life.augmented

AN6014

Application note

Introduction to SFSP versions for STM32H5 MCUs

Introduction

The system flash security package (SFSP) is stored within the internal boot ROM memory (system memory) of STM32H5 devices. The SFSP is programmed by STMicroelectronics during production and provides various security services to STM32H5 users.

1 General information

This document applies to STM32H5 Arm®-based devices.

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

1.1 Reference documents

Table 1. Reference documents

Reference	Document name	Document title
[1]	AN4992	*STM32 MCUs secure firmware install (SFI) overview* (application note)
[2]	AN6007	*ST immutable Root of Trust (STiRoT) overview* (application note)
[3]	AN6008	*STM32 Debug Authentication (DA) overview* (application note)
[4]	RM0481	*STM32H563/H573 and STM32H562 Arm®-based 32-bit MCUs* (reference manual)

1.2 Glossary

Table 2. Glossary

Abbreviation/notation	Meaning
RSS	Root security services
RSS_LIB	Root security services library
NSS_LIB	Nonsecure domain security library
STiRoT	STMicroelectronics immutable Root of Trust
RSS_DA	Root security services debug authentication
SFSP	System flash security package

2 SFSP description

The SFSP contains several types of firmware, each of them dedicated to a specific service:

- RSS is the firmware responsible for installing the RSSe library, which manages the SFI process (refer to reference document [1]).
- STiRoT manages the first secure boot stage of the STM32H5 device when the user selects STiRoT as its device root of trust (refer to reference document [2] for a detailed description of STiRoT). STiRoT provides two main services:
  - The secure boot, which is always executed after a system reset. It activates STM32H5 runtime protections and verifies the authenticity and integrity of the application before jumping to it.
  - The secure firmware update checks if an application image is available, and if found, it verifies the application authenticity and integrity before installing it after decryption.
- RSS_DA: refer to reference document [3] for a detailed description of RSS_DA and debug authentication services. RSS_DA provides the following debug authentication services:
  - Regression and partial regression (if supported) of the STM32H5 device.
  - Secure debug reopening of the STM32H5 device (if supported).
- RSS_LIB is a collection of services provided by the functions depicted in section 7.7.2 "RSS user functions" of reference document [4]. These services are only callable when the STM32H5 device enables TrustZone® and runs in the secure domain.
- NSS_LIB is a collection of services provided by the functions depicted in section 7.7.2 "RSS user functions" of reference document [4]. These services are callable when the STM32H5 device enables TrustZone® and runs in the nonsecure domain, or when the STM32H5 device disables TrustZone®.

2.1 STM32H503

For STM32H503 devices, the user can read the SFSP version as a word value at the address 0x0BF860CC.

STM32H503 SFSP embeds:

- RSS_DA
- NSS_LIB

2.2 STM32H573/533

For STM32H573 and STM32H533 devices, the user can read the SFSP version as a word value at the address 0x0BF960CC.

For these devices, SFSP embeds:

- RSS
- STiRoT
- RSS_DA
- RSS_LIB
- NSS_LIB

2.3 STM32H563/523

For STM32H563 and STM32H523 devices, the user can read the SFSP version as a word value at the address 0x0BF960CC.

For these devices, SFSP embeds:

- RSS
- RSS_DA
- RSS_LIB
- NSS_LIB

3 SFSP version history

3.1 STM32H503

Table 3. STM32H503 SFSP version history

Silicon revision	SFSP version	SFSP version @0x0BF860CC	Description	Known limitations
-	V1.2.0	0x01020000	SFSP structure changes	• User flash memory not fully visible from BL. • BL is not functional when ECC is enabled on SRAM2 via option bytes. • Discovery command displays wrong system information when product state is "open".
-	V1.3.0	0x01030000	• Handle ECC detection due to OTP flash area not written. • Fix known limitations on SFSP V1.2.0.	Debug authentication (regression and debug reopening) is not functional when the user enables IWDG via option bytes.
-	V1.4.0	0x01040000	Fix known limitations on SFSP V1.3.0.	-

3.2 STM32H573/563

Table 4. STM32H573/563 SFSP version history

Silicon revision	SFSP version	SFSP version @0x0BF960CC	Description	Known limitations
-	V2.0.0	0x00020000	3 chip certificate in system flash memory.	Data provisioning over SPI.
-	V2.1.0	0x02010000	4 chip certificate in system flash memory.	Data provisioning over SPI.
Rev Z	V2.2.0	0x02020000	• Enable data provisioning over SPI. • Fix known limitations on SFSP V2.1.0.	• Regression when EEPROM is enabled. • STiRoT max frequency at 240 MHz.
Rev X	V2.5.0	0x02050000	• STiRoT alive after partial regression. • Fix known limitations on SFSP v2.4.0.	Debug authentication (regression) not functional on STM32H563 with 1-M flash memory (STM32H562xG/ STM32H563xG).
Rev X	V2.6.0	0x02060000	Fix known limitations on SFSP v2.5.0. This SFSP version is limited to STM32H563.	-

3.3 STM32H533/523

Table 5. **STM32H533/523 SFSP version history**

Silicon revision	SFSP version	SFSP version @0x0BF960CC	Description	Known limitations
Rev A	V1.0.0	0x01000000	Support all SFSP features.	Debug Authentication not functional on STM32H523 (discovery command returns wrong SoC ID value & certificate chain based on SoC ID cannot be used).
Rev A	V1.2.0	0x01020000	Fix known limitations on SFSP v1.0.0.	-

Revision history

Table 6. **Document revision history**

Date	Version	Changes
12-Oct-2023	1	Initial release.
18-Mar-2024	2	Updated: • Section Introduction • Section 1: General information • Table 1. Reference documents • Table 2. Glossary • Section 2: SFSP description • Section 2.2: STM32H573/533 • Section 2.3: STM32H563/523 Added: • Section 2.3: STM32H563/523 • Section 3.3: STM32H533/523

Contents

List of tables