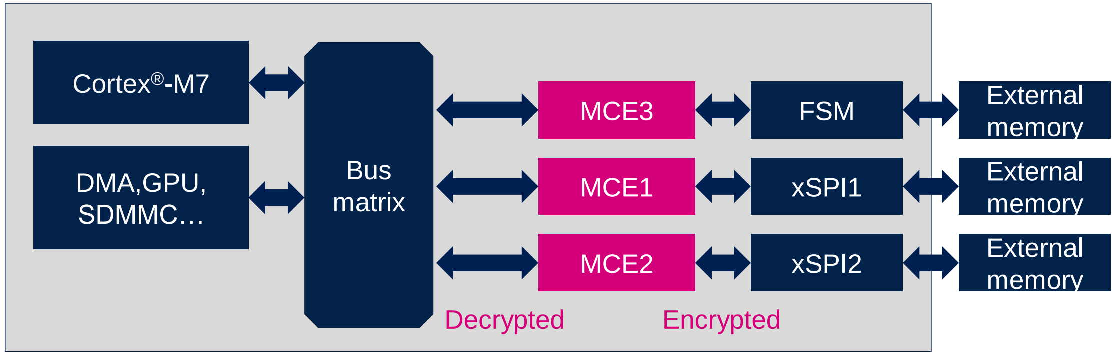
life.augmented

STM32H7R/S workshop bootflash MCU + OSPI + MCE

Overview

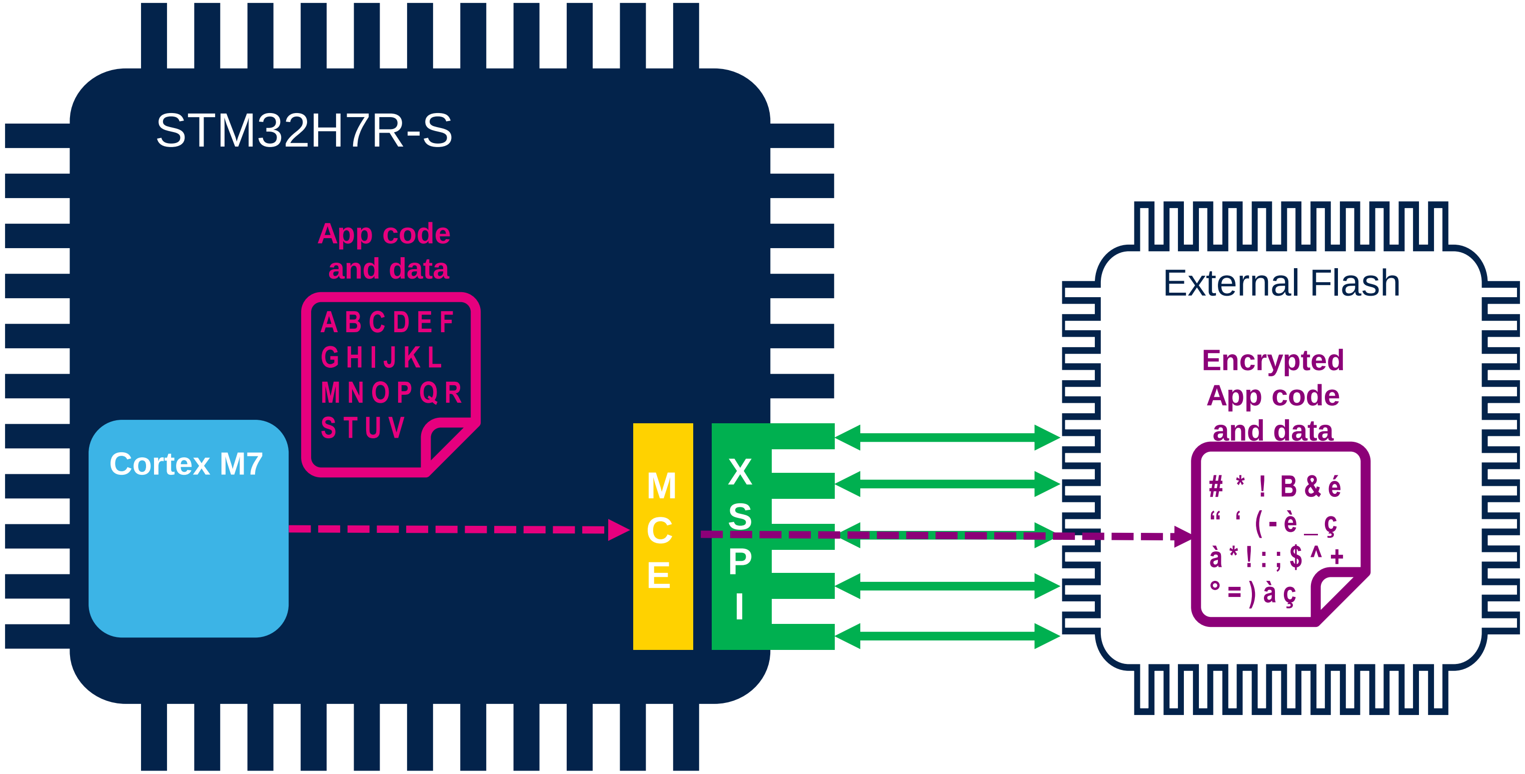
- External memory in-line encryption/ decryption, during memory-mapped operations
- MCE location:



Application benefits

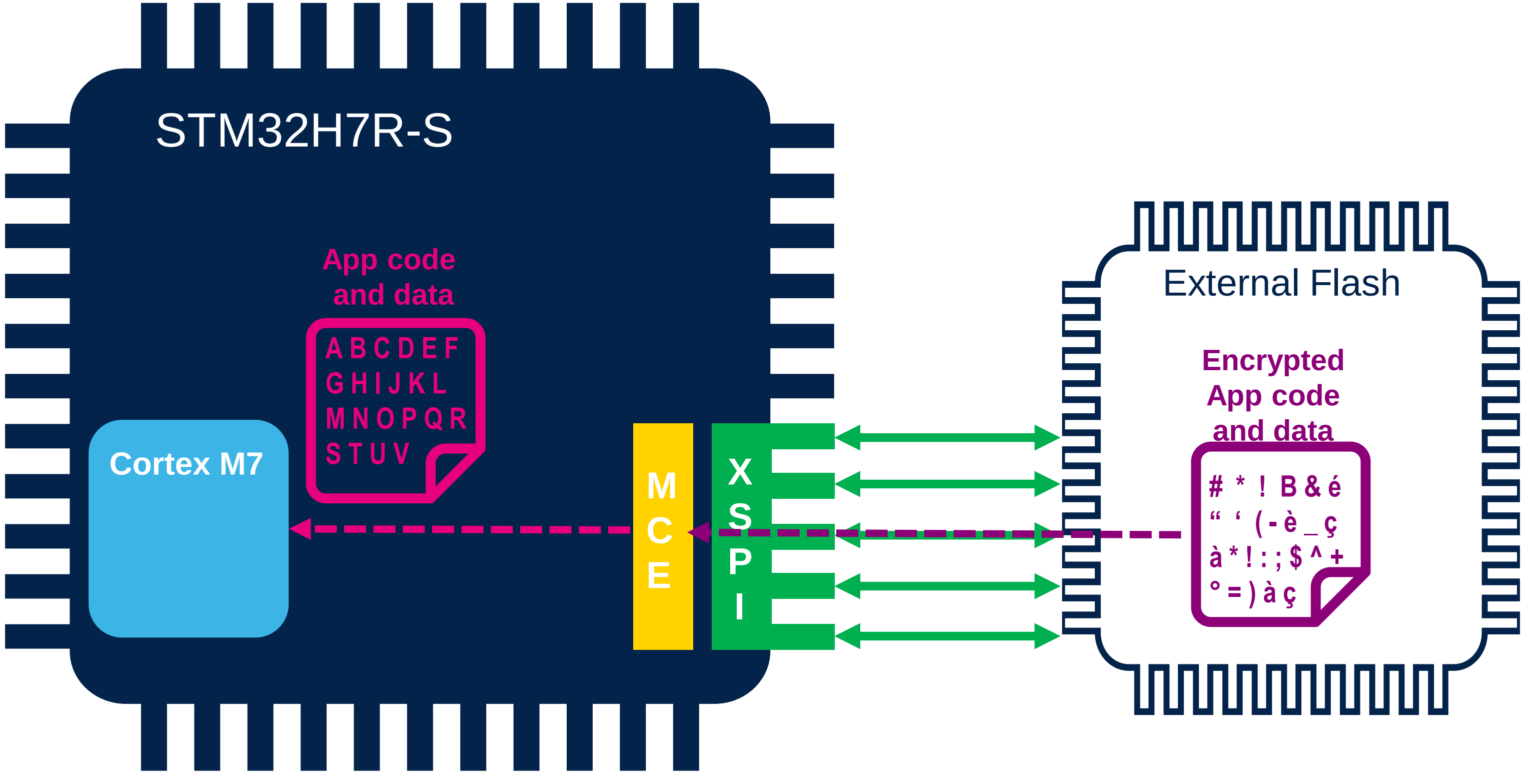
- External memory protection (NOR, SRAM)
- Up to 4 encrypted regions per MCE
- Security versus performance selection
  - From zero latency stream cipher to side-channel protected block cipher
- Embedded firewall (privilege, write)

Memory Cypher Engine Encrypt

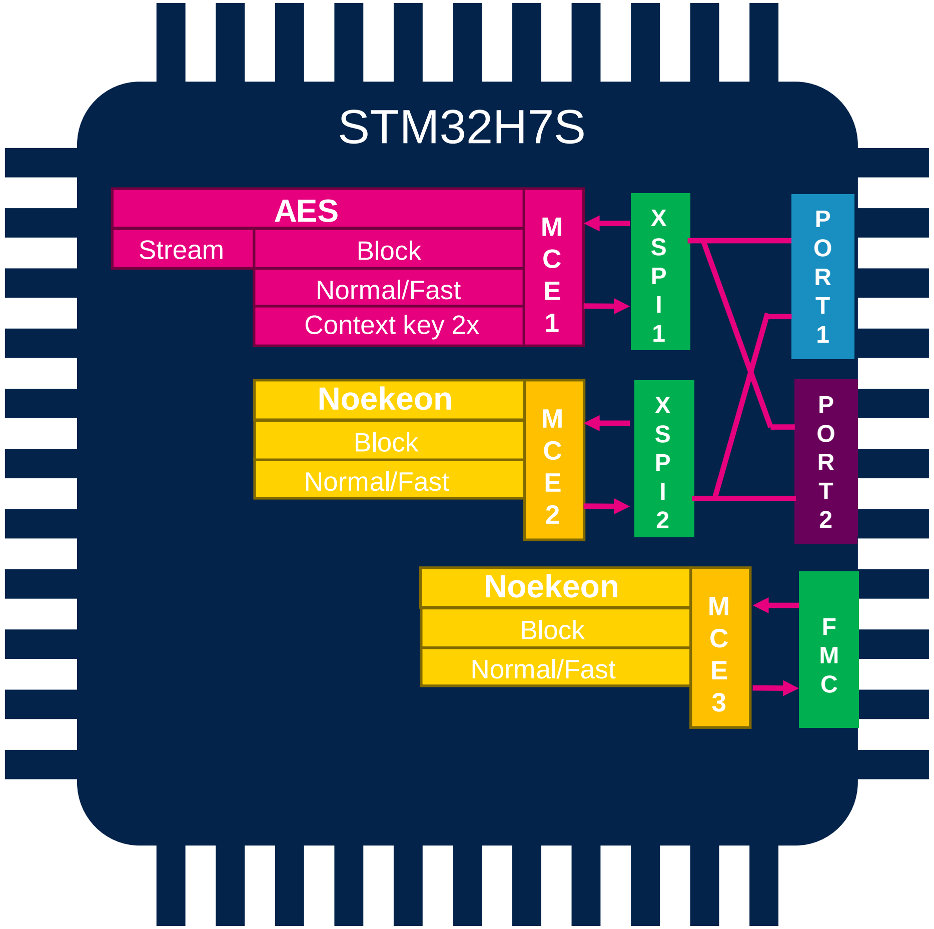


life.augmented

Memory Cypher Engine Decrypt



Memory Cypher Engine



Block Mode

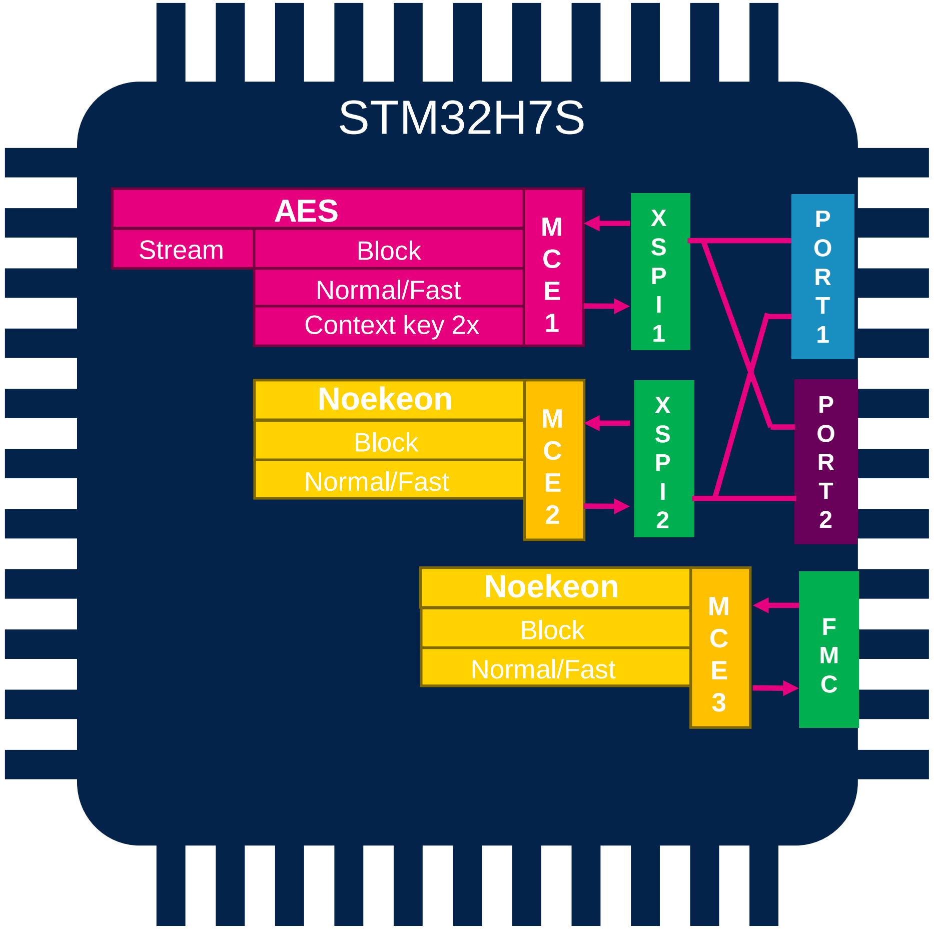
Cipher	Mode	AXI latency 16B data	Sequential access
AES	Normal	4+11=25	No
	Fast	4+11=15	No
Noekeon	Normal	14+7=21	No
	Fast	4+7=11	No

Stream Mode

Cipher	Mode	AXI latency 16B data	Sequential access
AES	Normal	11	Yes

life.augmented

Memory Cypher Engine



Block Mode

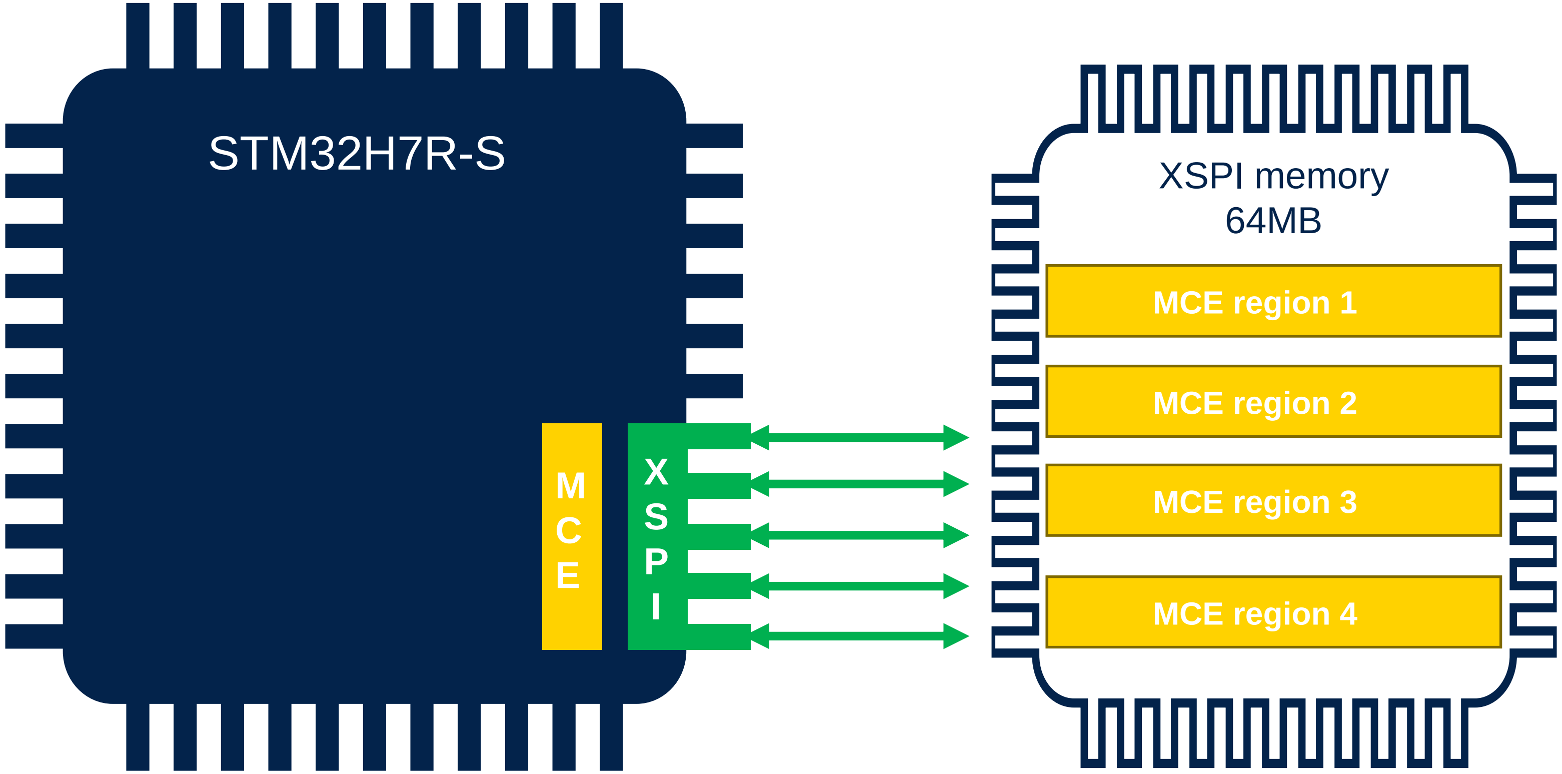
Cipher	Mode	AXI latency 16B data	Sequential access
AES	Normal	4+11=25	No
	Fast	4+11=15	No
Noekeon	Normal	14+7=21	No
	Fast	4+7=11	No

Stream Mode

Cipher	Mode	AXI latency 16B data	Sequential access
AES	Normal	11	Yes

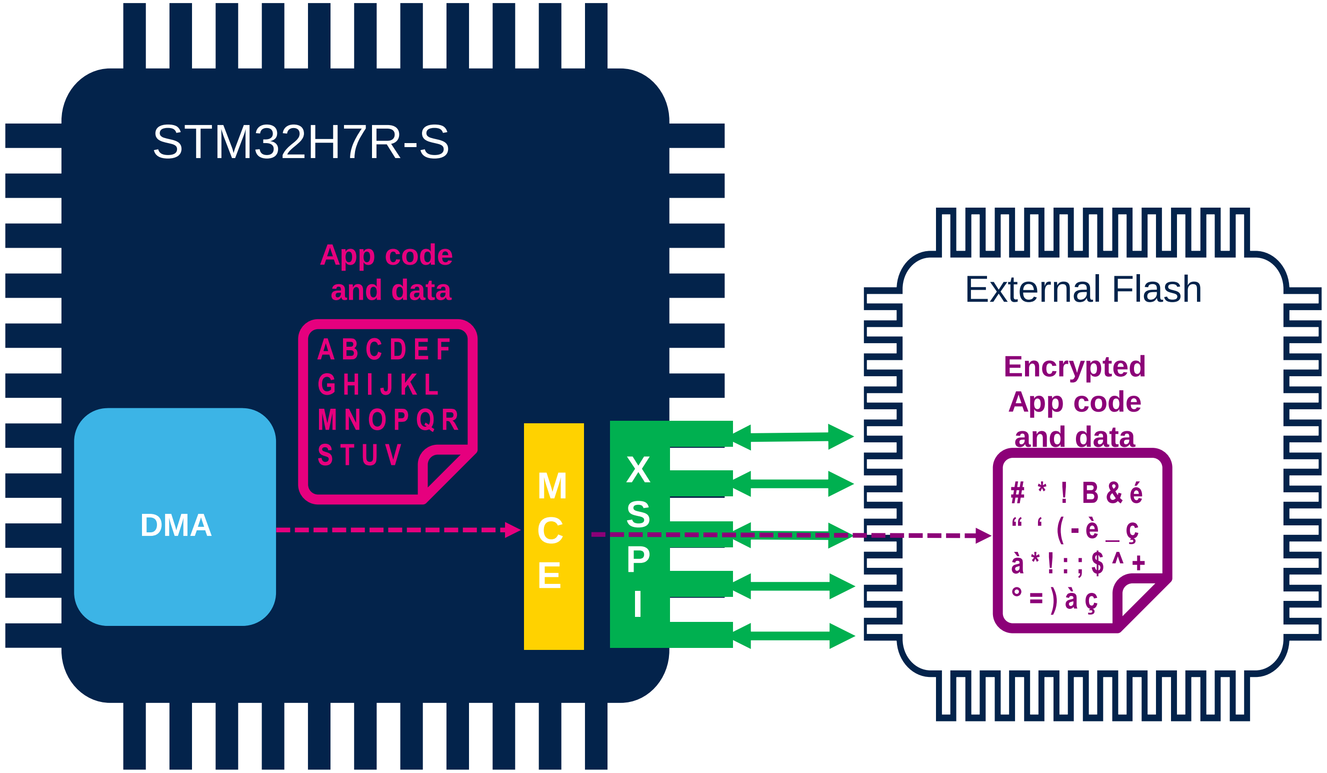
life.augmented

Memory Cypher Engine Stucture



- MCE can define up to 4 regions (granularity 4KB)
- Each region is defined by :
    - Address range
    - Crypto configuration

MCE encryption constraint



- MCE encrypt the external flash memory in memory map mode.
- To write in an external NOR flash, you need specific code sequence and guarantee it’s not interrupted.
- DMA should be used.

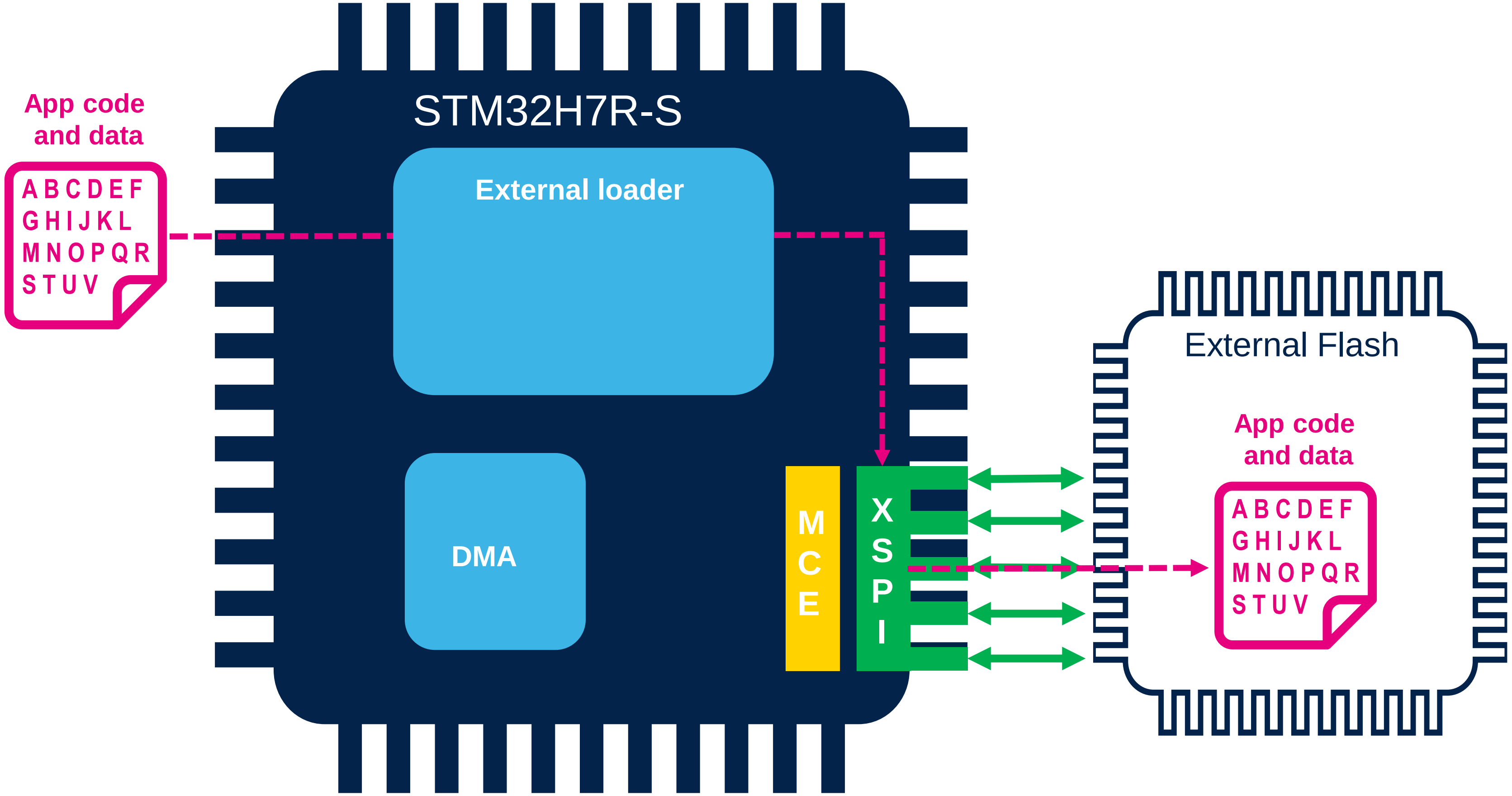
life.augmented

External loader and MCE

life.augmented

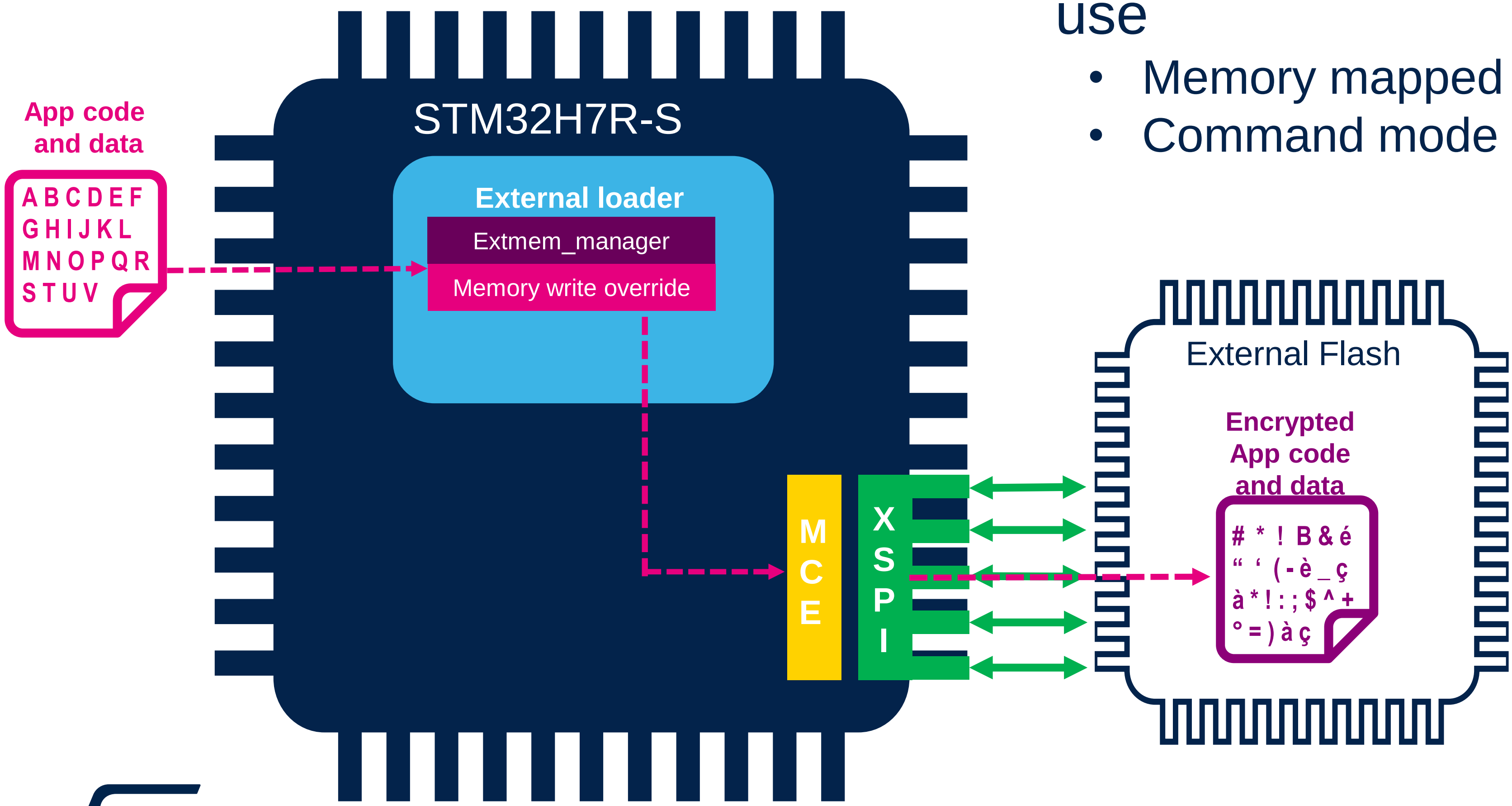
External loader default behavior

- By default, external loader program directly the memory thanks xSPI and in command mode



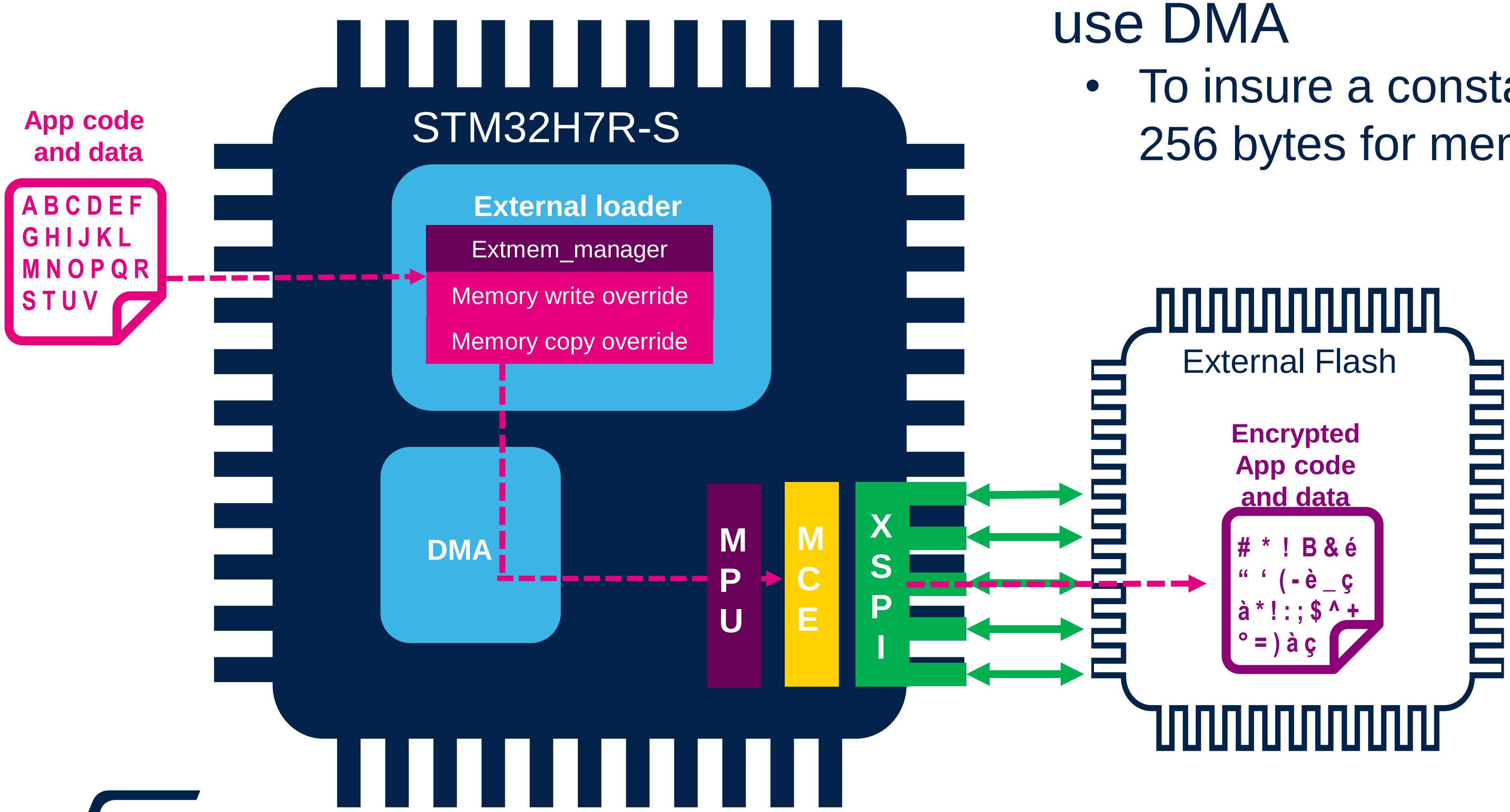
External loader and MCE

- We need to override memory write function to use
  - Memory mapped mode for memory programming
  - Command mode for access (erase, unlock)



External loader and MCE

- We need to override memory copy function to use DMA
  - To insure a constant 16byte write for the MCE and 256 bytes for memory(without read)



Remark : MPU should be configured to avoid access to unmapped region

Our technology starts with You

Find out more at www.st.com

© STMicroelectronics - All rights reserved.
ST logo is a trademark or a registered trademark of STMicroelectronics International NV or its affiliates in the EU and/or other countries.
For additional information about ST trademarks, please refer to www.st.com/trademarks.
All other product or service names are the property of their respective owners.

life.augmented