Navigate new EU security regulations with STM32 wireless solutions

February 2026

Romain Jayles / Thierry Crespo

What you can expect from today’s session

GOALS

RED & CRA regulations: impacts and ways to compliance

- Re-explore RED & CRA regulations
- Understand the STM32 policies
- Provide you with explanations on our policies
- Get to know the documents provided to help your compliance
- Understanding of security examples provided to help
- Spend time to answer your questions

RED & CRA regulations

Cybersecurity: RED & CRA regulations

STM32 Explore | On-demand webinar

Navigate new European security regulations with STM32Trust

This webinar was broadcasted on January 28, 2025

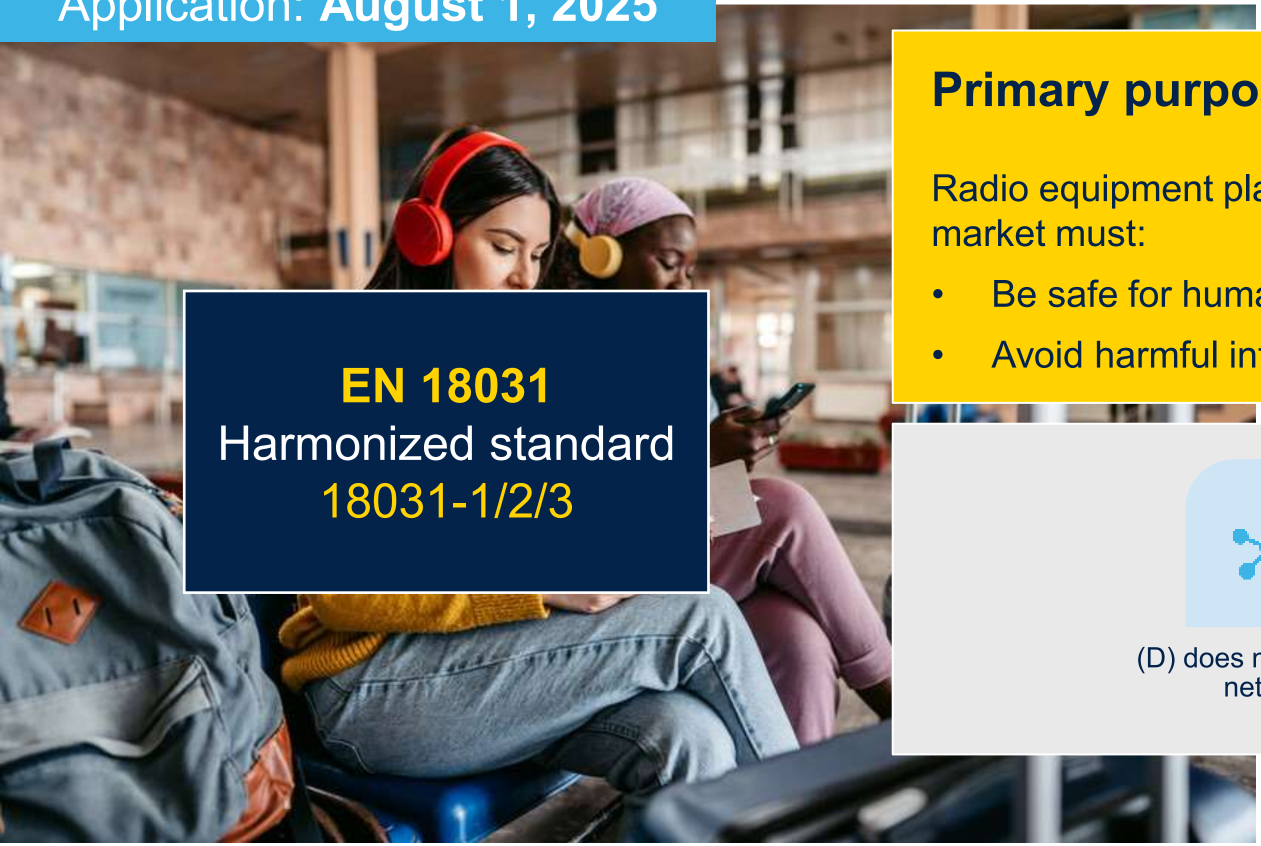
Deep dive into
RED & CRA
-
STM32Trust helps you
to meet conformance

Recap
Risk analysis
STM32 & STSAFE
security functions
Questions & answers

Cybersecurity: RED & CRA regulations

RED | **CRA** | **STM32Trust** | **STSAFE-A**

Application: **August 1, 2025**



EN 18031
Harmonized standard
18031-1/2/3

Primary purpose

Radio equipment placed on the EU market must:

- Be safe for humans and animals
- Avoid harmful interference

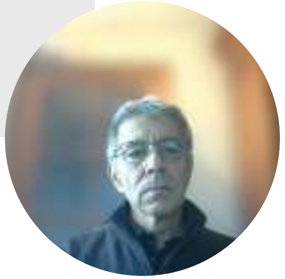
Cybersecurity requirements

- Active since October 2021
- Known as article **3.3 d,e,f**

(D) does not harm the network

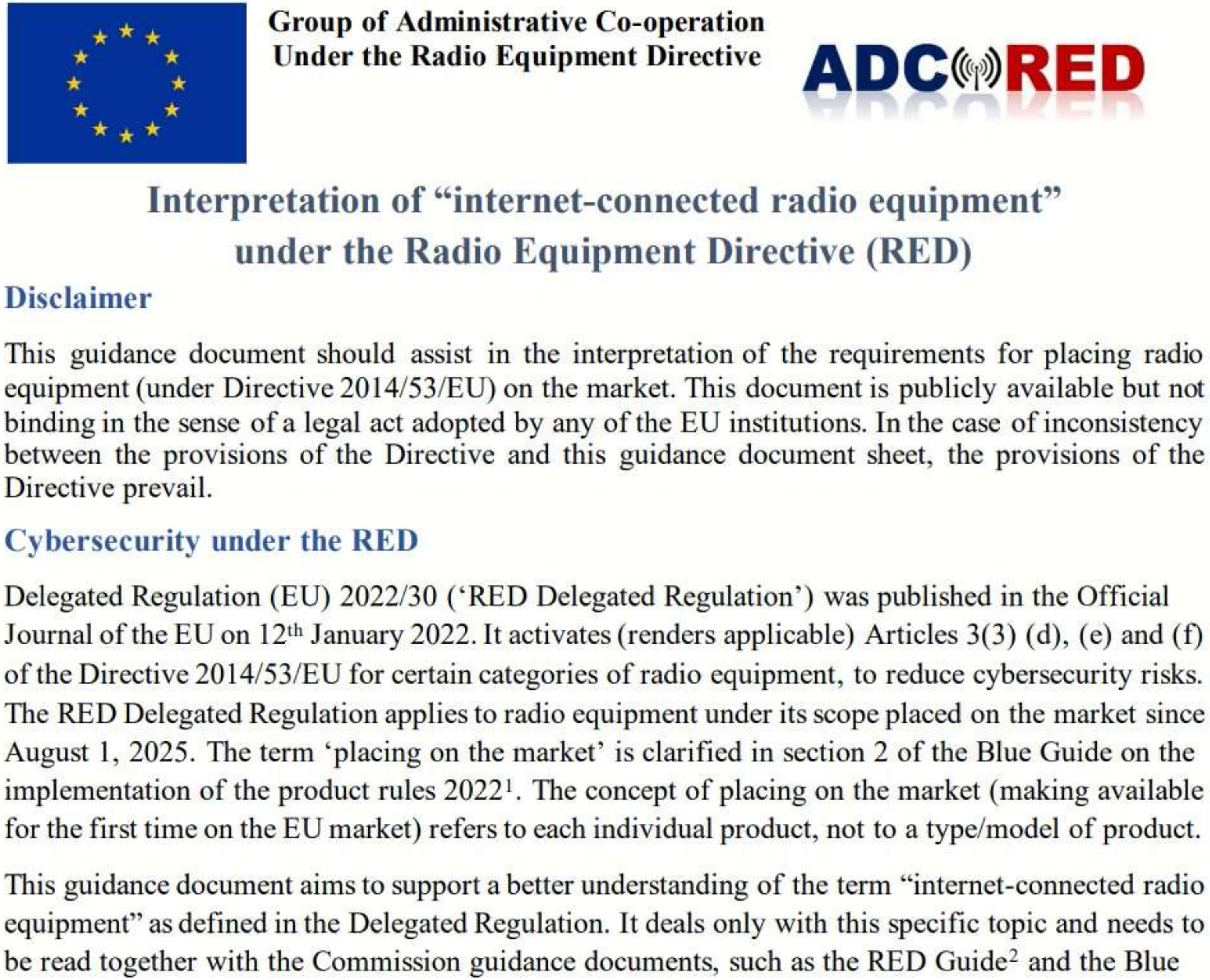
(E) personal data and privacy of the user and subscriber are protected

(F) ensuring protection from fraud



New

Interpretation of “internet-connected radio equipment” under the Radio Equipment Directive (RED) | Internal Market, Industry, Entrepreneurship, and SMEs



Group of Administrative Co-operation
Under the Radio Equipment Directive

ADCO RED

Interpretation of "internet-connected radio equipment" under the Radio Equipment Directive (RED)

Disclaimer

This guidance document should assist in the interpretation of the requirements for placing radio equipment (under Directive 2014/53/EU) on the market. This document is publicly available but not binding in the sense of a legal act adopted by any of the EU institutions. In the case of inconsistency between the provisions of the Directive and this guidance document sheet, the provisions of the Directive prevail.

Cybersecurity under the RED

Delegated Regulation (EU) 2022/30 ('RED Delegated Regulation') was published in the Official Journal of the EU on 12th January 2022. It activates (renders applicable) Articles 3(3) (d), (e) and (f) of the Directive 2014/53/EU for certain categories of radio equipment, to reduce cybersecurity risks. The RED Delegated Regulation applies to radio equipment under its scope placed on the market since August 1, 2025. The term 'placing on the market' is clarified in section 2 of the Blue Guide on the implementation of the product rules 2022[1]. The concept of placing on the market (making available for the first time on the EU market) refers to each individual product, not to a type/model of product.

This guidance document aims to support a better understanding of the term "internet-connected radio equipment" as defined in the Delegated Regulation. It deals only with this specific topic and needs to be read together with the Commission guidance documents, such as the RED Guide[2] and the Blue

STM32 Trust

STSECURE

Cybersecurity: RED & CRA regulations

RED | CRA | STM32Trust | STSAFE-A

Application: **4Q 2027**

Scope & purpose

Applies to "**all products with digital elements**" (hardware/software) put on the EU market.

Improves security of products through mandatory product and process requirements during the whole life cycle.

Timeline

- 2023 (Q4): text agreed
- 2024 (Q4): publication
- 2026 (H2): application of vulnerability / incident reporting
- 2027 (Q4): application for product & process requirements

Penalties

- **Possible recall or withdrawal of products** for non-compliance with cybersecurity requirements
- **Up to 15M€ or 2.5% WW turnover** for non-compliance with cybersecurity essential requirements
- **Up to 5M€ or 1% WW turnover** for incorrect, incomplete, or misleading information to the authorities

CRA requirements

Essential security requirements (annex I)

Products with digital elements shall be made available on the market only where they meet the essential cybersecurity requirements and the processes put in place by the manufacturer comply with the requirements

- Risk assessment: from assets to mitigation (security functions)
- Secure by design (secure software life cycle)
- No known exploitable vulnerabilities
- Regular security updates
- Resistances to denial-of-service (DoS) attack
- Minimize negative impact on the availability of services provided by others
- Device protection (authentication, confidentiality, integrity)
- Software bill of material (SBOM)
- Vulnerabilities handling, monitoring, disclosure

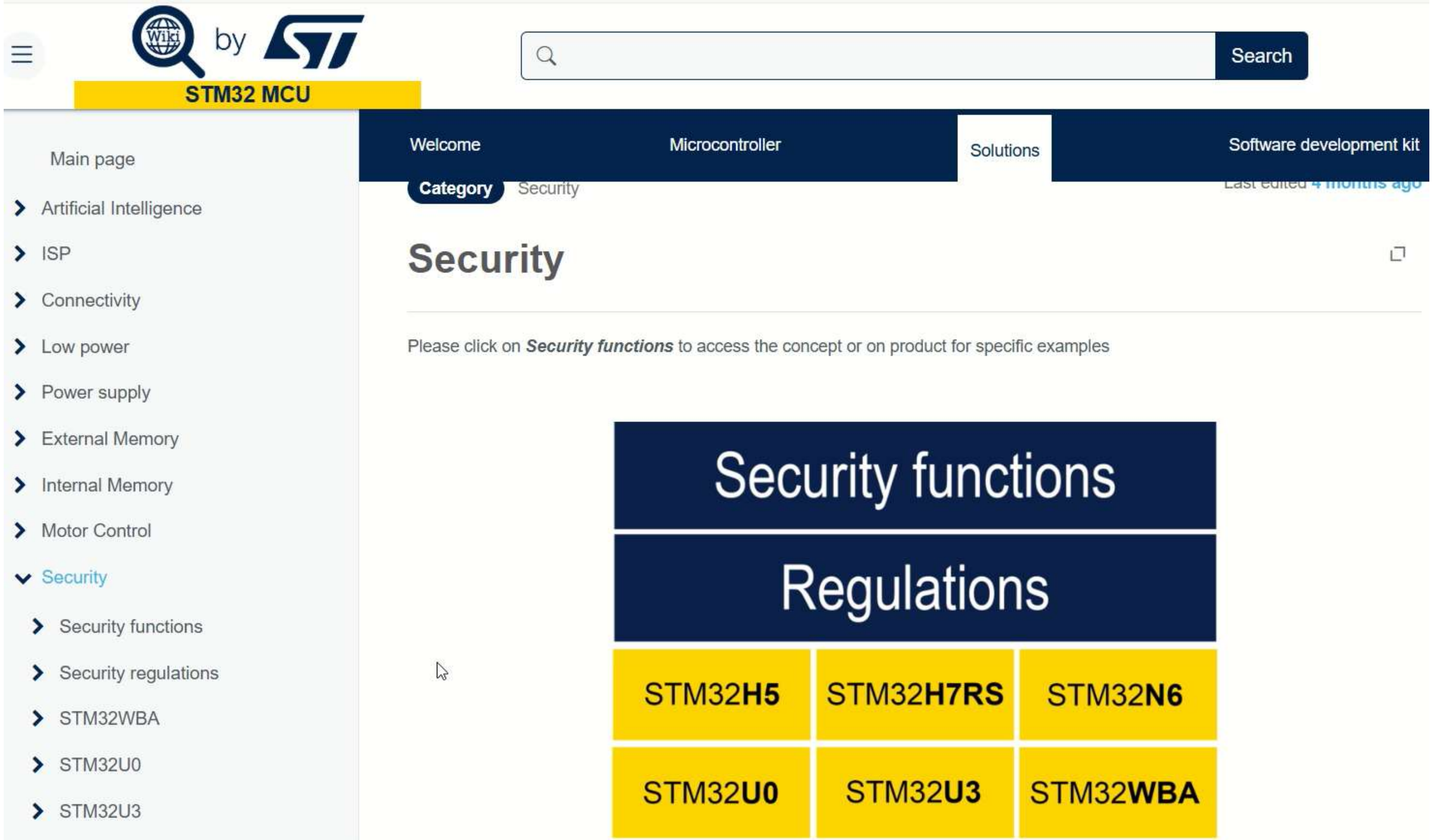
STM32 MCU

STM32 wiki pages Regulations

Where can I find information on STM32?

- Navigate new EU security regulations with ST solutions
- Introduction - stm32mcu
- Deep dive on RED
- Q&A for RED - stm32mcu
- Deep dive on CRA
- Q&A for CRA - stm32mcu
- Regulations on Post Quantum Cryptography - stm32mcu
- PSIRT - stm32mcu
- STM32Trust software security policies - stm32mcu
- STM32 Software security policies Q&A - stm32mcu

STM32 wiki pages
Regulations



Security

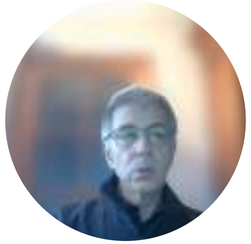
Please click on ***Security functions*** to access the concept or on product for specific examples

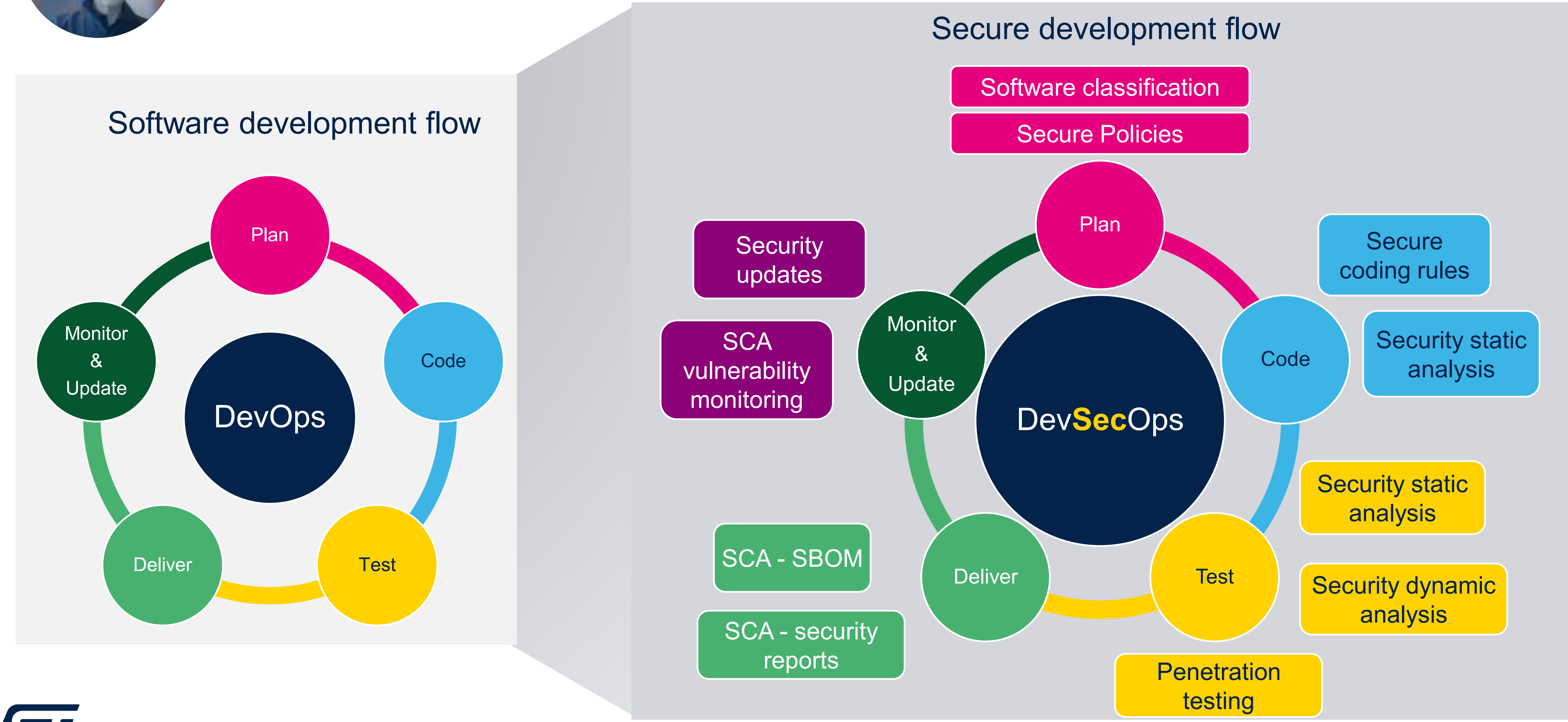
Security functions

Regulations

STM32**H5**	STM32**H7RS**	STM32**N6**
STM32**U0**	STM32**U3**	STM32**WBA**

From DevOps to DevSecOps



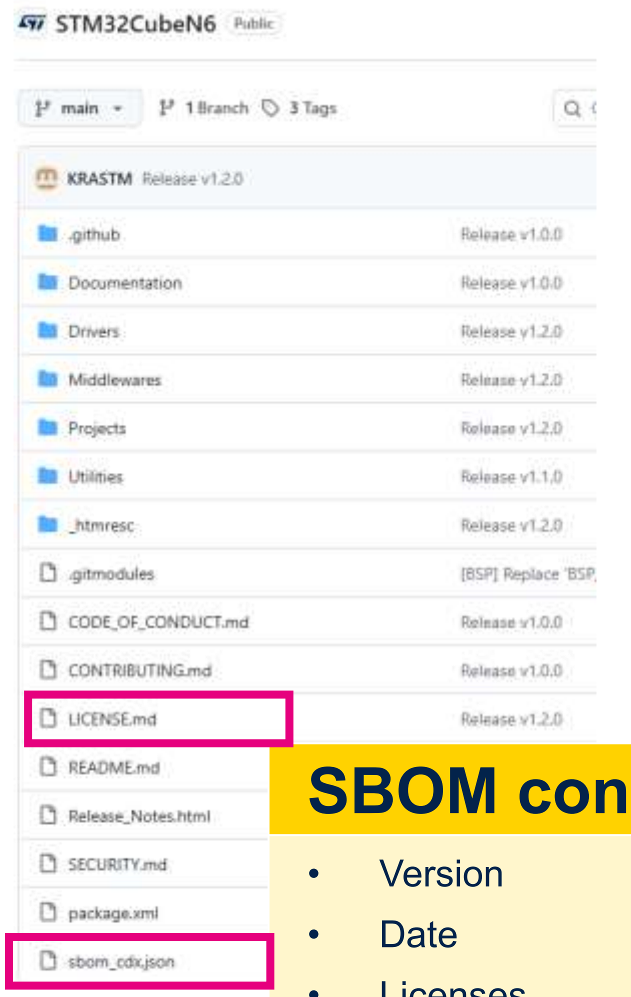


Software bill of material - SBOM

Enables your automated security policies

- ✓ Machine readable – CycloneDX format
- ✓ Additional human readable license file
- ✓ Enables automatic security scan policies
- ✓ Includes open sources & external deliverables
- ✓ Every component is tracked
- ✓ One SBOM file per package: sbom_cdx.json

SBOM management is strongly automated and delivered synchronized with the package delivery - CycloneDX is a modern ECMA standard (ECMA-424) for the software supply chain. The specification originates and is led by the OWASP Foundation and supported by the global information security community.

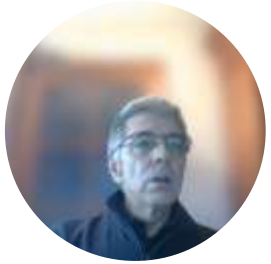


STM32CubeN6 Public

main · 1 Branch · 3 Tags

KRASTM Release v1.2.0

.github	Release v1.0.0
Documentation	Release v1.0.0
Drivers	Release v1.2.0
Middlewares	Release v1.2.0
Projects	Release v1.2.0
Utilities	Release v1.1.0
_htmresc	Release v1.2.0
.gitmodules	[BSP] Replace 'BSP
CODE_OF_CONDUCT.md	Release v1.0.0
CONTRIBUTING.md	Release v1.0.0
LICENSE.md	Release v1.2.0
README.md	
Release_Notes.html	
SECURITY.md	
package.xml	
sbom_cdx.json	



SBOM contents

- Version
- Date
- Licenses
- Copyrights inside License file

Give confidence to ST is compliant

A proof of compliance capabilities

Global Platform SESIP 3

psacertified™
level three

target certifications

Ready for **Radio Equipment Directive** (RED)

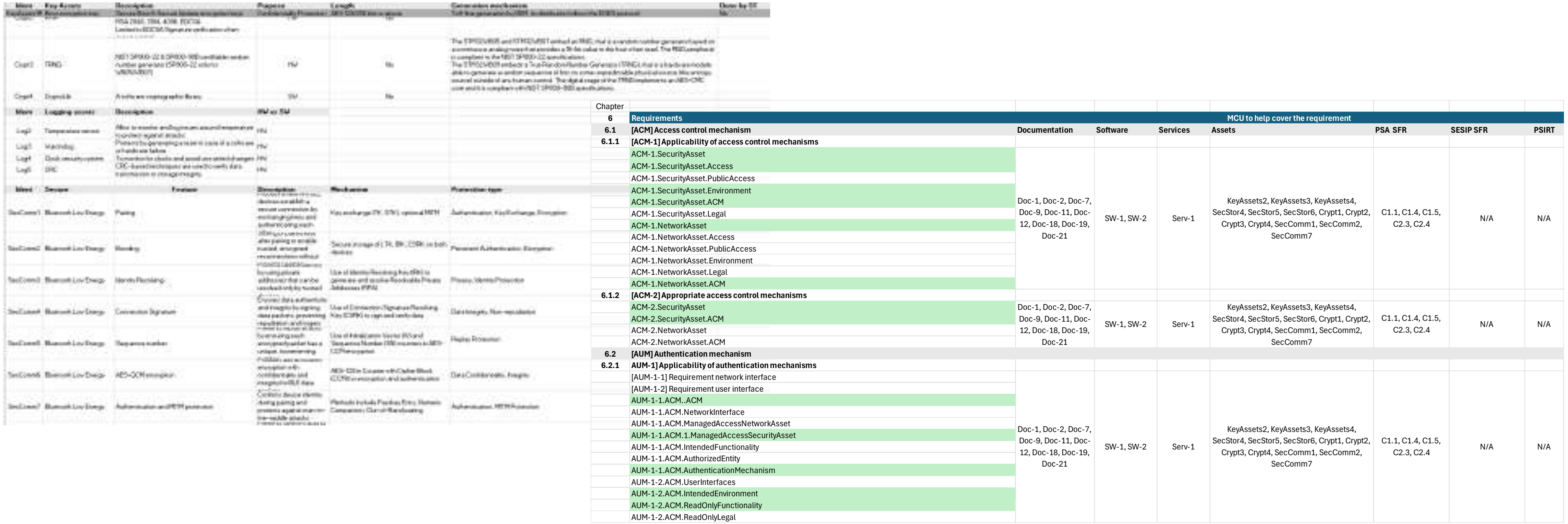
Formal **EU-TEC** done on NUCLEO-WBA55CG

+

Formal **Attestation of Conformance** done on product

Provide a set of documentation for your own certification

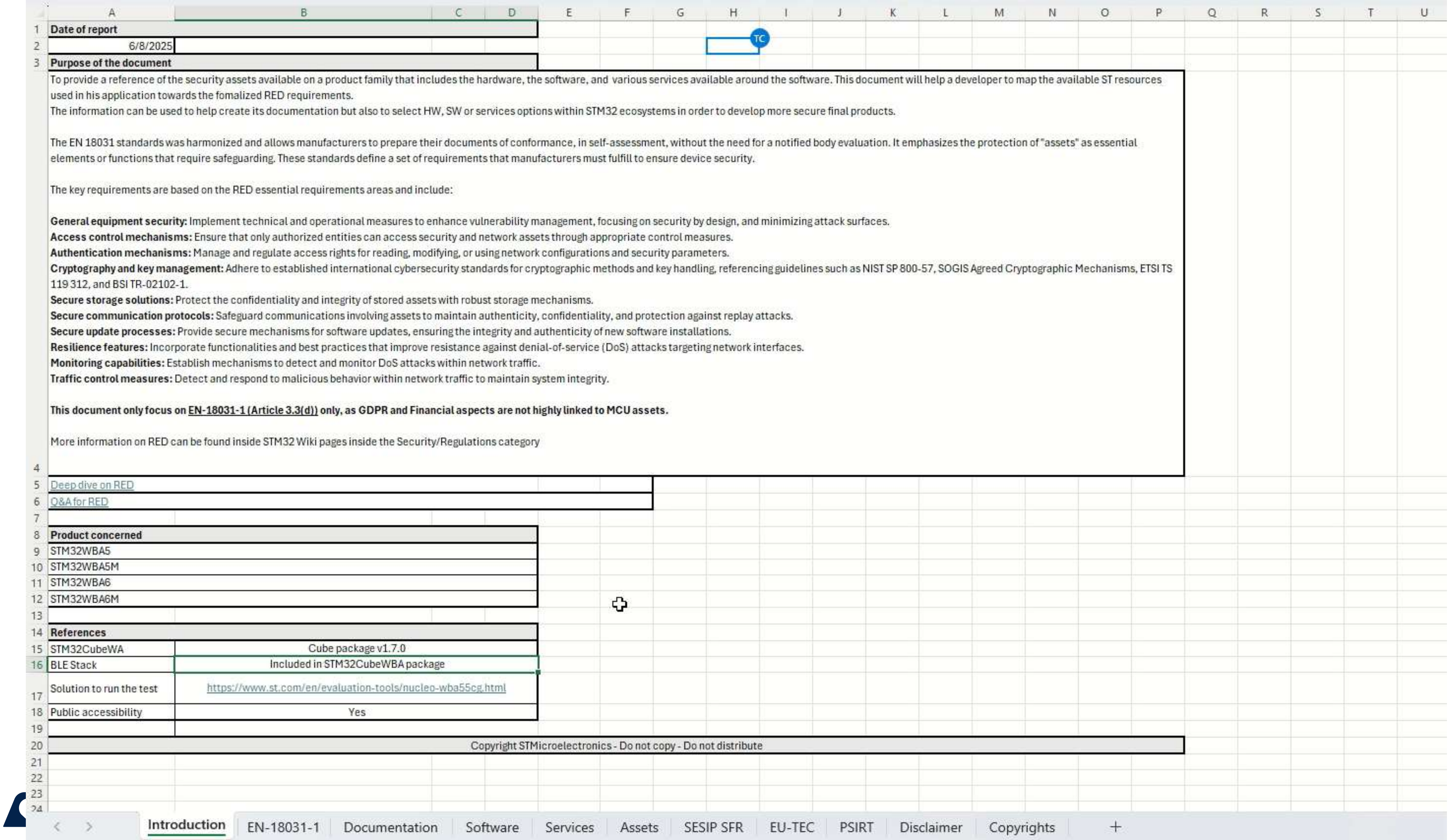
A set of mapping documents to help your compliance claims



Chapter								
6	Requirements	MCU to help cover the requirement						
6.1	[ACM] Access control mechanism	Documentation	Software	Services	Assets	PSA SFR	SESIP SFR	PSIRT
6.1.1	[ACM-1] Applicability of access control mechanisms							
	ACM-1.SecurityAsset	Doc-1, Doc-2, Doc-7, Doc-9, Doc-11, Doc-12, Doc-18, Doc-19, Doc-21	SW-1, SW-2	Serv-1	KeyAssets2, KeyAssets3, KeyAssets4, SecStor4, SecStor5, SecStor6, Crypt1, Crypt2, Crypt3, Crypt4, SecComm1, SecComm2, SecComm7	C1.1, C1.4, C1.5, C2.3, C2.4	N/A	N/A
	ACM-1.SecurityAsset.Access							
	ACM-1.SecurityAsset.PublicAccess							
	ACM-1.SecurityAsset.Environment							
	ACM-1.SecurityAsset.ACM							
	ACM-1.SecurityAsset.Legal							
	ACM-1.NetworkAsset							
	ACM-1.NetworkAsset.Access							
	ACM-1.NetworkAsset.PublicAccess							
	ACM-1.NetworkAsset.Environment							
	ACM-1.NetworkAsset.Legal							
	ACM-1.NetworkAsset.ACM							
6.1.2	[ACM-2] Appropriate access control mechanisms							
	ACM-2.SecurityAsset	Doc-1, Doc-2, Doc-7, Doc-9, Doc-11, Doc-12, Doc-18, Doc-19, Doc-21	SW-1, SW-2	Serv-1	KeyAssets2, KeyAssets3, KeyAssets4, SecStor4, SecStor5, SecStor6, Crypt1, Crypt2, Crypt3, Crypt4, SecComm1, SecComm2, SecComm7	C1.1, C1.4, C1.5, C2.3, C2.4	N/A	N/A
	ACM-2.SecurityAsset.ACM							
	ACM-2.NetworkAsset							
	ACM-2.NetworkAsset.ACM							
6.2	[AUM] Authentication mechanism							
6.2.1	AUM-1] Applicability of authentication mechanisms							
	[AUM-1-1] Requirement network interface	Doc-1, Doc-2, Doc-7, Doc-9, Doc-11, Doc-12, Doc-18, Doc-19, Doc-21	SW-1, SW-2	Serv-1	KeyAssets2, KeyAssets3, KeyAssets4, SecStor4, SecStor5, SecStor6, Crypt1, Crypt2, Crypt3, Crypt4, SecComm1, SecComm2, SecComm7	C1.1, C1.4, C1.5, C2.3, C2.4	N/A	N/A
	[AUM-1-2] Requirement user interface							
	AUM-1-1.ACM..ACM							
	AUM-1-1.ACM.NetworkInterface							
	AUM-1-1.ACM.ManagedAccessNetworkAsset							
	AUM-1-1.ACM.1.ManagedAccessSecurityAsset							
	AUM-1-1.ACM.IntendedFunctionality							
	AUM-1-1.ACM.AuthorizedEntity							
	AUM-1-1.ACM.AuthenticationMechanism							
	AUM-1-2.ACM.UserInterfaces							
	AUM-1-2.ACM.IntendedEnvironment							
	AUM-1-2.ACM.ReadOnlyFunctionality							
	AUM-1-2.ACM.ReadOnlyLegal							

Where can I find them ? →

Ask our online support
https://my.st.com/ols



Date of report

6/8/2025

Purpose of the document

To provide a reference of the security assets available on a product family that includes the hardware, the software, and various services available around the software. This document will help a developer to map the available ST resources used in his application towards the fomalized RED requirements.
The information can be used to help create its documentation but also to select HW, SW or services options within STM32 ecosystems in order to develop more secure final products.

The EN 18031 standards was harmonized and allows manufacturers to prepare their documents of conformance, in self-assessment, without the need for a notified body evaluation. It emphasizes the protection of "assets" as essential elements or functions that require safeguarding. These standards define a set of requirements that manufacturers must fulfill to ensure device security.

The key requirements are based on the RED essential requirements areas and include:

General equipment security: Implement technical and operational measures to enhance vulnerability management, focusing on security by design, and minimizing attack surfaces.
Access control mechanisms: Ensure that only authorized entities can access security and network assets through appropriate control measures.
Authentication mechanisms: Manage and regulate access rights for reading, modifying, or using network configurations and security parameters.
Cryptography and key management: Adhere to established international cybersecurity standards for cryptographic methods and key handling, referencing guidelines such as NIST SP 800-57, SOGIS Agreed Cryptographic Mechanisms, ETSI TS 119 312, and BSI TR-02102-1.
Secure storage solutions: Protect the confidentiality and integrity of stored assets with robust storage mechanisms.
Secure communication protocols: Safeguard communications involving assets to maintain authenticity, confidentiality, and protection against replay attacks.
Secure update processes: Provide secure mechanisms for software updates, ensuring the integrity and authenticity of new software installations.
Resilience features: Incorporate functionalities and best practices that improve resistance against denial-of-service (DoS) attacks targeting network interfaces.
Monitoring capabilities: Establish mechanisms to detect and monitor DoS attacks within network traffic.
Traffic control measures: Detect and respond to malicious behavior within network traffic to maintain system integrity.

This document only focus on EN-18031-1 (Article 3.3(d)) only, as GDPR and Financial aspects are not highly linked to MCU assets.

More information on RED can be found inside STM32 Wiki pages inside the Security/Regulations category

Deep dive on RED

Q&A for RED

Product concerned

STM32WBA5
STM32WBA5M
STM32WBA6
STM32WBA6M

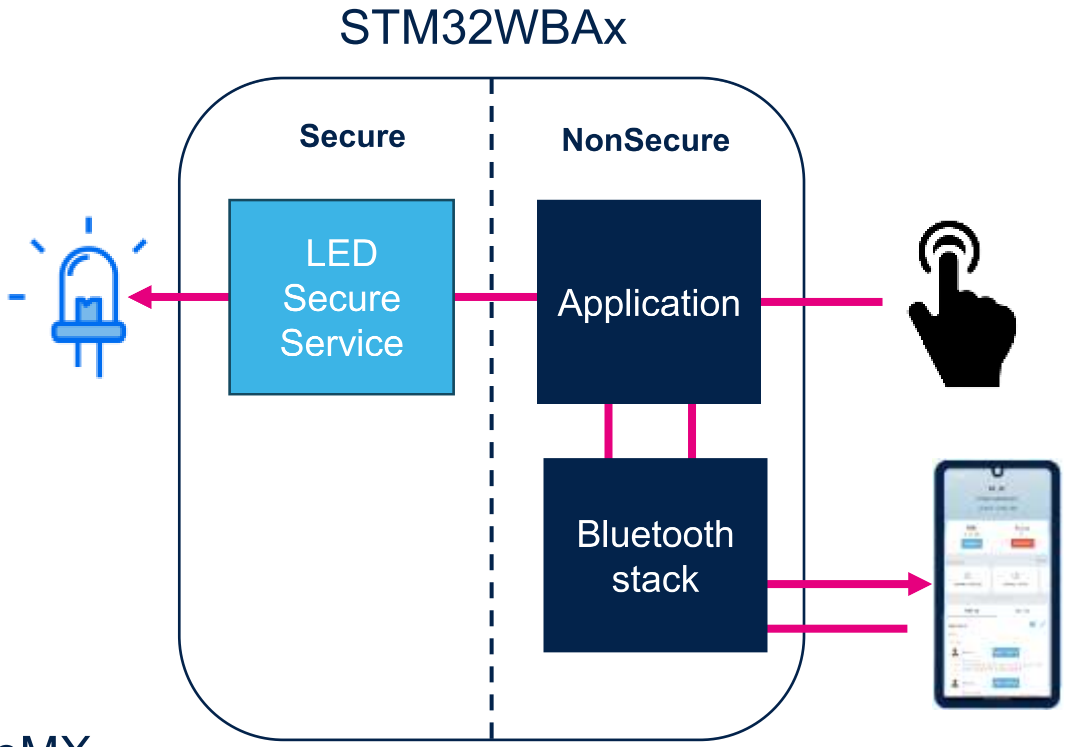
References	
STM32CubeWA	Cube package v1.7.0
BLE Stack	Included in STM32CubeWBA package
Solution to run the test	https://www.st.com/en/evaluation-tools/nucleo-wba55cg.html
Public accessibility	Yes

Security & Bluetooth® LE examples

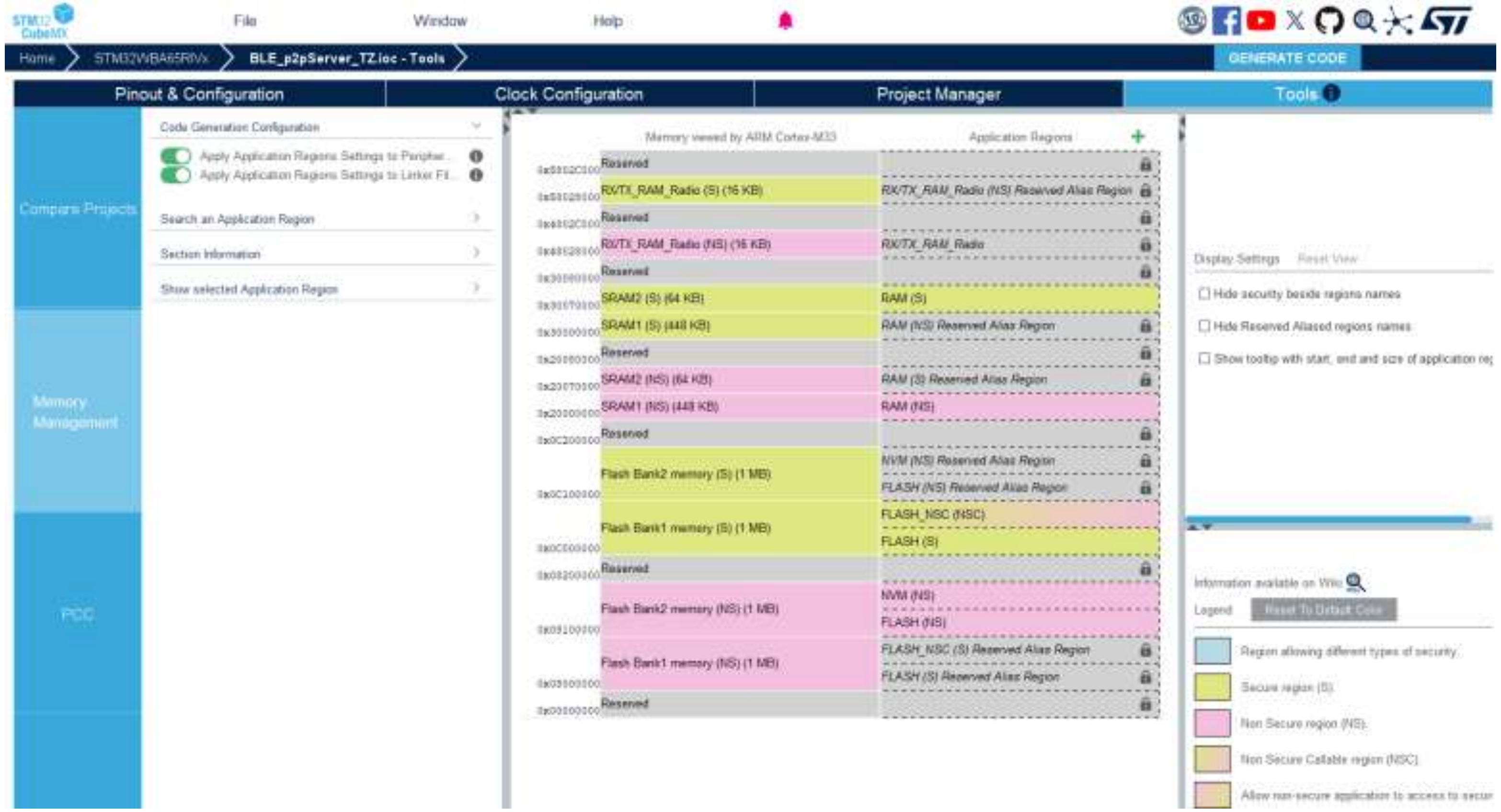
TrustZone® & Bluetooth® LE

- **BLE_p2pserver_TZ example:**
  - Wikipage: STM32WBA_BLE_&_TrustZone
  - Available on Nucleo-WBA{5/6}
  - Fully compatible with STM32CubeMX generation

- Illustrates:
  - How to use the Bluetooth® LE stack with the TrustZone® activated
  - How to create an isolated secure service
  - How to use the memory management tools of STM32CubeMX
  - How to use SAU/GTZC



TrustZone® project created with STM32CubeMX



Code Generation Configuration

- Apply Application Regions Settings to Peripher...
- Apply Application Regions Settings to Linker Fil...

Search an Application Region

Section Information

Show selected Application Region

	Memory viewed by ARM Cortex-M33	Application Regions
0x5002C000	Reserved	
0x50028000	RX/TX_RAM_Radio (S) (16 KB)	RX/TX_RAM_Radio (NS) Reserved Alias Region
0x4002C000	Reserved	
0x40028000	RX/TX_RAM_Radio (NS) (16 KB)	RX/TX_RAM_Radio
0x30080000	Reserved	
0x30070000	SRAM2 (S) (64 KB)	RAM (S)
0x30000000	SRAM1 (S) (448 KB)	RAM (NS) Reserved Alias Region
0x20080000	Reserved	
0x20070000	SRAM2 (NS) (64 KB)	RAM (S) Reserved Alias Region
0x20000000	SRAM1 (NS) (448 KB)	RAM (NS)
0x0C200000	Reserved	
	Flash Bank2 memory (S) (1 MB)	NVM (NS) Reserved Alias Region
0x0C100000		FLASH (NS) Reserved Alias Region
	Flash Bank1 memory (S) (1 MB)	FLASH_NSC (NSC)
0x0C000000		FLASH (S)
0x08200000	Reserved	
	Flash Bank2 memory (NS) (1 MB)	NVM (NS)
0x08100000		FLASH (NS)
	Flash Bank1 memory (NS) (1 MB)	FLASH_NSC (S) Reserved Alias Region
0x08000000		FLASH (S) Reserved Alias Region
0x00000000	Reserved	

Display Settings Reset View

- ☐ Hide security beside regions names
- ☐ Hide Reserved Aliased regions names
- ☐ Show tooltip with start, end and size of application re

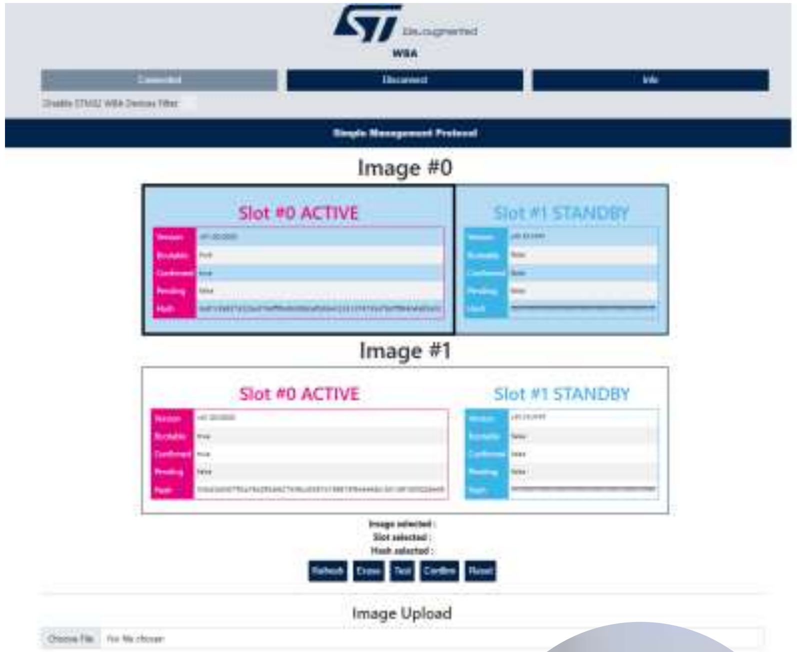
Information available on Wiki

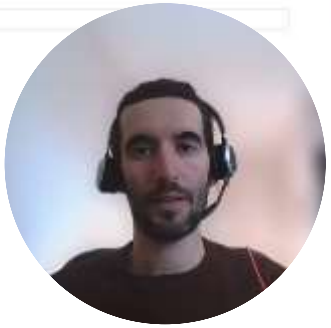
Legend Reset To Default Color

🟦	Region allowing different types of security.
🟨	Secure region (S).
🟪	Non Secure region (NS).
🟧	Non Secure Callable region (NSC).
🟧	Allow non-secure application to access to secur

Secure boot & FOTA over Bluetooth® LE

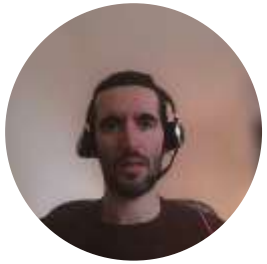
- **STM32WBA-BLE-OEMiROT-FOTA**
  - Github: STM32WBA-BLE-OEMiROT-FOTA
  - Wikipage: STM32CubeWBA Bluetooth® LE - OEMiROT & Secure Firmware Update
  - Multi-updater clients:
    - Web bluetooth App WBA
    - AuTerm
    - mynewt-mcumgr-cli
  - Available on STM32WBA65I-DK
- Illustrates:
  - How to use the Bluetooth® LE stack with the OEMiROT
  - How to perform Bluetooth® LE FOTA with the OEMiROT
  - How to use the smp/mcumgr layer to unify the Zephyr & Cube ecosystem for firmware update



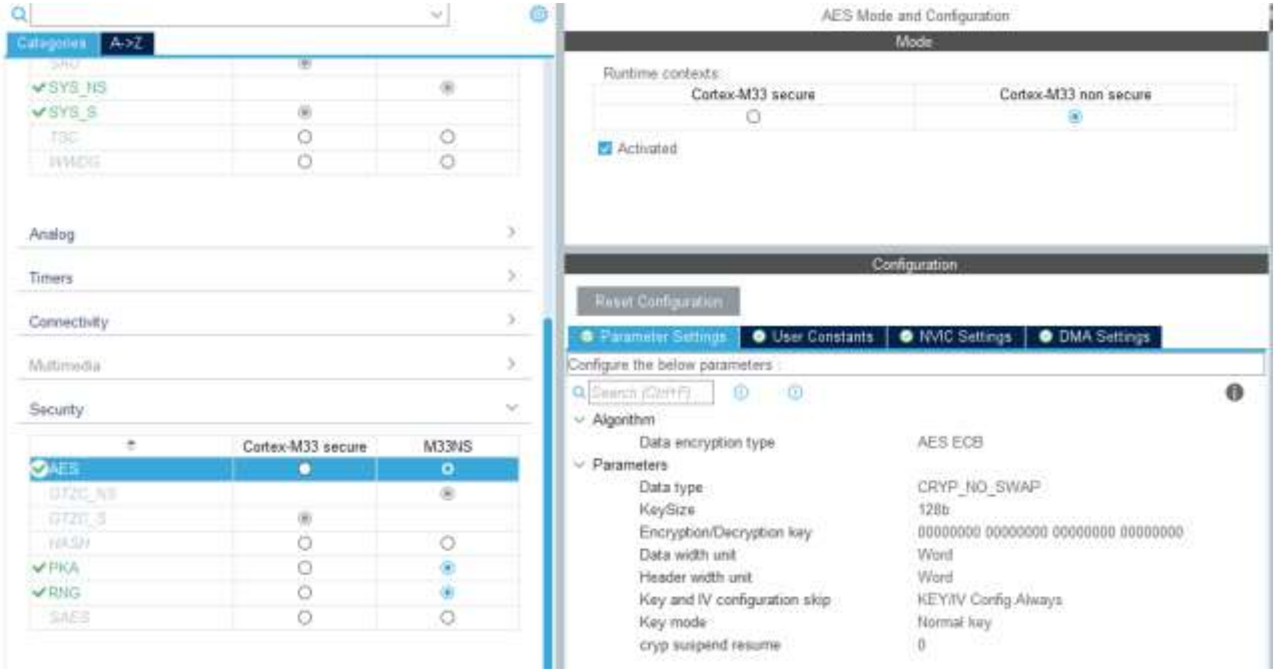


Miscellaneous STM32CubeWBA examples

Involved	Example	Comment
OEMxROT	Projects/Nucleo-WBAXX/Applications/ROT	Your root of trust
MPU	Projects/Nucleo-WBAXX/Examples/Cortex®	Using memory protection unit
CRC	Projects/Nucleo-WBAXX/Examples/CRC	Using error correction with CRC peripheral
AES	Projects/Nucleo-WBAXX/Examples/CRYP	Using the AES accelerators, with SCA protections
WP	Projects/Nucleo-WBAXX/Examples/FLASH	Protect your code with write protect (WP)
TrustZone®	Projects/NUCLEO-WBAXX/Templates/TrustZoneEnabled Projects/Nucleo-WBAXX/Examples/RTC Projects/Nucleo-WBAXX/Applications/BLE/BLE_p2pServer_TZ	Benefit of physical and logical isolation enabled by Arm® TrustZone®
SHA	Projects/Nucleo-WBAXX/Examples/HASH	Sign and verify integrity using SHA accelerators
PKA	Projects/Nucleo-WBAXX/Examples/PKA	Use public key accelerator for asymmetrical crypto
RNG	Projects/Nucleo-WBAXX/Examples/RNG	Get randoms with the certified random generator
Tamper	Projects/Nucleo-WBAXX/Examples/RTC	Detect intrusions thanks to tamper mechanisms
Bluetooth® LE	Projects/Nucleo-WBAXX/Applications/BLE/BLE_p2pServer_TZ Projects/Nucleo-WBAXX/Applications/BLE/BLE_TransparentMode & STM32CubeMonitor-RF	Bluetooth® LE application



STM32CubeMX configuration



	Cortex-M33 secure	M33NS
SRC	●	
✓ SYS_NS		●
✓ SYS_S	●	
TSC	○	○
IWWDG	○	○

	Cortex-M33 secure	M33NS
✓ AES	●	○
GTZC_NS		●
GTZC_S	●	
HASH	○	○
✓ PKA	○	●
✓ RNG	○	●
SAES	○	○

AES Mode and Configuration

Mode

Runtime contexts:

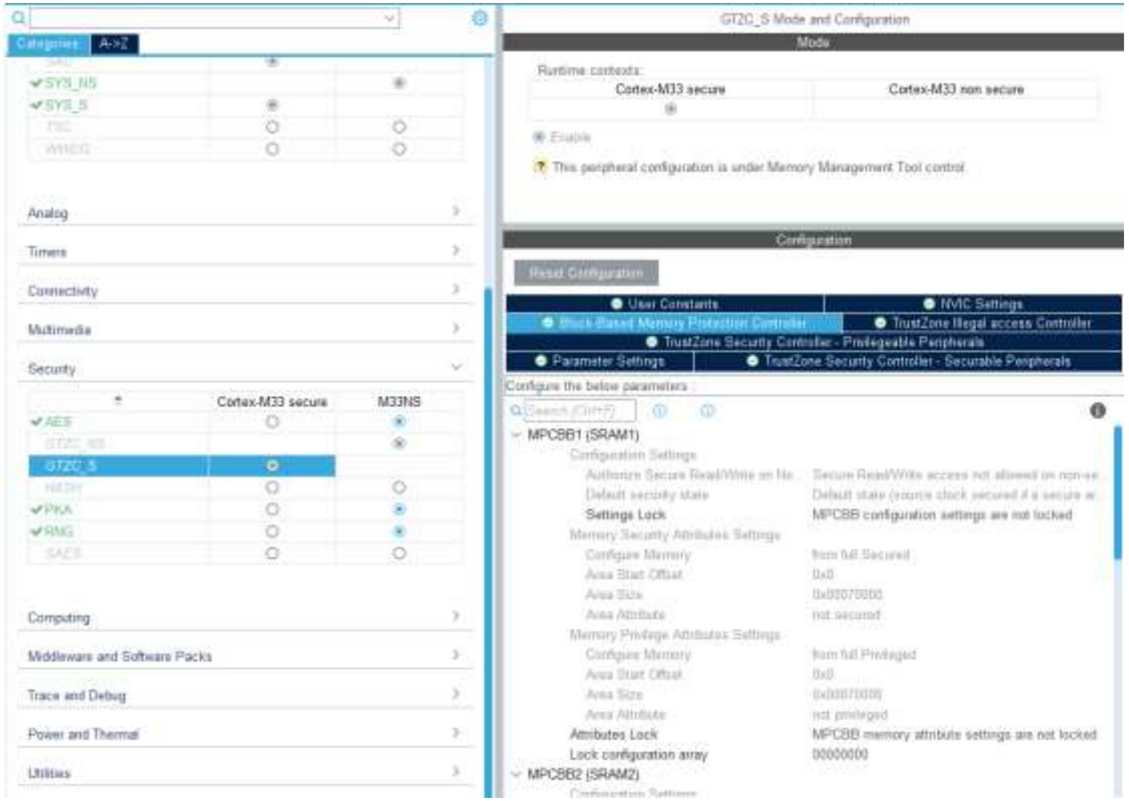
Cortex-M33 secure	Cortex-M33 non secure
○	●

☑ Activated

Configuration

Configure the below parameters :

- Algorithm
  - Data encryption type: AES ECB
- Parameters
  - Data type: CRYP_NO_SWAP
  - KeySize: 128b
  - Encryption/Decryption key: 00000000 00000000 00000000 00000000
  - Data width unit: Word
  - Header width unit: Word
  - Key and IV configuration skip: KEY/IV Config Always
  - Key mode: Normal key
  - cryp suspend resume: 0



Categories
A->Z
Analog
Timers
Connectivity
Multimedia
Security
Computing
Middleware and Software Packs
Trace and Debug
Power and Thermal
Utilities

	Cortex-M33 secure	M33NS
SRC	●	
✓ SYS_NS		●
✓ SYS_S	●	
TSC	○	○
IWWDG	○	○

	Cortex-M33 secure	M33NS
✓ AES	○	●
GTZC_NS		●
GTZC_S	●	
HASH	○	○
✓ PKA	○	●
✓ RNG	○	●
SAES	○	○

GTZC_S Mode and Configuration

Mode

Runtime contexts:

Cortex-M33 secure	Cortex-M33 non secure
●	

● Enable

This peripheral configuration is under Memory Management Tool control

Configuration

Reset Configuration
User Constants
NVIC Settings
Block-Based Memory Protection Controller
TrustZone Illegal access Controller
TrustZone Security Controller - Privilegeable Peripherals
Parameter Settings
TrustZone Security Controller - Securable Peripherals
Search (Ctrl+F)

Configure the below parameters :

- MPCBB1 (SRAM1)
  - Configuration Settings
    - Authorize Secure Read/Write on No...: Secure Read/Write access not allowed on non-se...
    - Default security state: Default state (source clock secured if a secure ar...
    - Settings Lock: MPCBB configuration settings are not locked
  - Memory Security Attributes Settings
    - Configure Memory: from full Secured
    - Area Start Offset: 0x0
    - Area Size: 0x00070000
    - Area Attribute: not secured
  - Memory Privilege Attributes Settings
    - Configure Memory: from full Privileged
    - Area Start Offset: 0x0
    - Area Size: 0x00070000
    - Area Attribute: not privileged
  - Attributes Lock: MPCBB memory attribute settings are not locked
  - Lock configuration array: 00000000
- MPCBB2 (SRAM2)
  - Configuration Settings

Takeaways

Takeaways

RED / CRA	Where we stand
ST is there to support you	Wiki checklist
When it comes to your application	A set of running examples to guide you

Our technology starts with You

Find out more at www.st.com