life.augmented

STM32Trust
The STM32 security framework for protecting embedded systems

STMicroelectronics

박시완 부장

Outline

Access useful links

See abbreviation glossary and definitions

life.augmented

Click to go to the relevant sections

What is security?

What is security?

Security is about ensuring:

Confidentiality

Protecting sensitive data and ensuring secrecy.

Integrity

Safeguarding data accuracy and protecting it from any modification.

Availability

Ensuring that functionality and/or data is available when it is needed.

life.augmented

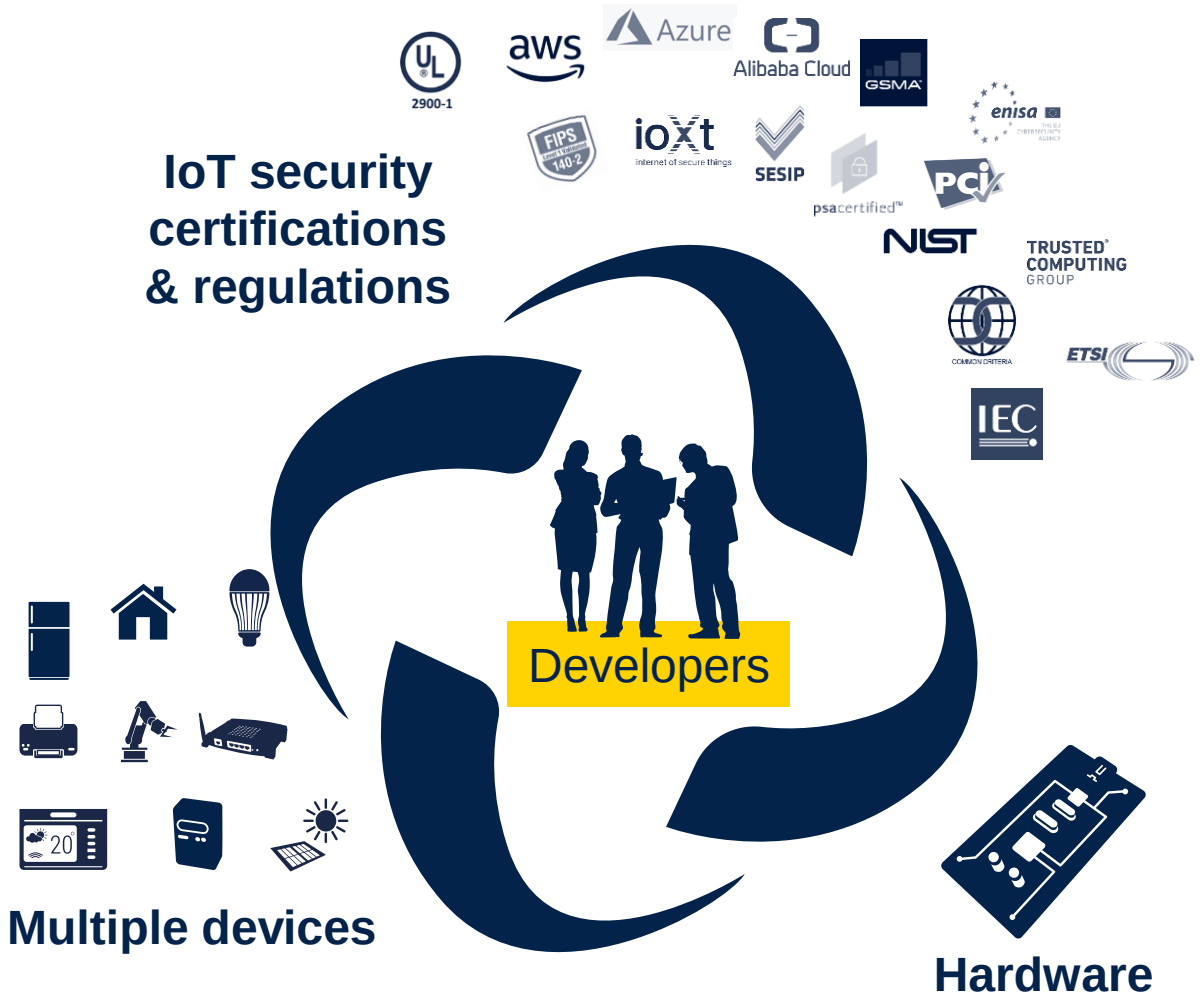
Addressing the security challenges and gaps

Security challenges for our customers

- Complex
- High cost
- Time to market

Missing link

Scalability, certification, maintenance.
Core security hardware and services



life.augmented

Our goal: protect customer assets

Data

- Confidentiality
- Secrets
- Regulations
- Authenticity

IP

- Software
- Data
- Processes
- Secrets

Connectivity

- Regulations
- Network access
- Data transfer
- Confidentiality
- Availability

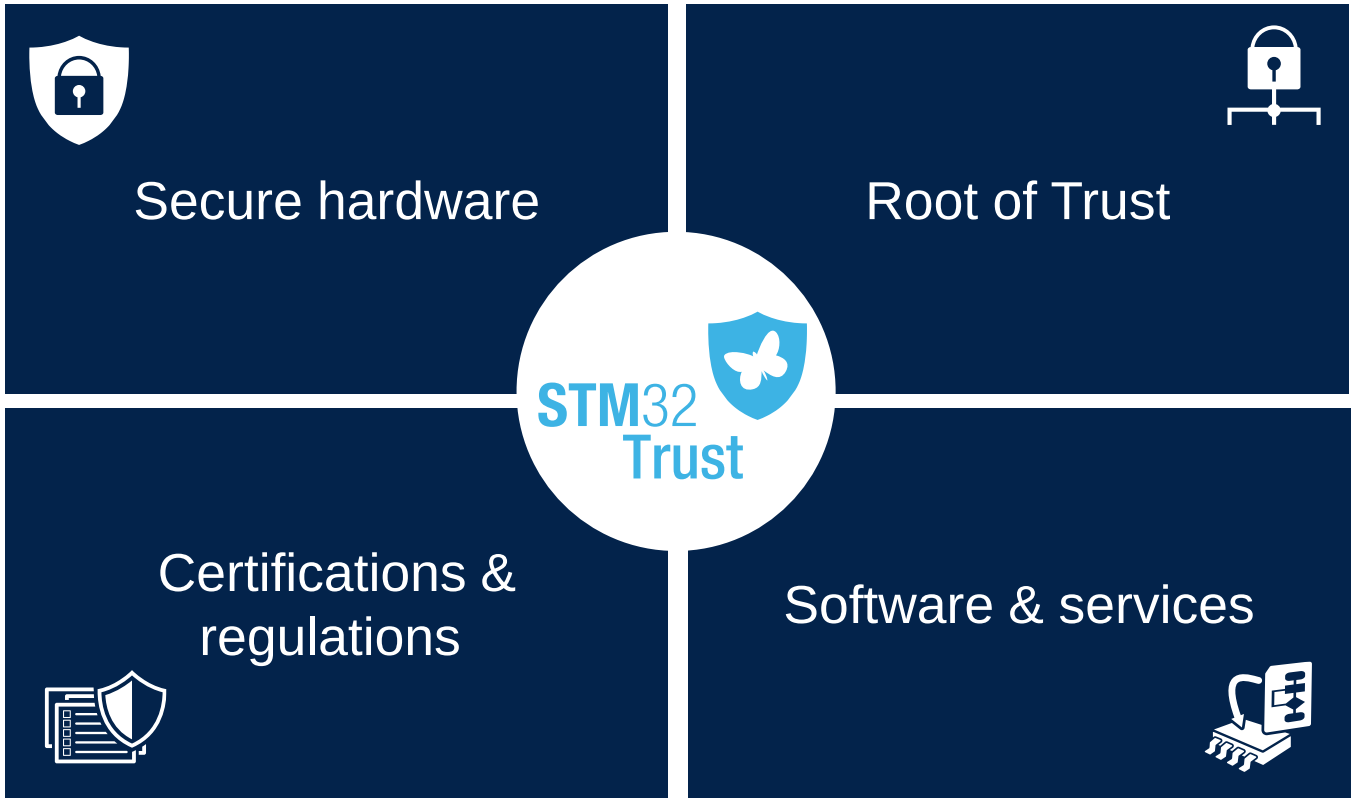
System trust

- Regulations
- Reliability
- Availability
- Authentication
- Confidentiality

The STM32Trust framework

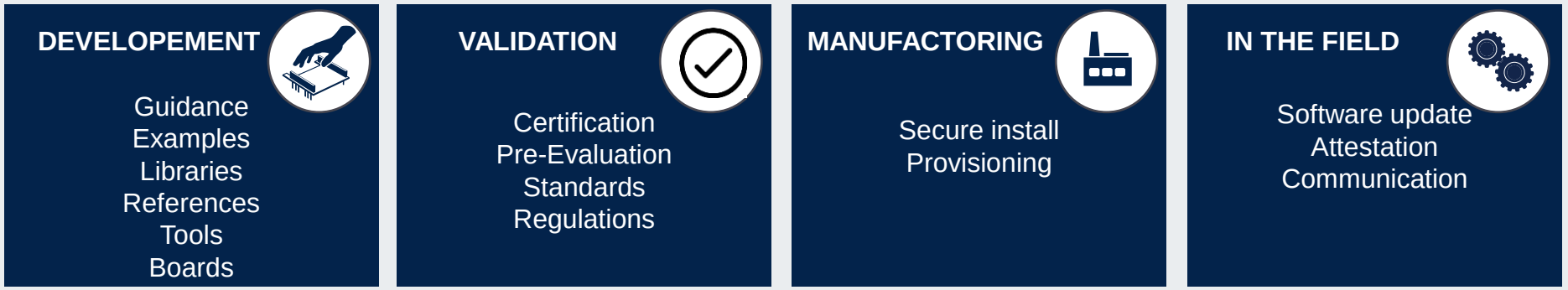
What is STM32Trust?

STM32Trust is built on key pillars to ensure security



Software and services

Use our services to protect your workflow, from the development phase to deployment in the field



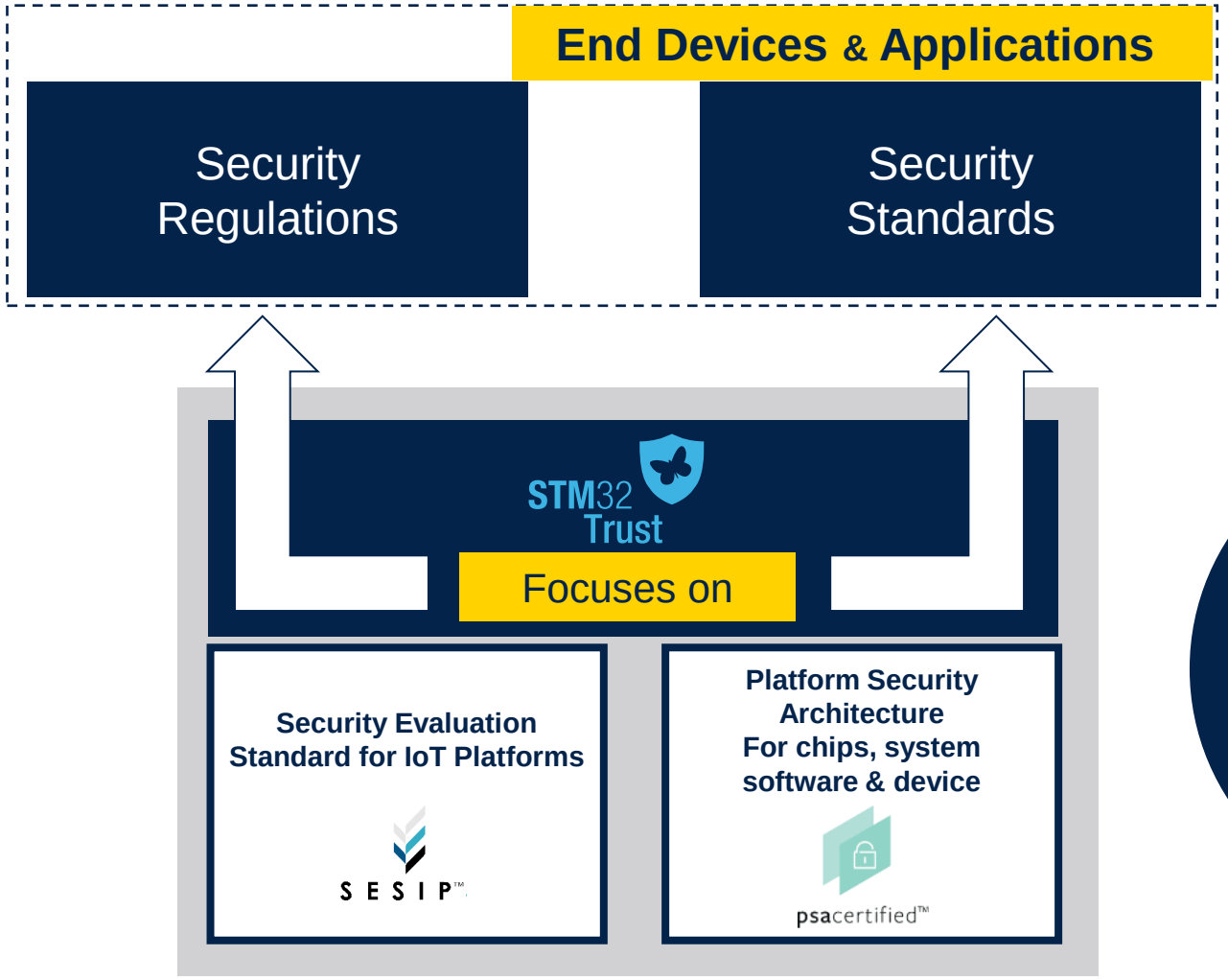
Supports

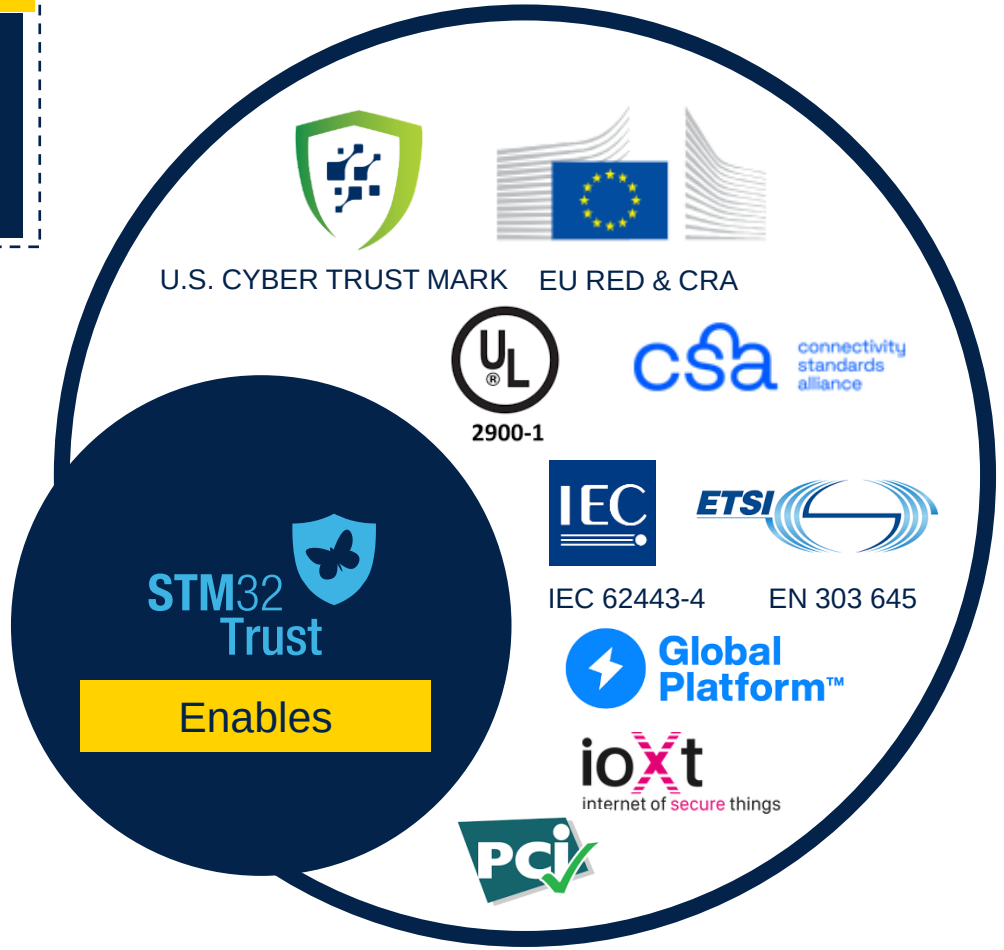
STM32Cube	TF-M, TF-A	Secure firmware install
PSA Certification	OP-TEE	Secure module install
SESIP Certification	Crypto libraries	Secure secret provisioning
NIST SP800-90B	Secure Manager	Secure element support

Simplifies

STM32 CubeExpansion

Certifications & Regulations





Focus on RED and CRA standards

Radio Equipment Directive (RED)

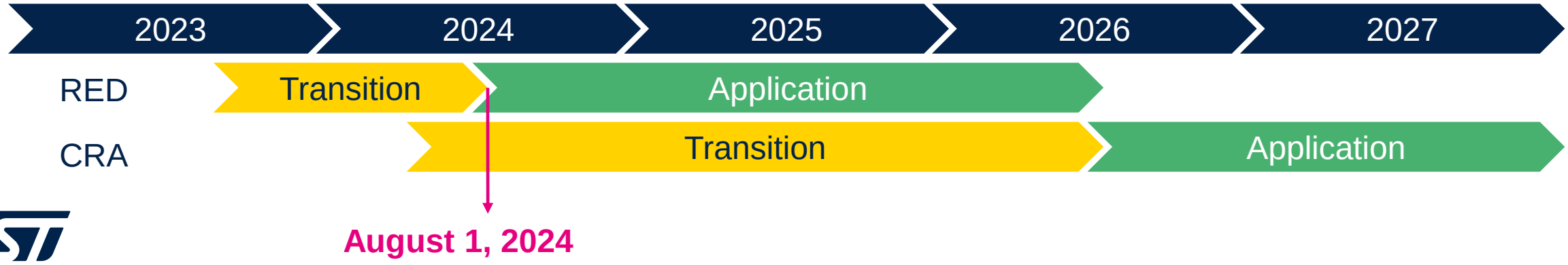
Goal: increase security for radio connected devices.

- Be capable of updating/patching products.
- Conformity assessment with risk-based approach according to the usage and environment of the device.
  - Hardware component: N/A
  - IoT consumer device: self-declaration
  - IoT industrial device: self-declaration

Cyber Resilience Act (CRA)

Goal: ensure more secure hardware and software products in the field

- Actively monitor vulnerabilities and provide updates/patches.
- Different security levels according to predefined categories.
  - Hardware component: third-party evaluation
  - IoT consumer device-: self-declaration
  - IoT industrial device: third-party evaluation



life.augmented

STM32Trust Security Functions

life.augmented

From assets to Security Functions

STM32Trust streamlines the IoT security Model with:

- A meta security framework with generic Security Functions
- The coverage of commonplace threats & vulnerabilities classes

Threats
Unauthorized access
Malware & ransomware
Denial of service (DoS)
Man-in-the-middle (MitM)
Physical tampering
Data privacy & integrity

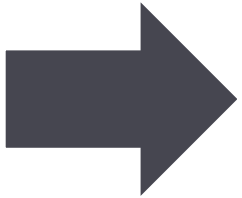
CWE vulnerabilities
Authentication & authorization
Encryption & cryptography
Network
Physical security
Software
Configuration & management

STM32Trust Security Functions
Identification / Authentication / Attestation
Application life cycle
Secure manufacturing
Software IP protection
Silicon device life cycle
Secure install / update
Secure storage
Isolation
Abnormal situation handling
Secure boot
Crypto engine
Audit / Log

Security Functions for RoT certification

STM32Trust Security Functions

- Identification / Authentication / Attestation
- Application life cycle
- Secure manufacturing
- Software IP protection
- Silicon device life cycle
- Secure install / update
- Secure storage
- Isolation
- Abnormal situation handling
- Secure boot
- Crypto engine
- Audit / Log



Mapping Security Functions (SF) to PSA Certified and SESIP for RoT security certification

PSA certified SFs

- Initialization
- Software isolation
- Secure storage
- Firmware update
- Secure state
- Cryptography
- Attestation
- Audit
- Debug
- Physical protection

SESIP SFs

- Identification and attestation
- Product life cycle
- Secure communication
- Extra attacker resistance
- Cryptographic functionality
- Compliance functionality
- …
- …
- …
- …

STM32Trust Security Functions explained

Security Functions	Definition
Identification / Authentication / Attestation	Unique identification of a device and/or software, and ability to detect its authenticity.
Application life cycle	Defines unchangeable incremental states to securely protect application states and assets.
Secure manufacturing	Device provisioning or personalization in untrusted environment with overproduction control.
Software IP protection	Ability to protect a section or the whole software package against external or internal reading, ”multitenant”.
Silicon device life cycle	Control states to securely protect silicon device assets during its lifetime.
Secure install / update	Installation or update of firmware with initial integrity & authenticity checks before programming & execution.
Secure storage	Ability to securely store secrets like data or keys.
Isolation	Isolation between trusted and non-trusted parts of an application.
Abnormal situation handling	Ability to detect and to react to abnormal hardware and software situations.
Secure boot	Ability to ensure the authenticity and integrity of an embedded application.
Crypto engine	Ability to process cryptographic algorithms, as recommended by security assurance schemes.
Audit / Log	Ability to keep trace of security events in an unchangeable way.

STM32 product target certifications

MPU		PSA Certified Level 1 STM32**MP15**	PSA Certified Level 1 SESIP3 STM32**MP13**
High perf MCUs		PSA Certified Level 1 STM32**H7**	PSA Certified Level 1 SESIP3 STM32**H5**
Mainstream MCUs	PSA Certified Level 1 STM32**G0**	PSA Certified Level 1 STM32**G4**	PSA Certified Level 1 STM32**C0**
Ultra-low-power MCUs	PSA Certified Level 1 STM32**L4/L4+**	PSA Certified Level 1 SESIP3 STM32L5	PSA Certified Level 3 SESIP3 STM32**U5**
Wireless MCUs			PSA Certified Level 3 SESIP3 STM32**MP13**

life.augmented

STM32Trust TEE Secure Manager

life.augmented

Secure Manager
First used in the STM32H5 platform

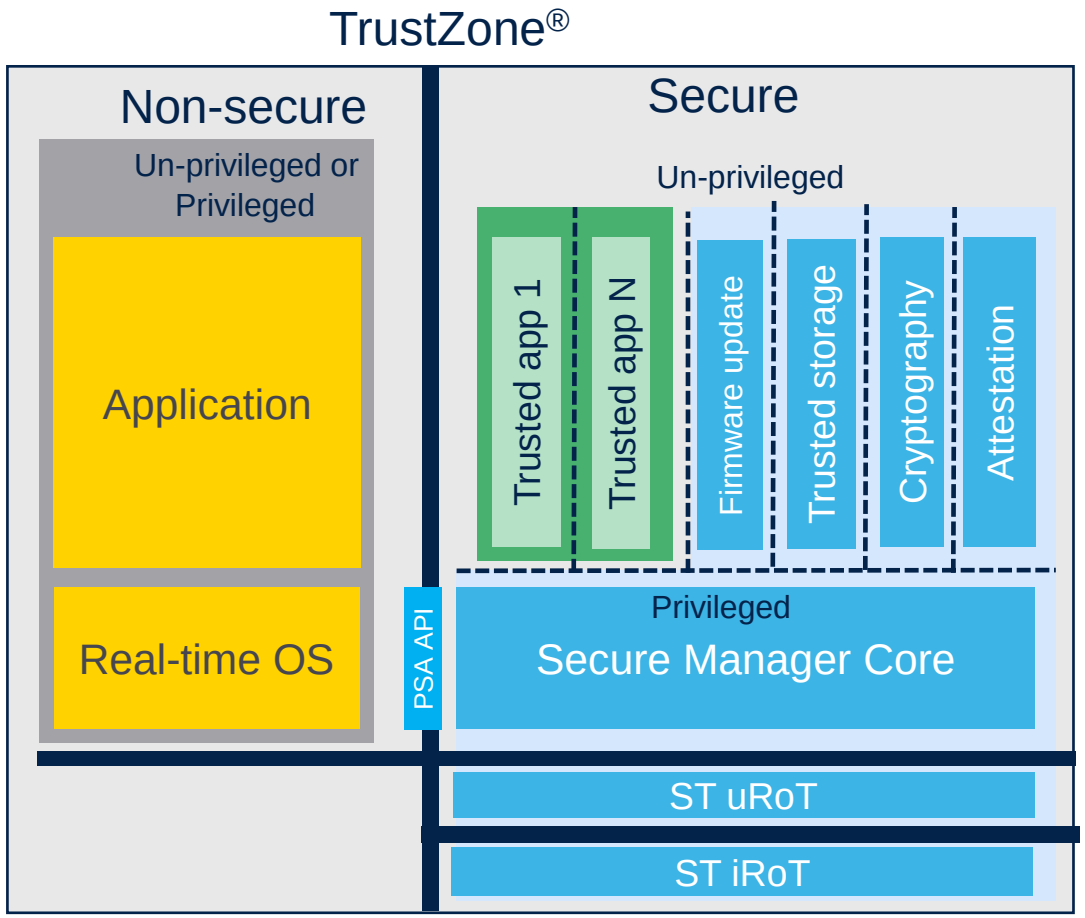
The STM32Trust TEE Secure Manager protects IP and simplifies your security journey

psacertified™ level three

SESIP™3

Target

Scope of Secure Manager



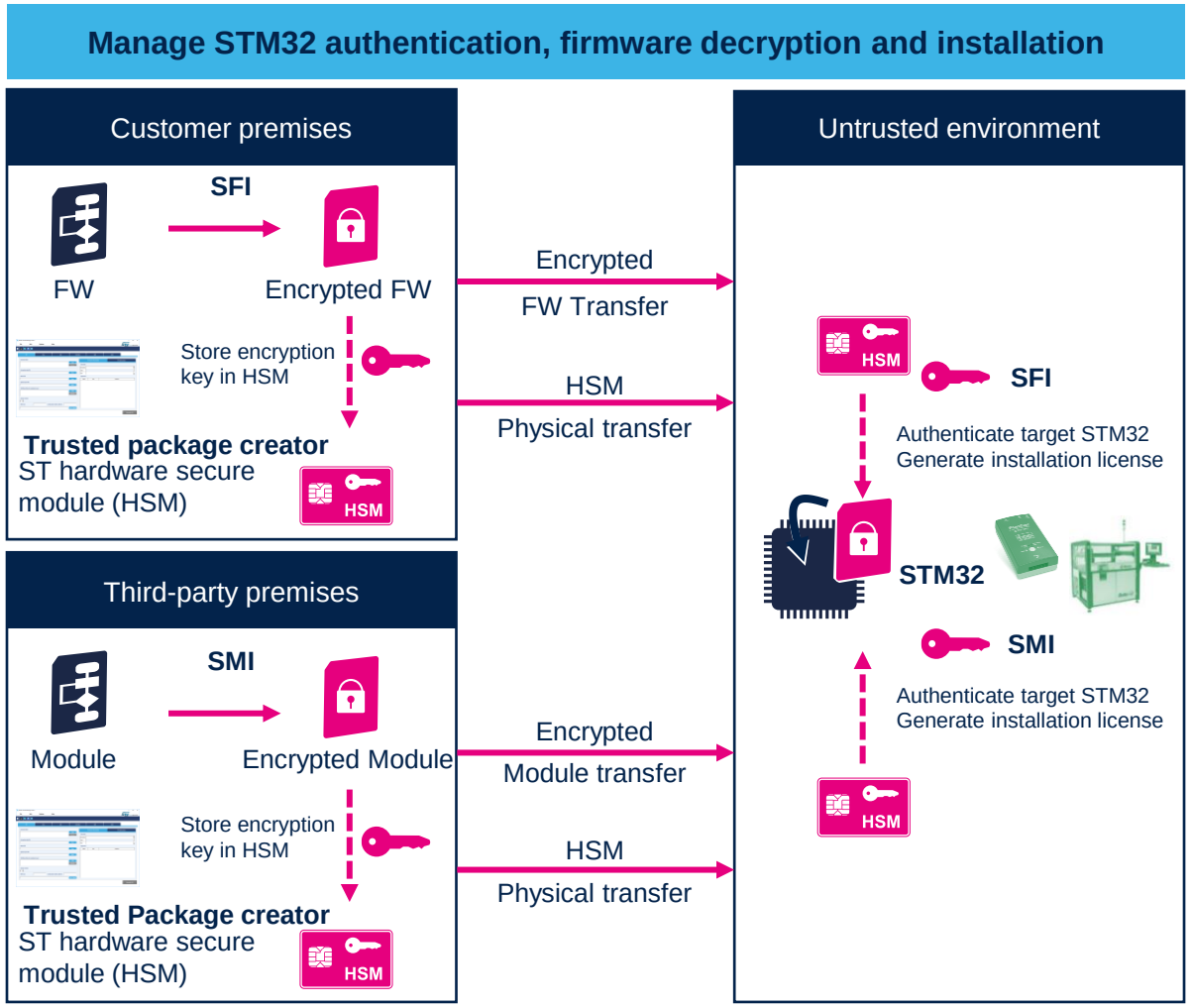
- ST platform ownership
- Turnkey set of security services
- Secure Manager Core to handle isolation
- Multitenant software IP protection
- Arm® PSA API compatible
- Designed for long-term-support (LTS)
- Modular secure update capable
- Optimized certification properties
- Certified and maintained by ST
- Covering the 12 security functions

life.augmented

Secure firmware and secret installation

life.augmented

Embedded secure firmware install - SFI



Secure Loader
embedded services provisioned by ST
➔ mass market approach

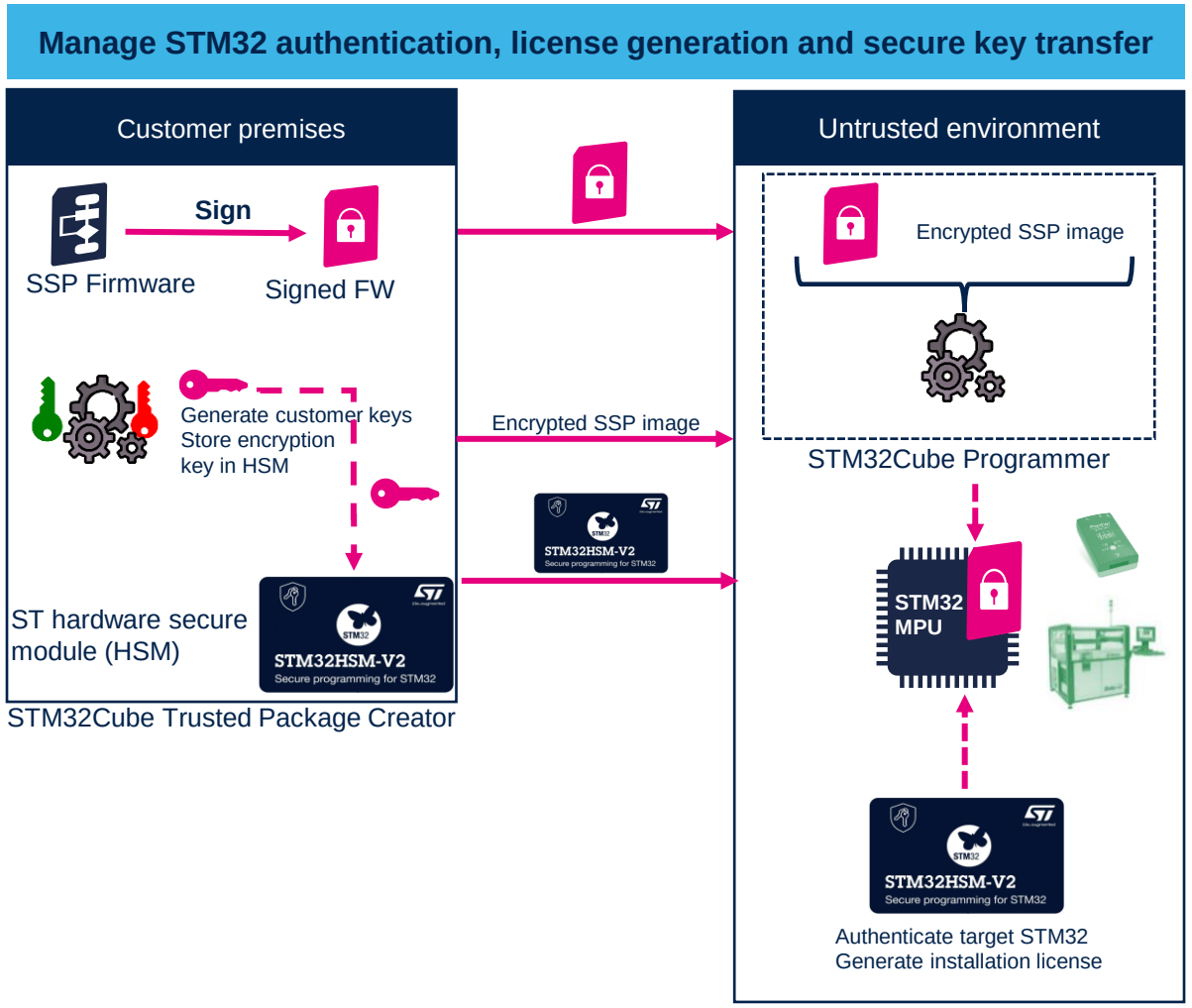
ST ecosystem
with
Encryption, HSM, and programming tools

Firmware cloning
protection on the first installation
via
UART / SPI / USB

Protect third-party software IP
(SMI)

life.augmented

Embedded secure secret provisioning - SSP



The SSP process prevents the OEM secrets from:

- Being accessed by the contract manufacturer
- Being extracted or disclosed
- Being over produced

ST ecosystem with Encryption, HSM, and programming tools

Protect secret customer keys

life.augmented

Security in practice

Customer example
focus on secure manufacturing

Asset

Product

Bob is at the head of a company designing toys.
He would like to avoid the counterfeiting of his company-branded toys.

What Bob needs to achieve

- Firmware protection during production
- Production management at manufacturer (no over- or under-production)
- Protection against the programing of other devices during production
- Firmware protection in the field

Required Security Functions

- Secure manufacturing
- Software IP protection
- Secure install / update
- Silicon device life cycle

Customer example
focus on isolation and IP protection

Asset

IP

Jon owns a company that sells firmware.
The firmware package features additional options that can be enabled by the user.

What Jon needs to achieve

- Firmware protection
- Ensure that the firmware package is isolated from customer firmware
- Ensure independent firmware updates
- Set application in a macrostate while ensuring it cannot be altered

Required Security Functions

- Software IP protection
- Code isolation
- Secure Install/Update
- Application life cycle

Security Functions and services in STM32 products

life.augmented

The STM32 portfolio

Five product categories

Wireless MCU

Short- and long-range connectivity

Ultra-low-power MCU

Mainstream MCU

High-performance MCU

32-bit general-purpose microcontrollers: from 75 to 3,224 CoreMark score

Embedded MPU

32- and 64-bit microprocessors





Enabling edge AI solutions

Scalable security

MPU portfolio

MCU portfolio

High performance products with security functions

STM32 Trust

STM32Fx

- STM32F3
- STM32F4
- STM32F7

Certification targets

STM32Trust Security Functions	Features		
	Hardware	**Software**	**Services**
Identification / Authentication / Attestation	Unique ID	-	STSAFE support
Application life cycle	OTP	-	-
Secure manufacturing	-	-	
Software IP protection	RDP, MPU, PCROP	-	
Silicon device life cycle	WPR, RDP, PCROP	-	CubeProgrammer
Secure install / update	HDP, WPR, RDP, UBE	X-CUBE-SBSFU	CubeProgrammer (digest, signature)
Secure storage	HDP, OTFDEC	-	-
Isolation	MPU, PCROP	-	-
Abnormal situation handling	Tamper, RTC, GPIO locking, ECC, CSS, Temp Sensor, watchdogs, PVD	-	-
Secure boot	RDP,WRP,MPU,	X-CUBE-SBSFU	CubeProgrammer (digest, signature)
Crypto engine	AES,HASH,TRNG	X-CUBE-CRYPTOLIB, PCL(1)	-
Audit / Log	-	-	-

Notes: (1) side channel protections

life.augmented

Mainstream products with security functions

STM32 Trust

STM32Gx

- STM32G0
- STM32G4

Certification targets

psacertified™ level one

STM32Trust Security Functions	Features		
	Hardware	**Software**	**Services**
Identification / Authentication / Attestation	Unique ID	-	STSAFE support
Application life cycle	OTP	-	-
Secure manufacturing	-	-	-
Software IP protection	RDP, MPU, PCROP	-	-
Silicon device life cycle	HDP, WPR, RDP, PCROP	-	CubeProgrammer
Secure install / update	HDP, WPR, RDP, UBE	X-CUBE-SBSFU	CubeProgrammer
Secure storage	HDP	-	-
Isolation	HDP, MPU	-	-
Abnormal situation handling	Tamper, RTC, GPIO lock, CSS, ECC, Temp. sensor, PVD, WD, BR	-	-
Secure boot	HDP, WPR, RDP, UBE, MPU	X-CUBE-SBSFU	CubeProgrammer
Crypto engine	HASH, AES, TRNG	X-CUBE-CRYPTOLIB,	-
Audit / Log	-	-	-

Notes: (1) side channel protections

life.augmented

Ultra-low-power products with security functions

STM32 Trust

STM32Lx

- STM32L0
- STM32L4
- STM32L5

Certification targets

STM32Trust Security Functions	Features		
	Hardware	**Software**	**Services**
Identification / Authentication / Attestation	Unique DI		-
Application life cycle	OTP	-	
Secure manufacturing	-	-	-
Software IP protection	RDP, Firewall, PcRoP, MPU		-
Silicon device life cycle	PCROP	-	CubeProgrammer
Secure install / update	RDP, MPU,	X-CUBE-SBSFU	CubeProgrammer
Secure storage	Firewall,		-
Isolation	Firewall, MPU, PCROP		-
Abnormal situation handling	Tamper, RTC, GPIO lock, CSS, ECC, Temp. sensor, PVD, WDT, Backup registers		-
Secure boot	RDP, WRP	X-CUBE-SBSFU	CubeProgrammer
Crypto engine	AES, HASH, TRNG	X-CUBE-CRYPTOLIB	-
Audit / Log	-		-

Notes: (1) side channel protections

life.augmented

Ultra-low-power products with security functions

STM32 Trust

STM32Lx

STM32L0

STM32L4

STM32L5

STM32Trust Security Functions	Features		
	Hardware	Software	Services
Identification / Authentication / Attestation	Unique DI		-
Application life cycle	OTP	-	
Secure manufacturing	RSS	SFI	-
Software IP protection	RDP, Firewall , PCROP, MPU		-
Silicon device life cycle	PCROP, RDP, WRP	-	CubeProgrammer
Secure install / update	RDP, MPU	X-CUBE-SBSFU	CubeProgrammer
Secure storage	Firewall	X-CUBE-SBSFU	-
Isolation	Firewall, MPU, PCROP	-	-
Abnormal situation handling	Tamper, RTC, GPIO lock, CSS, ECC, Temp. sensor, PVD, WD, BR		-
Secure boot	RDP,WRP,MPU	X-CUBE-SBSFU	CubeProgrammer
Crypto engine	AES, HASH, TRNG	X-CUBE-CRYPTOLIB, DPA resistance* (FIPS-140)	-
Audit / Log	-		-

Certification targets

psacertified™ level one

SESIP™1

** Contact your nearest sales office*

life.augmented

Ultra-low-power products with security functions

STM32 Trust

STM32L0

STM32L4

STM32L5

Certification targets

psacertified™ level one

SESIP3

STM32Lx	STM32Trust Security Functions	Features		
		Hardware	Software	Services
	Identification / Authentication / Attestation	Unique ID, Certificate	TF-M	-
	Application life cycle	OTP	-	
	Secure manufacturing	RSS	Secure firmware install	-
	Software IP protection	RDP, Firewall , PCROP, MPU	TF-M	-
	Silicon device life cycle	RDP, WRP, HDP	-	CubeProgrammer
	Secure install / update	RDP, MPU, UBE, TrustZone®	TF-M_SBSFU boot	CubeProgrammer
	Secure storage	AES Key storage, OTFDEC, HDP	TF-M	-
	Isolation	Firewall, MPU, PCROP	TF-M	-
	Abnormal situation handling	Tamper, RTC, GPIO lock, CSS, ECC, Temp. sensor, PVD, WD, BR		-
	Secure boot	RDP, WRP, MPU, UBE, HDP	TF-M_SBSFU boot	CubeProgrammer
	Crypto engine	AES, HASH, PKA, OTFDEC, TRNG	X-CUBE-CRYPTOLIB, TF-M	-
	Audit / Log	GTZC (global TrustZone® controller)	TF-M	-

life.augmented

AES Key storage	Write-only key registers in AES engine.

Ultra-low-power products with security functions

STM32 Trust

STM32Ux

STM32U5

STM32Trust Security Functions	Features		
	Hardware	Software	Services
Identification / Authentication / Attestation	Unique ID, device certificate	TF-M	STSAFE support
Application life cycle	OTP	TFM	-
Secure manufacturing	RSS	STM32HSM-V1 (link)	XCUBE-SFI
Software IP protection	RDP, MPU	TFM	XCUBE-SFI
Silicon device life cycle	RDP, WRP, HDP	-	CubeProgrammer
Secure install / update	TrustZone®, HDP, MPU, UBE, RDP	X-CUBE-SBSFU, TFM_SBSFU Boot	CubeProgrammer
Secure storage	TrustZone®,AESKey,OTFDEC,HDP	TF-M	-
Isolation	MPU, HDP, TrustZone®	TF-M	-
Abnormal situation handling	Tamper, RTC, GPIO lock, CSS, ECC, Temp. sensor, PVD, WD, BR	-	-
Secure boot	TructZone, RDP,WRP,MPU,UBE,HDP	X-CUBE-SBSFU, TFM_SBSFU Boot	CubeProgrammer
Crypto engine	TRNG, HASH, OTFDEC, AES, PKA(1)	X-CUBE-CRYPTOLIB, TF-M	-
Audit / Log	GTZC	TF-M	-

Certification targets

psacertified™ level three

SESIP™3

Certificate includes physical protections

Notes: (1) side channel protections

life.augmented

High performance products with security functions

STM32Hx

STM32H5

STM32H7

Certification targets

psacertified™ level three

SESIP™3

Certificate includes physical protections

STM32Trust Security Functions	Features		
	Hardware	**Software**	**Services**
Identification / Authentication / Attestation	DHUK, X509 certificates Device certificate	EAT (Secure Manager / TF-M)	STSAFE support
Application life cycle	OTP	Secure Manager, TF-M	
Secure manufacturing	iRoT (RSS)	SFI, SSFI (SM)	XCUBE-SFI
Software IP protection	Product states, HDPL, MPU, WRP, TZ	Secure Manager, TF-M	XCUBE-SFI
Silicon device life cycle	Product states, HDPL, WRP	-	CubeProgrammer
Secure install / update	TrustZone®, UBE, Bootlock, STiRoT, HPDL, WPR, Product State	uRoT/MCUBoot	CubeProgrammer
Secure storage	HDPL, OTFDEC, HUK, SAES, TrustZone®	ITS (SM/TF-M)	-
Isolation	HDPL, TZ, MPU, Product State	Secure Manager, TF-M	-
Abnormal situation handling	Tamper, RTC, GPIO lock, CSS, ECC, Temp. sensor, PVD, WD, BR	Tamper (SM)	-
Secure boot	TructZone, UBE, Bootlock, STiRoT, HPDL, WPR, Prod.State	iRoT/uRoT/MCUBoot	CubeProgrammer
Crypto engine	TNG, Hash (SHA1/2), OTFDEC, SAES(1), AES, PKA(1)	Mbed™, NetxDuo, X-CUBE-CRYPTOLIB, Secure Manager, TF-M	-
Audit / Log	-	Secure Manager, TF-M	-

Notes: (1) side channel protections

life.augmented

Wireless products with security functions

STM32 Trust

STM32Wx

- STM32WB
- STM32WBA
- STM32WL5

Certification targets

STM32Trust Security Functions	Features		
	Hardware	**Software**	**Services**
Identification / Authentication / Attestation	Unique DI, Certificate	-	-
Application life cycle	OTP	-	-
Secure manufacturing	-	-	-
Software IP protection	RDP, MPU	-	-
Silicon device life cycle	RDP, WRP	-	CubeProgrammer
Secure install / update	RDP, MPU, FUS on CM0	X-CUBE-SBSFU on Cortex® M4	CubeProgrammer
Secure storage	CKS	-	-
Isolation	MPU	-	-
Abnormal situation handling	Tamper, RTC, GPIO lock, CSS, ECC, Temp. sensor, PVD, WD, BR	-	-
Secure boot	RDP,WRP,MPU, FUS on CM0	X-CUBE-SBSFU on Cortex® M4	CubeProgrammer
Crypto engine	AES, HASH, PKA, TRNG	X-CUBE-CRYPTOLIB,	-
Audit / Log	-	-	-

life.augmented

Wireless products with security functions

STM32 Trust

STM32WB

STM32WBA

STM32WL5

STM32Wx	STM32Trust Security Functions	Features		
		Hardware	Software	Services
	Identification / Authentication / Attestation	Unique ID, Certificate	TF-M	-
	Application life cycle	OTP	-	
	Secure manufacturing	RSS	Secure Firmware install	-
	Software IP protection	RDP, Firewall, PCROP, MPU	TF-M	-
	Silicon device life cycle	RDP, WRP, HDP	-	CubeProgrammer
	Secure install / update	RDP, MPU, TrustZone®	TF-M_SBSFU Boot	CubeProgrammer
	Secure storage	AES Key storage, HDP	TF-M	-
	Isolation	Firewall, MPU, PCROP	TF-M	-
	Abnormal situation handling	Tamper, RTC, GPIO lock, CSS, ECC, Temp. sensor, PVD, WD, BR		-
	Secure boot	TrustZone®, Bootlock, RDP, WRP, MPU, HDP	TF-M_SBSFU Boot	CubeProgrammer
	Crypto engine	AES, HASH, PKA, TRNG	X-CUBE-CRYPTOLIB,	-
	Audit / Log	GTZC (global TrustZone® controller)	TF-M	-

Certification targets

psacertified™ level three

SESIP™3

Certificate includes physical protections

life.augmented

MPU products with security functions

STM32 Trust

STM32MPx

★ STM32MP157

★ STM32MP135

STM32Trust Security Functions	Features		
	Hardware	Software	Services
Identification / Authentication / Attestation	Unique ID	TF-M, TF-A, OP-TEE	STSAFE support
Application life cycle	OTP, RDP	-	
Secure manufacturing	SSP, HSM	SSP, secure boot ROM	SSP, STM32Trusted package creator
Software IP protection	RDP, MPU	-	-
Silicon device life cycle	RDP, WRP	-	CubeProgrammer
Secure install / update	FSBL, MPU	X-CUBE-SBSFU	CubeProgrammer
Secure storage	AES, DES, TRNG	-	-
Isolation	MPU, TrustZone®	OP-TEE	-
Abnormal situation handling	RDP, Tamper, RTC, GPIO, CSS, ECC, Temp. sensor, PVD	-	-
Secure boot	RDP, MPU	X-CUBE-SBSFU	CubeProgrammer
Crypto engine	AES, HASH, PKA, TRNG	X-CUBE-CRYPTOLIB,	-
Audit / Log	RTC, Tamper	TF-M	-

Certification targets

psacertified™ level three

SESIP™3

Certificate includes physical protections

life.augmented

Enhancing STM32 security assurance levels with STSECURE

life.augmented

The building blocks of security

Crypto engine

- Basic crypto services embedded in dedicated ICs

Computer firmware

- Pure software countermeasures against remote software attacks mainly
- Self-evaluated solution

MCU / MPU with embedded security

Broad MCU portfolio

- Countermeasures against remote software and board level attacks
- **STM32Trust** Security framework
- Arm® TrustZone®
- **SESIP** & **PSA** certifications
- Secure programming services

MCU + Secure element

Trusted components

- Tamper resistance (Hardware & SoC)
- **Common Criteria**, **GSMA**, TCG certifications
- Proven against all attacks (remote software, board level and silicon level attacks)

Life cycle Security Centric devices

- Secure development methodology
- Secure personalization & key provisioning
- Secure supply chain
- Certified Common Criteria sites

Main STM32 MCU / MPU

Unique Identity	SW Isolation
TRNG	Process Isolation
Crypto	Security Life Cycle
Secure Boot	Root of Trust
Secure Upgrade	DPA
Secure FW Inst	STSAFE Drivers

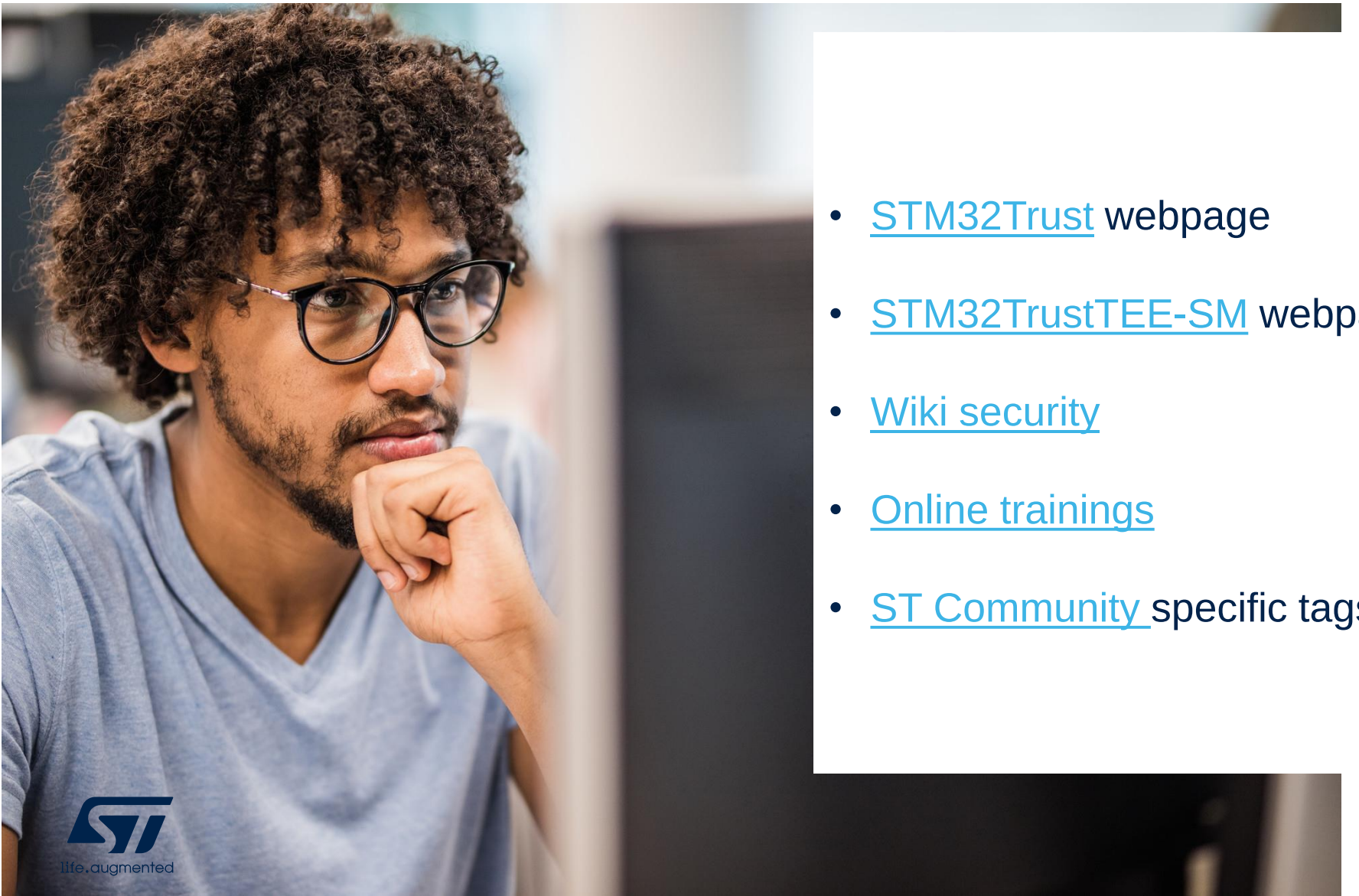
Secure companion chip

- STSAFE Application
- Root of Trust
- Key Storage
- Crypto Functions
- 6KB Data Storage

life.augmented

Where to find help

Documentation and useful links

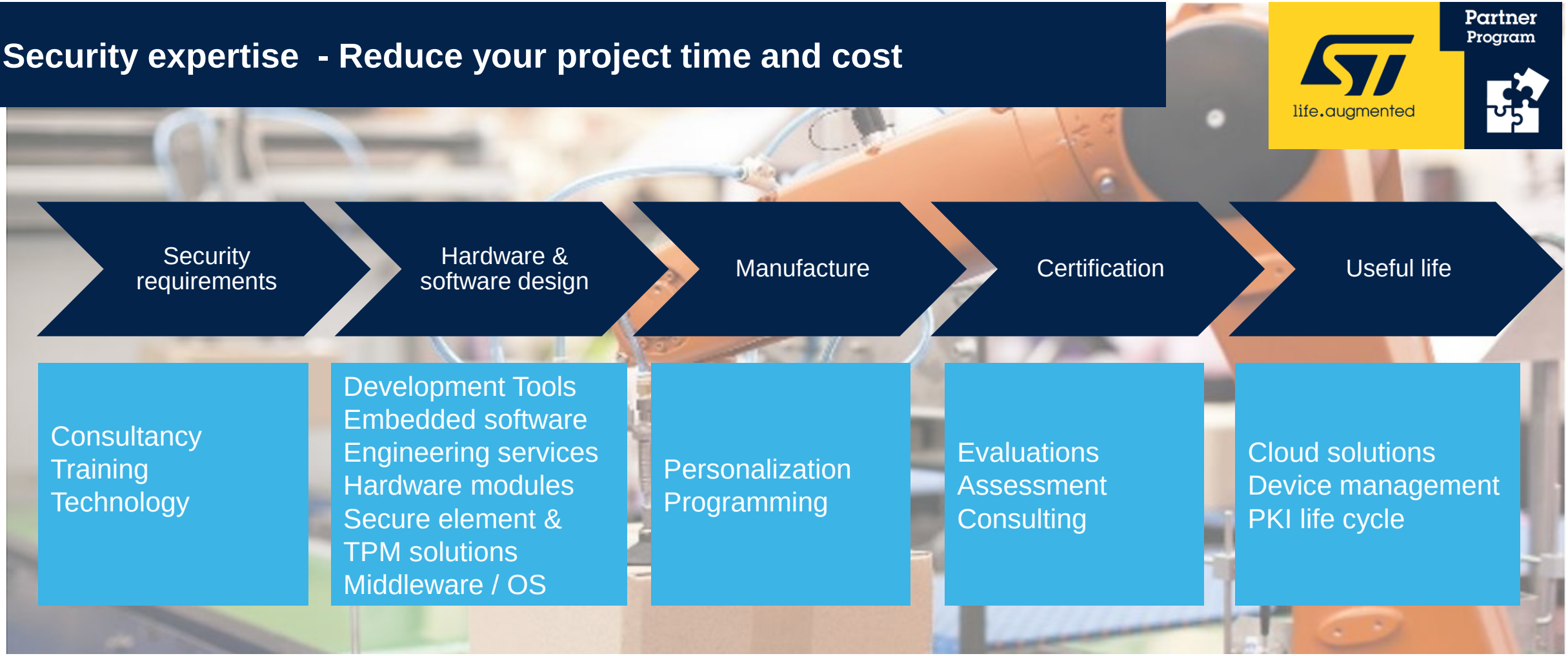


- STM32Trust webpage
- STM32TrustTEE-SM webpage
- Wiki security
- Online trainings
- ST Community specific tags

Get support from ST authorized partners

Security expertise - Reduce your project time and cost

life.augmented Partner Program



life.augmented

Our technology starts with You

Find out more at www.st.com/stm32trust

life.augmented