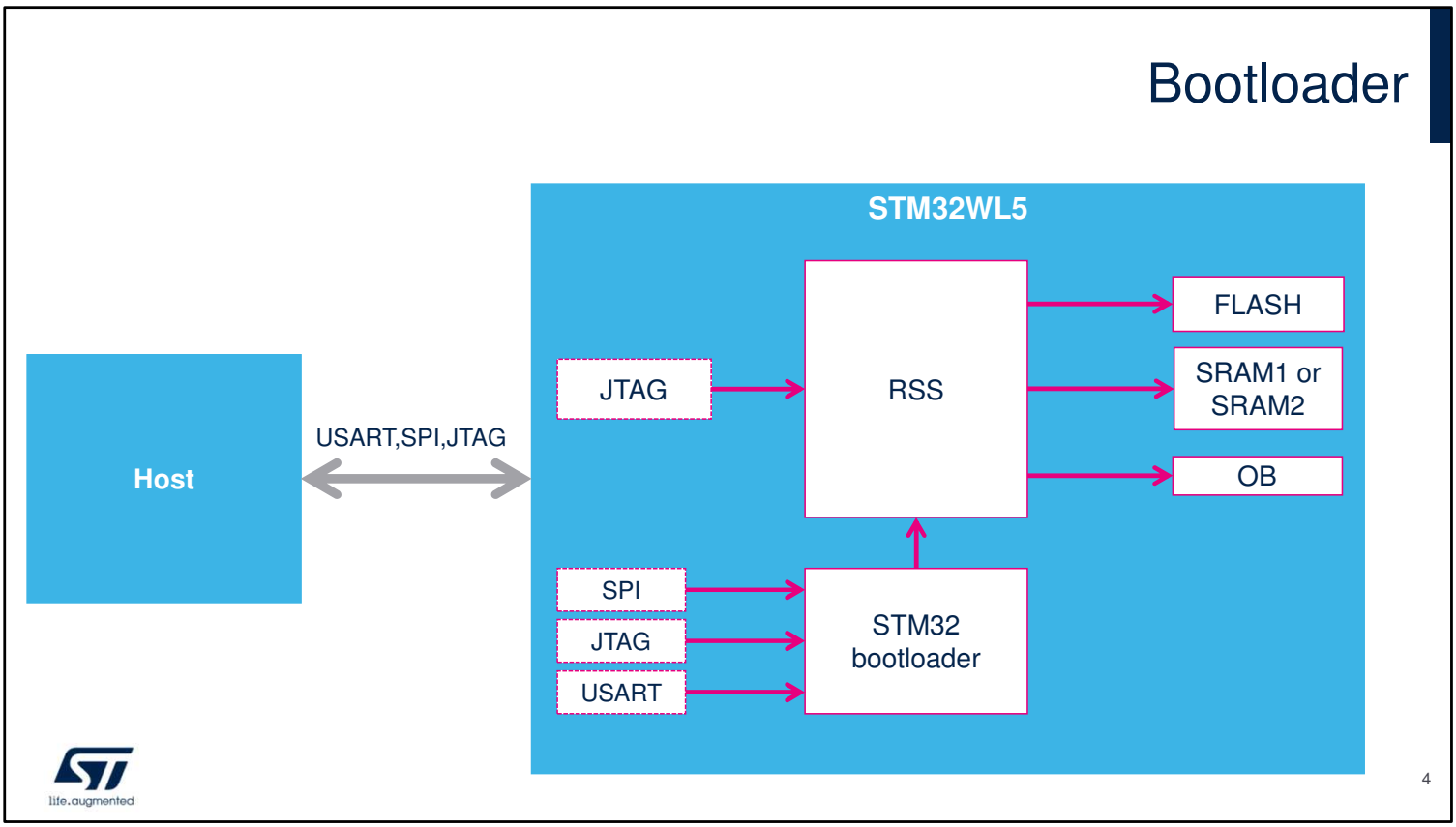


life.augmented

3

The flash memory has an information block containing:

- System memory from which the CPU1 (Cortex M4) boots in system memory boot mode. This area is reserved and contains the bootloader used to reprogram the Flash memory through one of the following interfaces: USART, I2C1 or SPI. It is programmed by STMicroelectronics when the device is manufactured and protected against spurious write/erase operations. For further details, refer to the application note STM32 microcontroller system memory boot mode (AN2606).
- System memory from which the CPU2 (Cortex M0+) boots in System memory boot mode. This area is reserved and contains the SFI/RSS firmware used to authenticate and install the firmware in Flash memory through one of the following interfaces: USART, I2C or SPI. It is programmed by STMicroelectronics when the device is manufactured and protected against spurious write/erase operations.



On the STM32WL5x microcontroller, the secure bootloader is stored in the internal flash memory (system memory) and supports following interfaces: USART, SPI and JTAG.

The STM32WL5x secure bootloader allows the execution of the SFI process several times after complete erase of the internal user Flash memory, if erasure is allowed by installed application.

The embedded bootloader is used to program flash memory and runs on the CPU1 (Cortex M4). It can be used to load content in non-secure memory areas.

The embedded secure firmware install process as part of the root security services (SFI/RSS) allows the programming of the flash as the embedded bootloader . It runs on the CPU2 (Cortex M0+) and can be used to load content in both secure and non secure memory areas.

The secure bootloader is a standard ST bootloader with additional security features.
During the SFI process, the secure bootloader never allows any other code to access the user Flash memory or SRAM.

Secure firmware install (SFI)

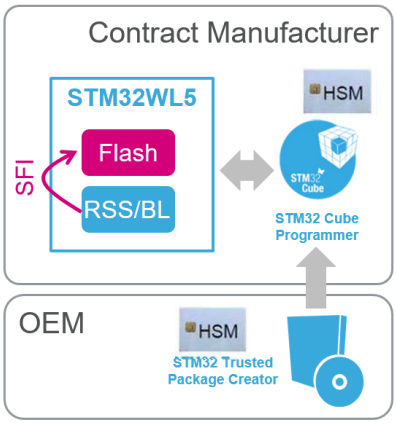
- Secure firmware install (SFI) is a global solution for STM32WL5 Series of microcontrollers, allowing secure and counted installation of OEM firmware in untrusted production environment (such as OEM contract manufacturer).
- SFI is implemented using the secure bootloader and RSSE (root security services extension).
- Refer to AN5511 for more details on SFI tools

life.augmented

Secure firmware install (SFI) is a global solution for STM32WL5 Series of microcontrollers, allowing secure and counted installation of OEM firmware in untrusted production environment (such as OEM contract manufacturer).
SFI is implemented using the secure RSS and the secure bootloader. OEM firmware protected by SFI can be store in the device's embedded flash.
the STM32WL5 SFI solution consists in having the whole OEM firmware and the option bytes encrypted with an AES secret key, thanks to STM32 Trusted Package Creator tool. This is done during OEM firmware development.
Confidentiality of this AES secret key is ensured using an STM32 device unique key pair, with the private key readable only by the RSS.

For more information please refer to application note AN5511 for secure firmware install (SFI) solutions.

SFI security features



- Only genuine STMicroelectronics STM32 microcontrollers can install the protected firmware via SFI. It can be done in a non-trusted environment/facility.
- The number of STM32 devices on which the firmware has been installed can be counted inside the HSM
- Authenticity, integrity and confidentiality of the OEM internal firmware (and option bytes) are checked before embedded Flash is programmed with decrypted firmware (and option bytes).
- STM32CubeProgrammer supports secure programming of SFI images for STM32WL5 microcontrollers via USART, SPI or JTAG

life.augmented

6

Only genuine STMicroelectronics STM32WL5 microcontrollers can install the protected firmware via SFI. The number of STM32 devices on which the firmware has been installed can be counted inside the hardware security module (HSM) associated with the SFI process (see next slide).

OEM firmware and the option bytes are encrypted thanks to STM32TrustedPackageCreator tool, during OEM firmware development. OEM also uses this tool to program the Hardware security module (HSM) with its AES secret key, its nonce, and a maximum installation counter. OEM contract manufacturer uses STM32CubeProgrammer + provisioned HSM to initiate SFI process and sends encrypted SFI image to the STM32WL5 device.

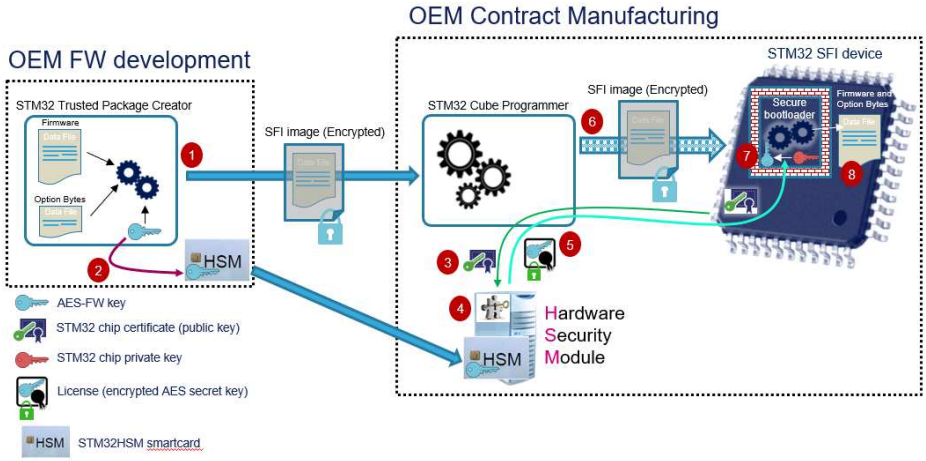
Authenticity, integrity and confidentiality of the OEM internal firmware (and option bytes) are checked before embedded

Flash is programmed with decrypted firmware (and option bytes).

SFI to internal flash

- SFI image (encrypted) available from STM32 Trusted Package Creator
- OEM programs HSM with AES secret key
- HSM provides license to STM32
- Device certificate retrieval
- STM32 device authentication in HSM
- SFI process launch

- RSS retrieves OEM AES secret key encrypted in license
- Encrypted firmware and option bytes decryption then programming



Secure firmware install to internal Flash memory goes as follow (numerical steps are represented on the schematic):
1/ OEM creates OEM FW (.sfi)
2/ OEM provisions OEM FW key in HSM
3/ Cube programmer gets Certificate
4/ HSM creates the License
5/ STM32 gets the License
6/ STM32 gets the OEM FW (.sfi)
7/ STM32 decrypts the OEM FW and OB
8/ STM32 programs the OEM FW and OB

Related peripherals and trainings

- Refer to these trainings linked to RSS
  - STM32WL5-Security-Memories Protection
    - Protecting code and/or data from external and/or internal attacks
  - STM32WL5-System-CM0+ security” module

life.augmented

Please refer to Memory protection, Flash or Boot training if you want to know more on those topics.
Also find a list of peripherals related to the RSS and the SFI.

References

- For more details and additional information, refer to the following
  - RM0453: STM32WL5 Reference Manual.
  - AN2606: “STM32 microcontroller system memory boot mode”
  - AN4992: Overview of secure firmware install (SFI)
  - AN5511: “STM32WL5x SFI tools, bootloader and RSS interface”
  - UM2237: STM32CubeProgrammer software description
  - UM2238: STM32 Trusted Package Creator software description

life.augmented

9

For more details, please refer to:

- Application note AN2606 about STM32 microcontroller system memory boot mode.
- Application note AN4992 about Overview of secure firmware install (SFI) and application note AN5511 about STM32WL5x SFI tools, bootloader and RSS interface.
- User manuals for STM32CubeProgrammer and STM32 Trusted Package Creator are also available on the ST website.