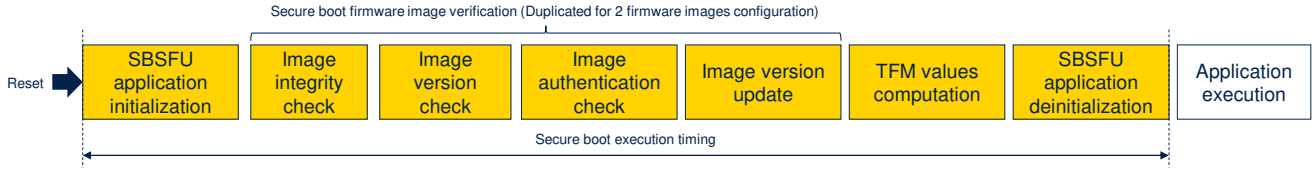
Hello, and welcome to this presentation on secure firmware update timing.

TFM_SBSFU_Boot Operations

- The execution timing of the “Secure Boot” function depends directly on implementation of the cryptographic algorithms but also on other system parameters such as:
  - The hardware configuration: Hardware acceleration capability, maximum clock frequency 160MHz, instruction cache enabled
  - The number of firmware images: single or double
  - The number of firmware slots: Primary and secondary slots or Primary slot only
  - The firmware image size
  - The size of Flash memory area used to store the firmware image version
  - The SBSFU cryptography scheme configuration (Asymmetric cryptography based on RSA or ECC)
  - The SBSFU configuration: TFM support or not



life.augmented

The TFM_SBSFU_BOOT application implements the "Secure Boot" function and the "Secure Firmware Update“ function.
The following parameters affect the execution timing of the secure boot function :

- The hardware configuration
- The number of firmware images
- The number of firmware slots
- The firmware image size
- The size of the flash memory area used to store the firmware image version
- The SBSFU cryptography scheme configuration
- The SBSFU configuration: with or without TFM support
- The compiler optimization options.

Each step of the Secure Boot sequence is detailed on the figure

- SBSFU application initialization
- Image integrity check
- Image version check
- Image authentication
- Image version update
- TFM value computation
- SBSFU application deinitialization.

The activating of the run-time protection (HDP) and cleaning of the SRAM used by the SBSFU application are performed during the deinitialization of the SBFSU application.

TFM_SBSFU_Boot application performance

Secure boot timing depends on lots of system parameters

Operation name		Dimensioning parameters
SBSFU application initialization	3 ms	• The amount of RAM used by SBSFU application • The size of the flash area used to store the firmware image version • The number of firmware image
Image integrity check	2.5 ms for 31 KB image 8.3 ms for 177 KB image	• The image size
Image version check	0.5 ms	• The size of the flash area used to store the firmware image version
Image authentication check	5 ms (RSA 2048-bit hardware) +6 ms (RSA 3072-bit hardware)	• The cryptographic scheme configuration • The STM32U5/s hardware-accelerated cryptography capability
Image version update	0.5 ms	• The size of the Flash area used to store the firmware image version
TFM value computation: ➢ % SBSFU application code size	2.5 ms	• Only applicable with TFM secure application configuration • The size of the SBSFU application
SBSFU application deinitialization: ➢ % RAM size used by SBSFU Application	1.4 ms	• The size of the RAM used by the SBSFU application

The "Secure Boot" function uses cryptographic algorithms, which can be implemented in full software (mbedcrypto software implementation) or can be accelerated by the STM32U5 hardware cryptographic accelerators.
The execution timing of the “Secure Boot” function depends directly on the implementation of the cryptographic algorithms but also on other system parameters, as indicated in the table.

The table indicates the time to execute each step of the secure boot operation sequence described in the previous slide.
The reference SBSFU configurations used to measure these timing are the following:

• IDE: Keil® (toolchain MDK-ARM 5.31.0 with option "-Oz image size")
• The hardware configuration: hardware-accelerated cryptography capability,160 MHz, instruction cache enabled
• The number of firmware images: two firmware images
• The number of firmware slots: primary and secondary slots
• The size of the firmware images: 31 Kbytes and 177 Kbytes
• The size of the flash memory area used for the firmware image version storage: 8 Kbytes
• The SBSFU cryptography scheme configuration: RSA2048, firmware encryption supported
• The SBSFU configuration: TFM supported

“Secure Boot” execution timing indications

- **This table gives some “Secure Boot” execution timing values for 2 configurations**

Configuration description	Secure Boot execution Timing
Configuration -1-	30 ms
• 160 MHz, instruction cache activated on internal memories • **2 firmware images (177 Kbytes, 31 Kbytes)** • 2 slots • RSA 2048 **with hardware-accelerated cryptography capability** • **TFM configuration** • Keil® IDE (toolchain MDK-ARM5.31.0 with option "-Oz image size")	
Configuration -2-	
• **1 firmware image (76 Kbytes)** • RSA 2048 **with software cryptography** • **SBSFU configuration (no TFM secure services)**	

- Configuration differences between configurations are highlighted in bold
- The Cryptography timing fluctuates slightly according to key value

life.augmented

4

This table gives “Secure Boot” execution timing values for two configurations.
The common features for both configurations are:

- Keil® IDE (toolchain MDK-ARM 5.31.0 with option "-Oz image size")
- 160 MHz operation, instruction cache enabled on internal memories
- 2 slots.

The features specific to configuration number one are:

- 2 firmware images (177 Kbytes, 31 Kbytes)
- RSA 2048 with hardware-accelerated cryptography capability
- TFM configuration.

The features specific to configuration number two are:

- 1 firmware image (76 Kbytes)

- RSA 2048 with software cryptography
- SBSFU configuration (no TFM secure services).

These two different configurations lead to the same secure boot execution timing: 30 ms.

Thank you

life.augmented

Thank you for attending this presentation!
You can refer to UM2851 for more details on secure firmware update performance metrics and to the following presentations that detail how TFM works:

- TFM flash memory footprint
- TFM offer in STM32U5.