Introduction to SFSP versions for STM32H7Rx/7Sx MCUs

Introduction

The system flash security package (SFSP) is stored within the internal boot ROM memory (system memory) of STM32 devices. SFSP is programmed by STMicroelectronics during production and provides various security services to STM32 users.

This document applies to the products listed in Table 1 below.

Table 1. Applicable products

Type	Part number or product series
Microcontrollers	STM32H7R3/7S3 line, STM32H7R7/7S7 line

In the following sections, STM32 refers to the products listed in Table 1 above, unless stated otherwise.

1 General information

This document applies to Arm®-based devices.

Note: Arm and Cortex are registered trademarks of Arm Limited (or its subsidiaries) in the US and/or elsewhere.

arm

1.1 Referenced documents

Table 2. Referenced documents

Reference	Document ID	Definition
[1]	RM0477	*STM32H7Rx/Sx Arm®-based 32-bit MCUs* (Reference manual)
[2]	AN4992	*Introduction to secure firmware install (SFI) for STM32 MCUs* (Application note)
[3]	AN6008	*Getting started with debug authentication (DA) for STM32 MCUs* (Application note)
[4]	AN6045	*Getting started with STiRoT (ST immutable Root of Trust) for STM32H7S MCUs* (Application note)
[5]	ES0596	*STM32H7R3xx, STM32H7R7xx, STM32H7S3xx, STM32H7S7xx device errata (Errata sheet)*

1.2 Glossary

Table 3. Glossary

Abbreviation/notation	Meaning
HDPL	Hide protect level
OBKey	Option byte key
RSS	Root security services
RSS_DA	Root security services debug authentication
RSS_LIB	Root security services library
SFSP	System flash security package
STiRoT	STMicroelectronics immutable Root of Trust

2 SFSP description

SFSP is a package that contains several types of firmware, each of them dedicated to a specific service:

- RSS is the firmware responsible for:
  - Activating security mechanisms during boot.
  - Selecting the boot on bootloader, RSS_DA, STiRoT, or user flash memory, depending on the product configuration.
  - Installing the RSSe library (on request), which manages the SFI process (refer to document [2]).
  - Providing services for OBkeys and HDPL0 option bytes provisioning.
  - Configuring the product state.
- STiRoT manages the first secure boot stage of the STM32 device when the user selects STiRoT as its device root of trust. (Refer to document [4] for a detailed description of STiRoT.) STiRoT provides two main services:
  - The secure boot, which is always executed after a system reset. It activates STM32 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 document [3] for a detailed description of RSS_DA and debug authentication services. RSS_DA provides the following debug authentication services:
  - Regression of the STM32 device.
  - Secure debug reopening of the STM32 device.
  - Force new image download.
- RSS_LIB is a collection of services provided by the functions depicted in section 4.10.2, "RSS user functions", of document [1].

The STM32 user can read the SFSP version as a word value at the address 0x1FF1FDD0.

2.1 STM32H7Rx

STM32H7Rx SFSP embeds:

- RSS
- RSS_DA
- RSS_LIB

2.2 STM32H7Sx

STM32H7Sx SFSP embeds:

- RSS
- STiRoT
- RSS_DA
- RSS_LIB

3 SFSP version history

Table 4. **STM32H7Rx/7Sx SFSP version history**

Silicon revision	SFSP version	SFSP version @0x1FF1FDD0	Description	Known limitations
Rev Y	V1.1.0	0xFF010100	Initial version	Refer to document [5]
Rev B	V2.0.0	0xFF020000	Fix the following limitations referred to in the following document [5] sections: • 2.2.5 • 2.2.7 • 2.2.8 • 2.2.9 OBkeys provisioning can be done without encryption for STM32H7Sx.	Refer to document [5]
	V2.1.0	0xFF020100	Fix the following limitations referred to in the following document [5] sections: • 2.2.10 • 2.2.11 • 2.2.12 • 2.2.13 • 2.2.14 The RTC is no longer initialized after STiRoT execution. Tamper event detected during RSS/RSS_DA/STiRoT execution is reported in BKPSRAM. Refer to document [4] for more details.	Refer to document [5]

Revision history

Table 5. **Document revision history**

Date	Version	Changes
06-Mar-2024	1	Initial release.
09-Oct-2024	2	Updated: Table 4. STM32H7Rx/7Sx SFSP version history
27-Oct-2025	3	Updated: • Table 2. Referenced documents • Table 4. STM32H7Rx/7Sx SFSP version history

Contents

List of tables

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.

In the event of any conflict between the provisions of this document and the provisions of any contractual arrangement in force between the purchasers and ST, the provisions of such contractual arrangement shall prevail.

The 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.

The 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 the 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.

If the purchasers identify an ST product that meets their functional and performance requirements but that is not designated for the purchasers' market segment, the purchasers shall contact ST for more information.

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.