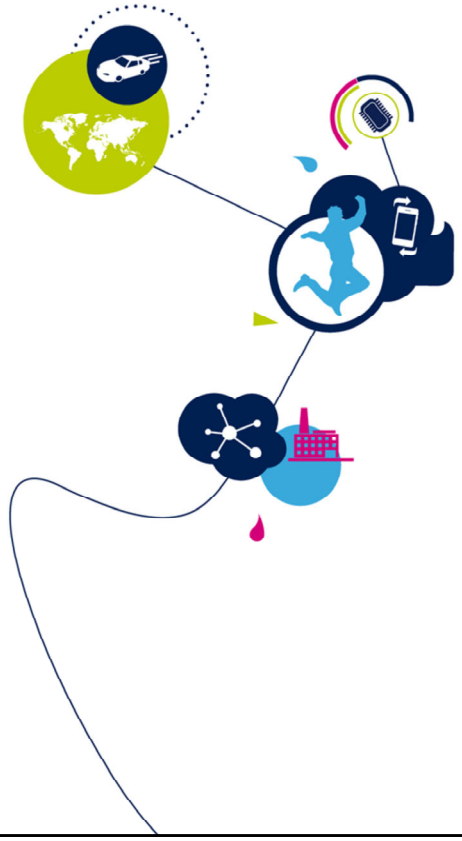
STM32WB – CM0+ Security

Cortex-M0+ security

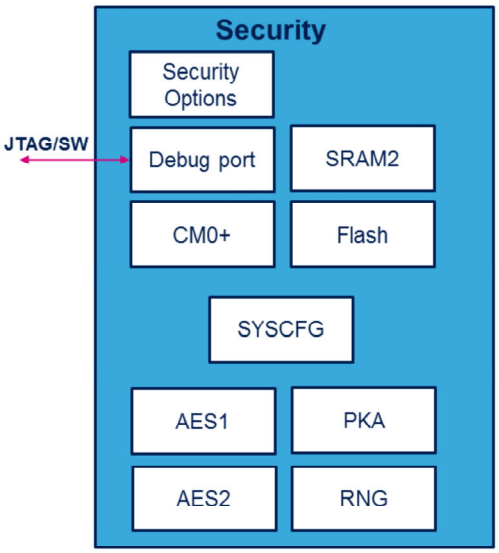
Revision 1.0



life.augmented

Hello, and welcome to this presentation of the STM32WB Cortex M0+ security features.

Overview

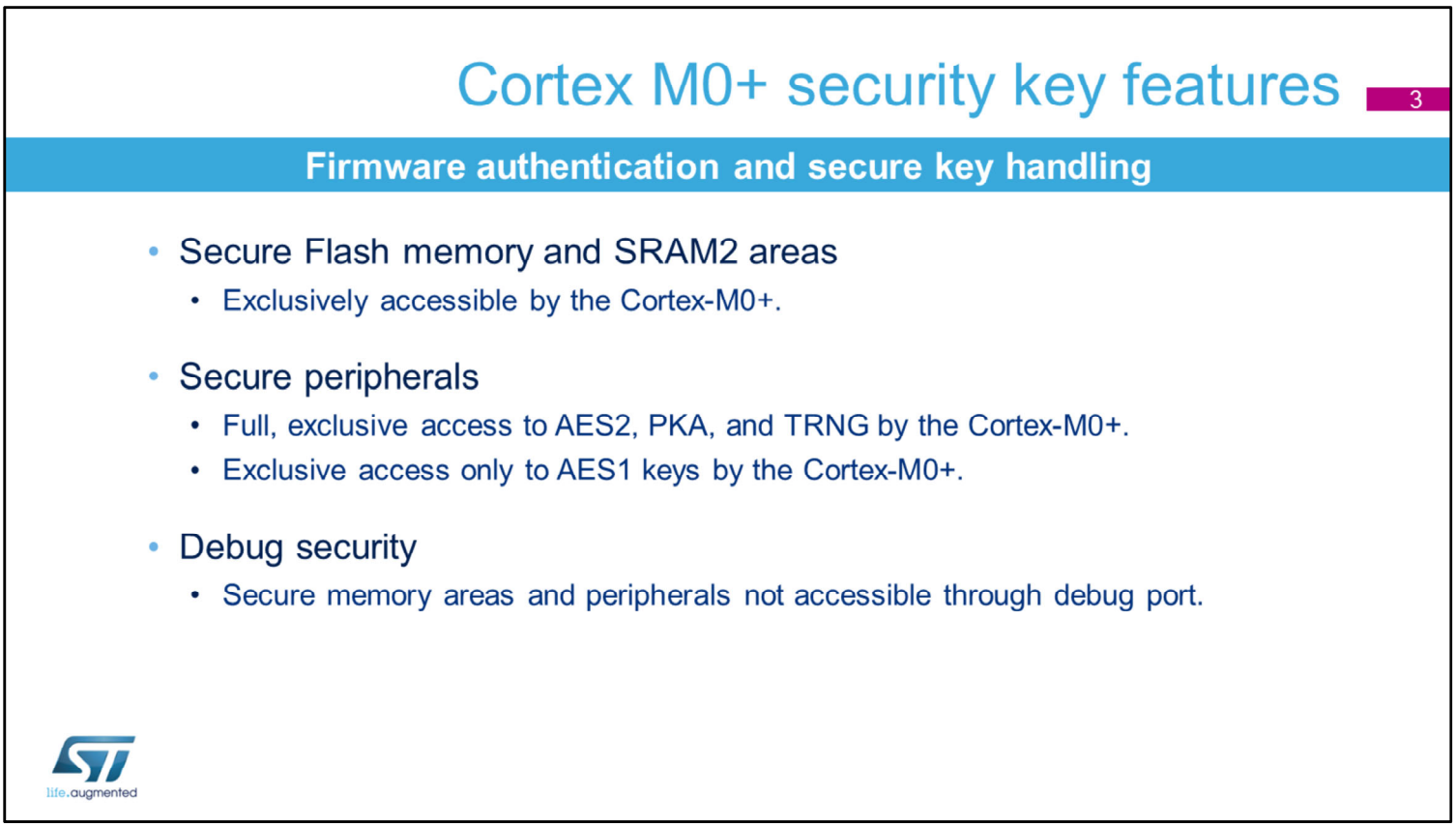


- The Cortex-M0+ security manages:
  - Exclusive Cortex-M0+ access.
  - Cortex-M0+ firmware security in:
    - Flash memory and SRAM2
    - Debug access
  - Peripheral security for:
    - AES, PKA, and TRNG
- Control through secure user options and SYSCFG secure register bits.

Application benefits

- Storage of application keys on the secure CM0+ side.
- Secure cryptography
- Authentic and secure ST radio firmware updates

The Cortex M0+ security manages the firmware and peripheral security, and is used to authenticate the ST radio firmware and allows the secure handling of cryptographic keys.
The Cortex M0+ security uses secure options to control Flash memory, SRAM2 and Debug security. The AES encryption machine, Private Key Accelerator, and True Random Number Generator are peripherals whose security is managed dynamically by the secure Cortex-M0+ core through secure register bits in the System Configuration block.



The Cortex-M0+ security is based on giving exclusive access to a secure area in Flash memory and in SRAM2a and SRAM2b.
Additionally, peripherals such as AES1, AES2, Private Key Accelerator and True Random Number Generator can be made secure, to allow secure cryptography and key generation.
The secure memory areas and peripherals are not accessible by the Cortex-M4 and neither through the debugger.

Cortex M0+ security

- Flash memory and SRAM2 areas and CM0+ Debug Security
  - Enabled by ST at STM32WB production after RSS programing.
  - Parameter modified by Secure Firmware updated via RSS.
- Secure peripherals
  - Enabled by Connectivity firmware running on CM0+
    - AES2, PKA, and TRNG security autonomously handled by CM0+.
    - AES1 key security handled by CM0+ on CM4 application request.

life.augmented

The Cortex M0+ security is completely handled by the Cortex M0+ itself. At STM32WB production, the Cortex M0+ security is enabled after the Root Security Service (RSS) firmware has been programmed into the User Flash memory. Any subsequent Cortex M0+ firmware update (Connectivity stack, or RSS) is handled by the RSS and modifies the Cortex M0+ security parameters as needed.
The AES2, PKA, and RNG security is fully handled by the Cortex M0+ whenever needed by the Cortex M0+ firmware. The AES1 key security is also managed by the Cortex M0+ when requested by the Cortex M4 application firmware.

Secure Options Registers

- Cortex-M0+ security is configured by secure User Options.

Register	Fields									
OPTR (*)	User Options								ESE	RDP
SFR (*)	res.						DDS	res.	FSD	SFSA
SRRVR (*)	C2OPT	NBRSD	SNBRSA	res.	BRSD	SBRSA	SBRV			

*OPTR: Options Register
*SFR: Secure Flash Register
*SRRVR: Secure Ram and Reset Vector Register

- When the Cortex-M0+ security is enabled, the secure User Options are exclusively writable by the Cortex-M0+.
  - The non-secure Cortex-M4 can read the secure User Options for example to determine the size of the secure areas.

life.augmented

The Cortex-M0+ security is controlled through secure user options loaded at device startup in the Secure Flash Register and Secure RAM and Reset Vector Register.
The secure user options can only be modified by the secure Cortex-M0+, i.e. to change parameters when a secure Cortex-M0+ software is updated.
The non-secure Cortex-M4 has read access to the secure user options to be able to determine the start of the secure areas.

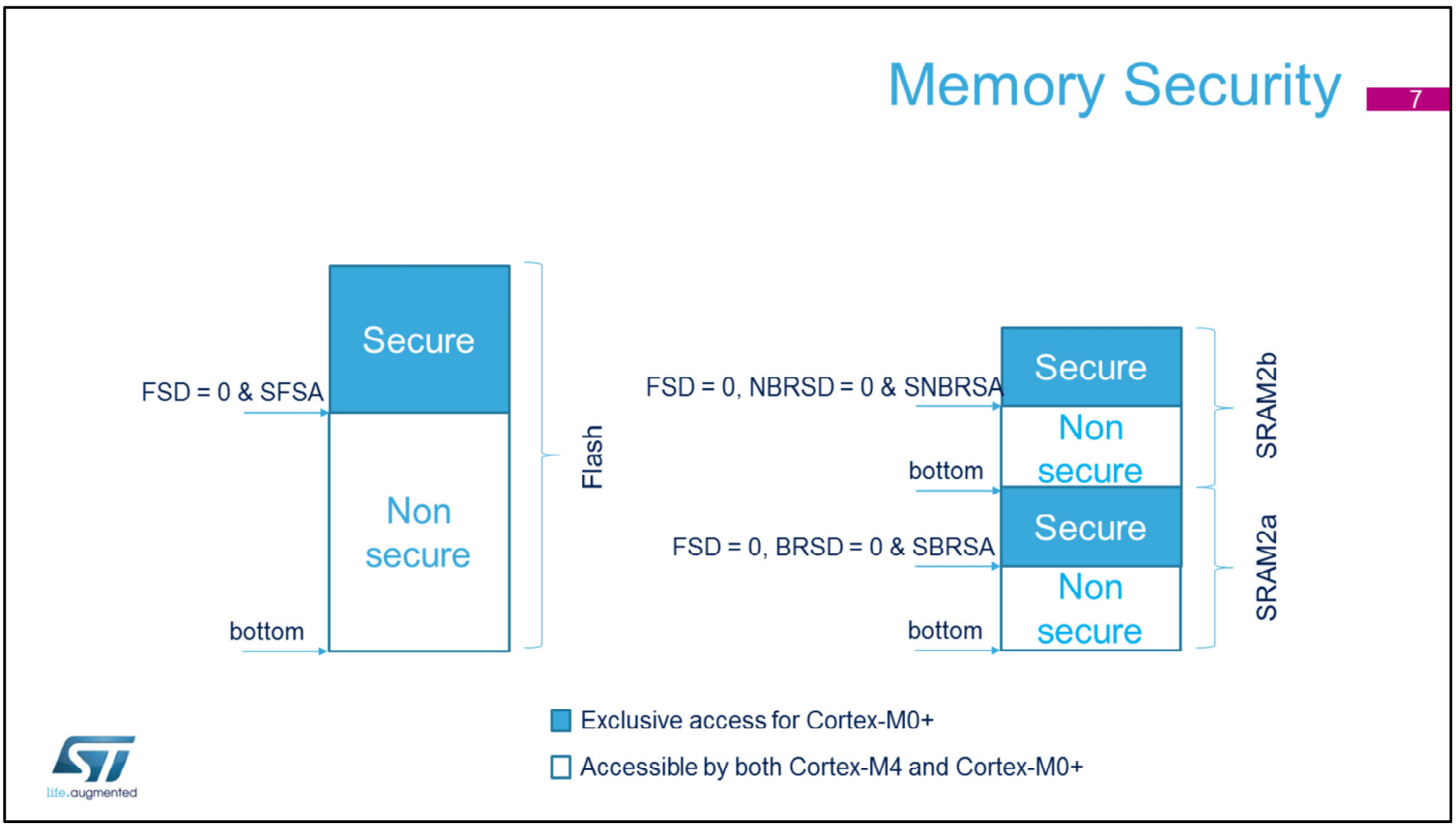
Secure user options

- Memory security handled by secure user options
- Flash memory security
  - Security enable (**FSD**) ➔ Global enable of the Cortex-M0+ security
  - Secure Flash Start Address (**SFSA**)
    - The Flash memory is secure from this start address until the top of the flash memory.
- RAM security
  - RAM security enable (**BRSD:** backup RAM2a) (**NBRSD:** non-backup RAM2b)
  - Secure RAM Start Address (**SBRSA:** backup RAM2a) (**SNBRSA:** non-backup RAM2b)
    - The RAM is secure from its start address until the top of the RAM.
- Enable security environment (**ESE**)
  - This bit a read-only bit as the security is always enabled.

life.augmented

Memory security is enabled and configured by secure user options.
The Flash Security Disable bit, enables the Global Cortex-M0+ security.
The Secure Flash Start Address, defines the start address from which the Flash memory is secure.
The Backup RAM Security Disable bit controls the security on the backup RAM, and the Secure Backup RAM Start Address defines the start address from which the backup RAM is secure.
The Non Backup RAM Security Disable bit is used to enable security on the non-backup RAM, and the Secure Non Backup RAM Start Address defines the start address from which the non-backup RAM is secure.
The Debug access to the secure areas is controlled by the Debug Disable Security bit.
The Enable Security Environment bit is a read-only bit as

the security is always enabled on the Cortex-M0+ core.



The top of the memories can be secured for exclusive Cortex-M0+ access.
The top of the Flash memory, starting from the Secure Flash Start Address, is secure when the Flash Security Disable bit (FSD) is set to “0”.
The top of the backup SRAM2a, starting from the Secure Backup RAM Start Address (SBRSA), is secure when both the Flash Security Disable and Backup RAM Security Disable (BBRSD) bits are set to “0”.
The top of the non-backup SRAM2b, starting from the Secure Non-Backup RAM Start Address (SNBRSA), is secure when both the Flash Security Disable and Non-Backup RAM Security Disable (NBRSD) bits are set to “0”.
It is possible to only secure the Flash memory without any RAM security; however, it is recommended to secure both the Flash memory and RAM used by the Cortex-

M0+ software.

Cortex-M0+ boot reset vector

- The Cortex-M0+ boot reset vector is programmed in the Secure Boot Reset Vector (**SBRV**) option.
  - Word-aligned value.
- The Cortex-M0+ may boot from Flash memory or SRAM2 (a or b) as selected by the Secure CPU2 option (**C2OPT**).
- At production, the Cortex-M0+ boot reset vector is set in Flash memory at the RSS boot reset vector.

life.augmented

The Cortex-M0+ boot reset vector is to be programmed in the secure boot reset vector option and secure CPU2 option. At production, the Cortex-M0+ boot reset vector points to the Root Secure Service start address in Flash memory. In Secure mode, the Cortex-M0+ boot reset vector can only be changed by the secure Cortex-M0+ side.

Debug disable

Debug access handled by secure options

- Debug access control is independent from security
- Controlled by the Secure Debug Disable option (**DDS**)
  - Disable debug port access to the Cortex-M0+
- Debug can be enabled and disabled in Secure and Non-secure modes.
  - In secure mode debug access can only be changed by the secure Cortex-M0+ side.

life.augmented

Cortex-M0+ debug access is controlled by the Debug Disable Option bit. It is independent from security and can be enabled and disabled in both Secure and Non secure modes. In Secure mode, debug access control can only be changed by the secure Cortex-M0+ side.

Security & memory erase

- Flash Page Erase
  - Secure pages can only be erased by the secure Cortex-M0+.
- Flash Mass Erase
  - The Flash memory can only be mass erased when requested by the Cortex-M0+.
  - Flash Mass Erase operations requested by the non-secure Cortex-M4 are rejected.
- Flash Erase due to RDP regression
  - Only the non-secure Flash memory area is multiple page erased.
- Flash Mass Erase due to RDP regression
  - Flash Mass Erase and SRAM2 erase is performed and security including RSS are removed.
  - ST radio stack authentication is lost and can no longer be programmed.

life.augmented

The STM32WB has a single Flash memory for both the Coretex-M4 and Cortex-M0+ software. The Cortex-M0+ security prevents secure Flash memory pages from being erased by the non-secure Cortex-M4. A Cortex-M4 Flash Mass Erase operation will be rejected, and a Multiple Block Erase has to be used to erase the Cortex-M4 software.

When regressing the ReaD Protection from Level 1 to Level 0, only the non-secure part of the Flash memory will be erased. The secure Cortex-M0+ software will be retained.

The complete Flash memory is mass erased and the security is removed only when regressing the ReaD Protection from Level 1 to Level 0. In this case, the ST radio stack authentication and security is lost and can no longer be programmed.

Secure System Configuration bits

- Secure System Configuration bits are used to handle peripheral security
  - Peripheral security is only available when Security is enabled in (FSD)
    - AES1 key security, enabled by SAES1
      - A secure application key storage feature is provided by the Cortex-M0 software.
    - AES2 full security, enabled by SAES2
    - PKA full security, enabled by SPKA
    - True RNG full security, enabled by SRNG
  - Peripheral security
    - can be managed dynamically.
    - is enabled/disabled by the secure Cortex-M0+.
    - security enable bits can be read by the Cortex-M4.

life.augmented

The AES accelerator 1, AES accelerator 2, Public Key Accelerator and True Random Number Generator peripherals can dynamically be made secure by Cortex-M0+ firmware through secure register bits in the System Configuration block. The AES 2, Public Key Accelerator and True Random Number Generator peripherals provide full peripheral security. The AES 1 provides only key security, which allows the application running on the Cortex-M4 to use cryptography with a secure key. Secure key storage is provided by the Cortex-M0+ firmware.
The Cortex-M4 may read the peripheral security bit to determine its security status.

Secure Cryptography

- Radio stack cryptographic keys are generated and stored at the secure Cortex-M0+ side.
- Cortex-M0+ radio stack provide cryptographic key management features (CKS: Cryptographic Key Storage):
  - Allows the Application to generate and store cryptographic keys.
  - Allows the Application to load a cryptographic key stored in the secure AES1.

life.augmented

The radio stack running on the Cortex-M0+ provides cryptographic key management to the Application
The cryptographic keys are generated and stored on the secure Cortex-M0+ side using the Cryptographic Key Storage (CKS).

Secure Firmware Update

13

- Secure firmware can only be updated via the secure RSS, running on the Cortex-M0+.
  - The RSS is preprogrammed at STM32WBxx factory level.
- Secure firmware download is enabled through:
  - ICP via the system bootloader
  - IAP including OTA.
- The secure Cortex-M0+ is able to update the user options in all RDP levels.
- Secure firmware
  - Radio stack
  - RSS

life.augmented

The STM32WB includes a preprogrammed RSS which allows the secure Cortex-M0+ software to be updated. Both the Radio stack software and the RSS itself can be updated.
Secure software can be downloaded via In-Circuit Programming by the system bootloader or via In-Application Programming by an application bootloader including Over The Air (OTA).
Secure Cortex-M0+ software update is possible in all ReaD Protection levels (0, 1, and 2).

Events

Cortex-M4 action:	Generated event:
Cortex-M4 write access* to secure RAM memory area	Bus error
Cortex-M4 write access to secure peripheral registers	Bus error
Cortex-M4 requesting a mass erase of secure flash	Bus error
Cortex-M4 requesting a page erase of a secure flash page	Bus error
Cortex-M4 requesting a secure flash page	Bus error
Cortex-M4 data write operation to secure flash	Bus error
Cortex-M4 read access to secure flash memory area	Bus error + read zero value
Cortex-M4 read access to secure RAM memory area	Read zero value
Cortex-M4 read access to secure peripheral registers	Read zero value

* When RDP level is 1 and booting from SRAM1 no bus error is generated. (SRAM2 is locked)

life.augmented

This slide lists the events generated by the Cortex-M0+ security feature. Events are only generated to the non-secure Cortex-M4. Depending on the Cortex-M4 access type, a bus error is generated to the non-secure Cortex-M4. Reading secure areas returns zeros. Only the secure user options and system configuration peripheral security enable bits can be read by the non-secure Cortex-M4.

Related peripherals

- Refer to these trainings linked to this feature:
  - STM32WB Power control (Flash memory interface)
    - Secure user options
  - STM32WB System configuration (SYSCFG)
    - Secure peripheral enable bits
  - BLE stack
    - Secure Cortex-M0+ BLE stack

life.augmented

In addition to this training, you may find the flash memory interface and system configuration modules useful.