life.augmented

STM32Trust

The STM32 security framework for protecting embedded systems

STM32

Outline

1 What is security?

2 STM32Trust framework

3 STM32Trust security functions

4 STM32Trust TEE Secure Manager

5 Security in practice

6 Security functions by product

Access useful links

See abbreviation glossary and definitions

life.augmented

Click to go to the relevant sections

What is security?

life.augmented

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.

Confidentiality
C.I.A
TRIAD
Availability
Integrity

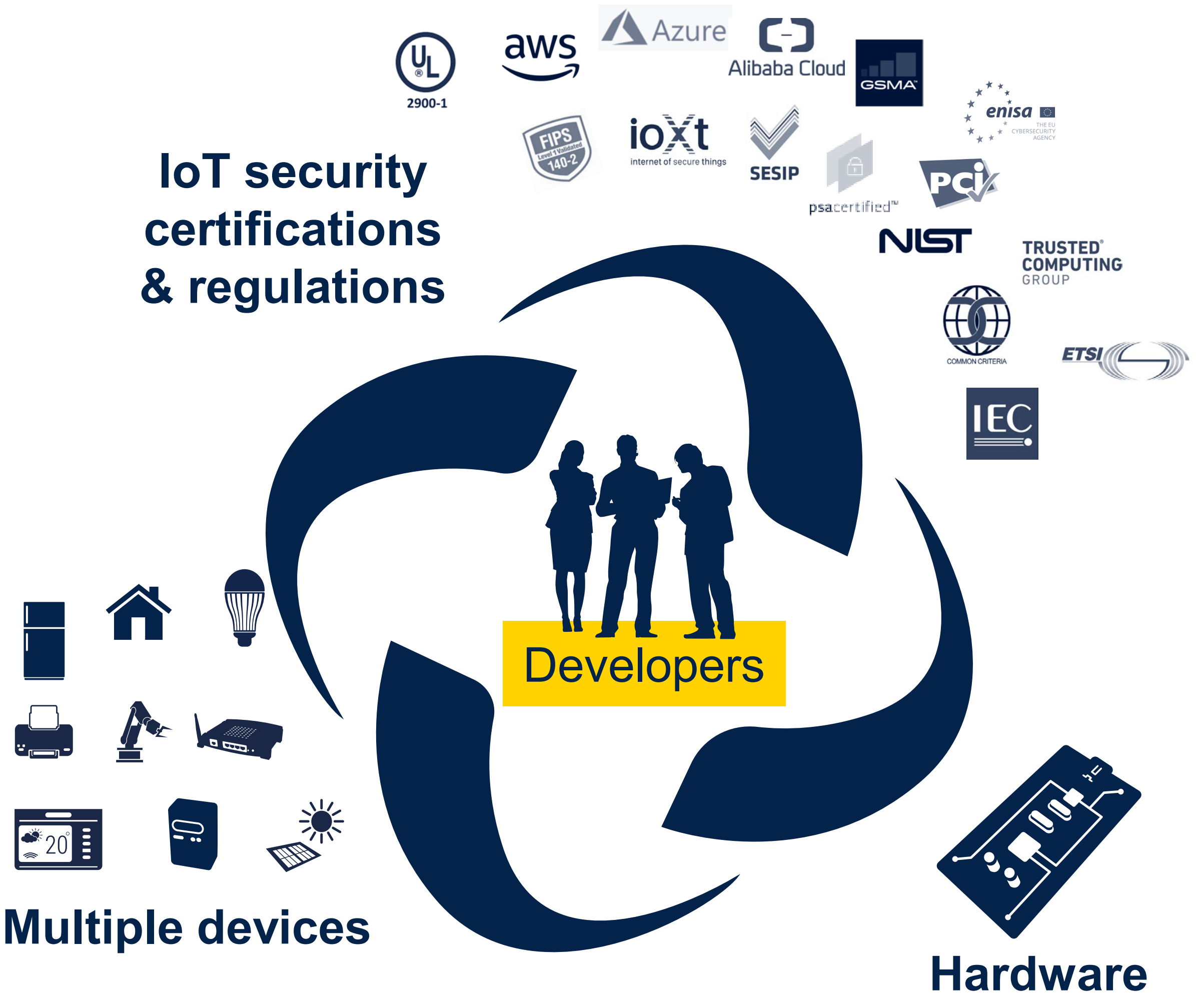
Addressing the security challenges and gaps

Security challenges for our customers

Complex	High cost	Time to market

Missing link

Scalability, certification, maintenance.
Core security hardware and services



IoT security certifications & regulations

Developers

Multiple devices

Hardware

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

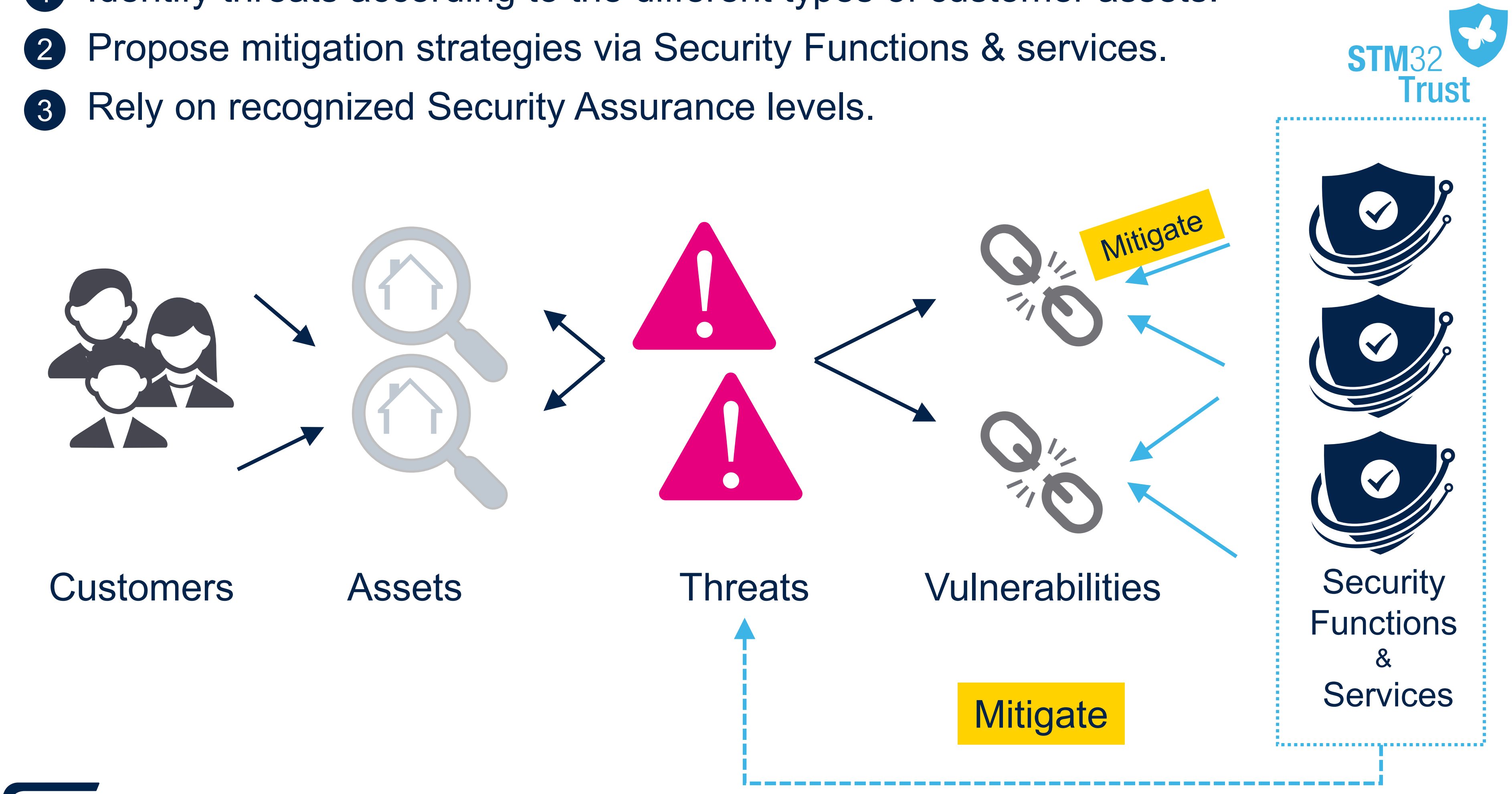
Availability

Authentication

Confidentiality

Threat assessment workflow

1. Identify threats according to the different types of customer assets.
2. Propose mitigation strategies via Security Functions & services.
3. Rely on recognized Security Assurance levels.



Threats exploit **vulnerabilities** & damage **assets**.

Protections mitigate **vulnerabilities** & therefore can mitigate **threats**.

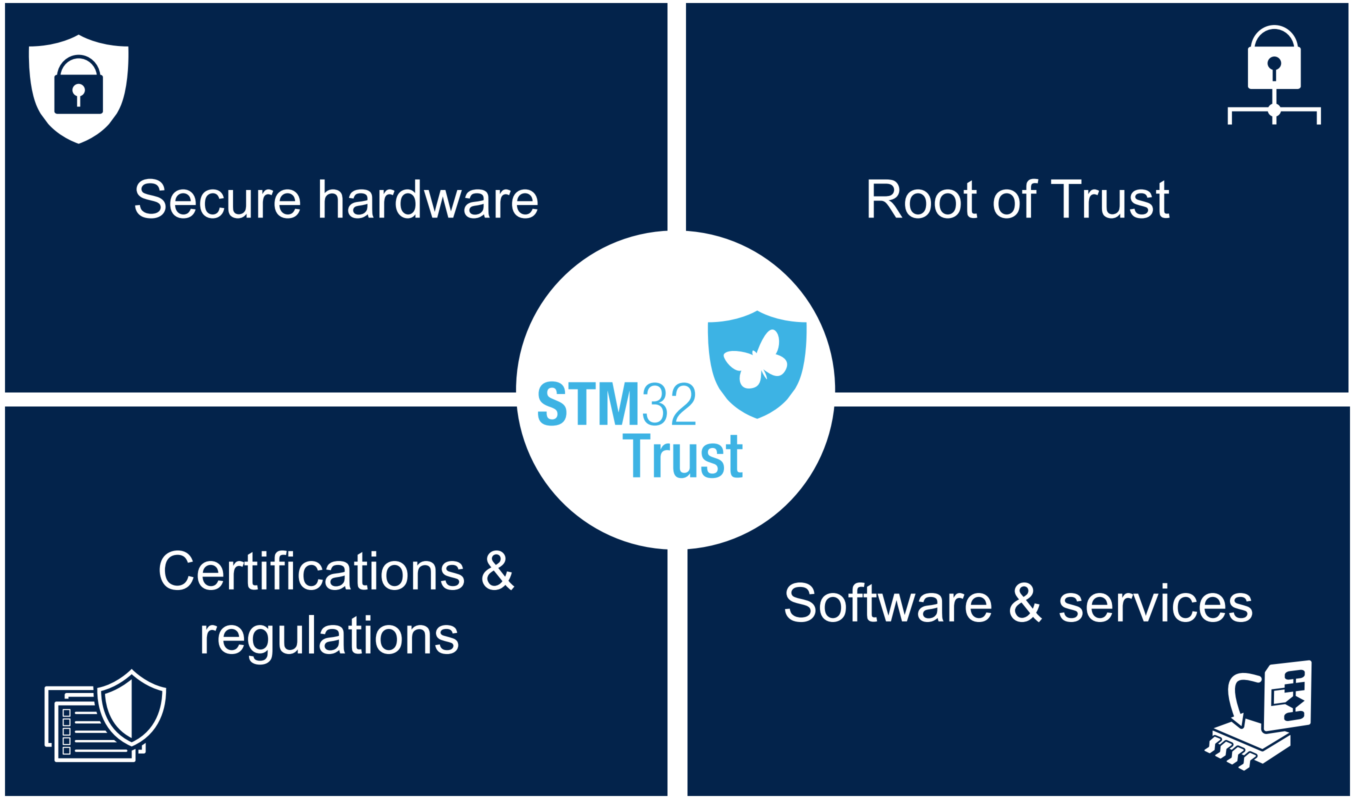
life.augmented

The STM32Trust framework

life.augmented

What is STM32Trust?

STM32Trust is built on key pillars to ensure security



Secure hardware

Root of Trust

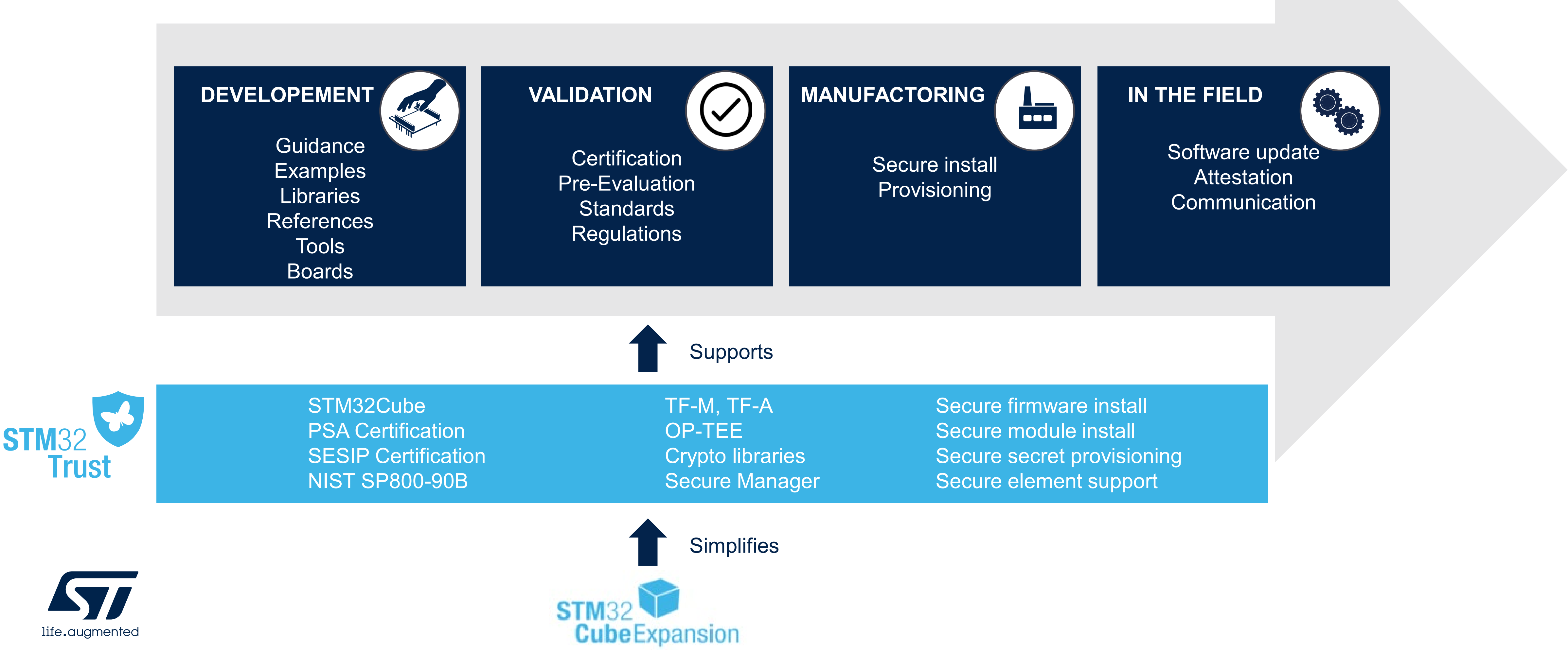
STM32 Trust

Certifications & regulations

Software & services

Software and services

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



DEVELOPEMENT

Guidance
Examples
Libraries
References
Tools
Boards

VALIDATION

Certification
Pre-Evaluation
Standards
Regulations

MANUFACTORING

Secure install
Provisioning

IN THE FIELD

Software update
Attestation
Communication

Supports

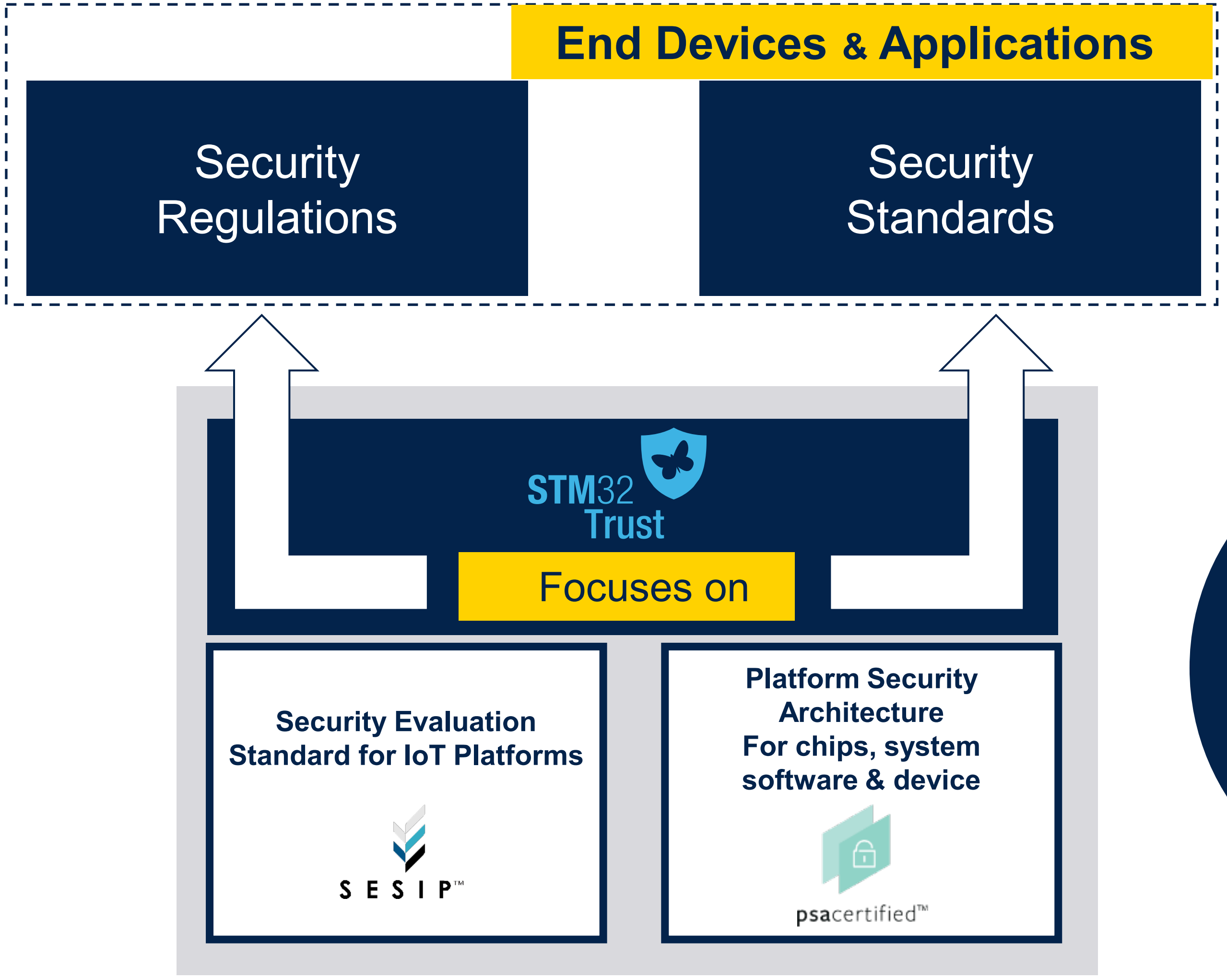
STM32Cube
PSA Certification
SESIP Certification
NIST SP800-90B

TF-M, TF-A
OP-TEE
Crypto libraries
Secure Manager

Secure firmware install
Secure module install
Secure secret provisioning
Secure element support

Simplifies

Certifications & Regulations



End Devices & Applications

Security Regulations

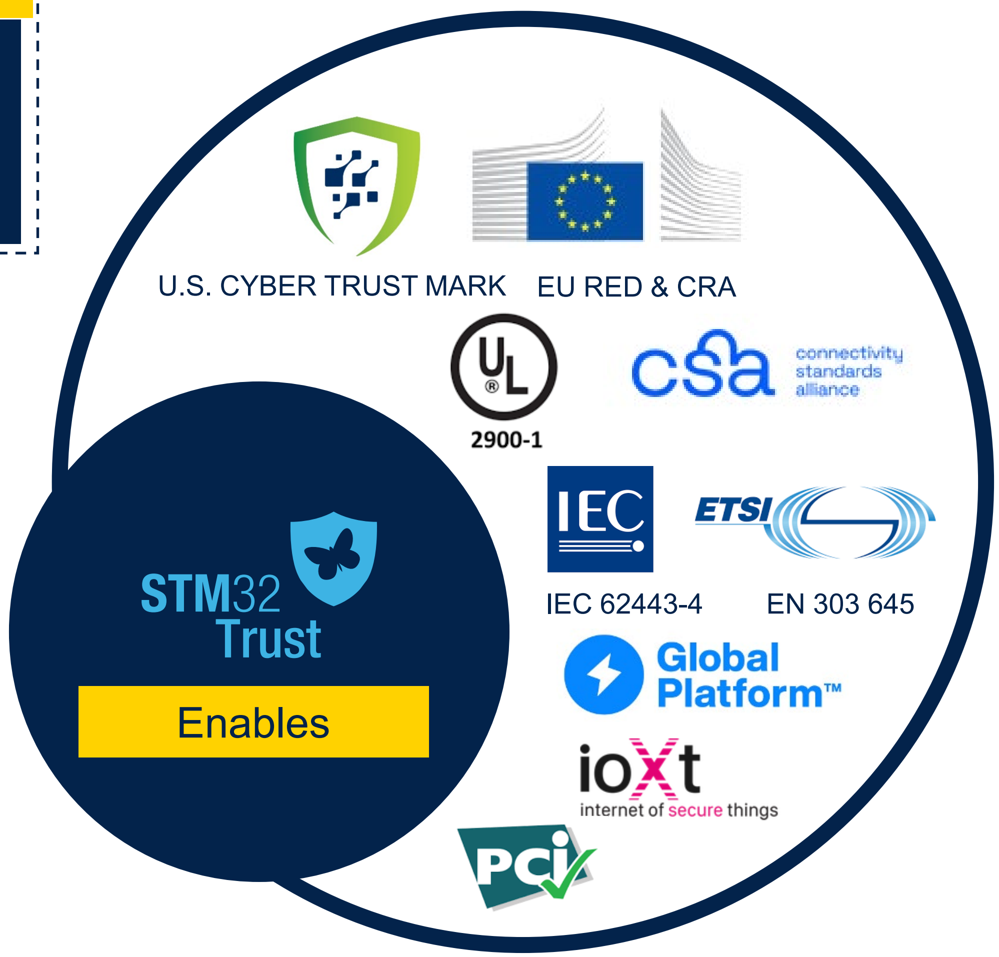
Security Standards

STM32 Trust

Focuses on

Security Evaluation Standard for IoT Platforms

Platform Security Architecture For chips, system software & device



STM32 Trust

Enables

U.S. CYBER TRUST MARK

EU RED & CRA

2900-1

IEC 62443-4

EN 303 645

UL
csa connectivity standards alliance
IEC
ETSI
Global Platform™
ioXt
internet of secure things
PCI

Focus on RED and CRA standards

Radio Equipment Directive (RED)

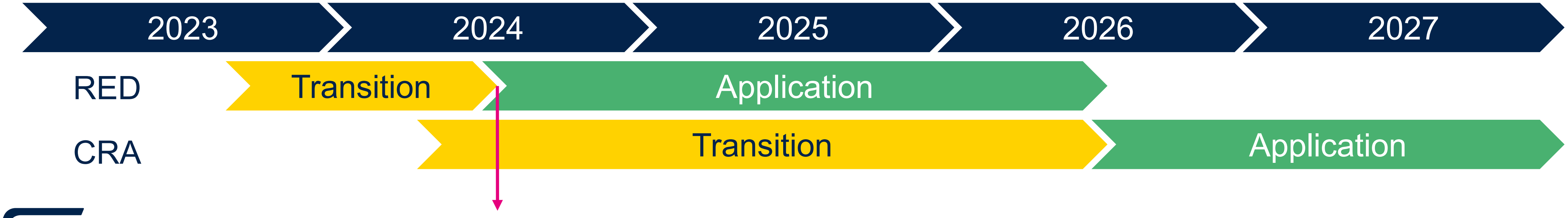
Goal: increase security for radio connected devices.

- 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



August 1, 2024

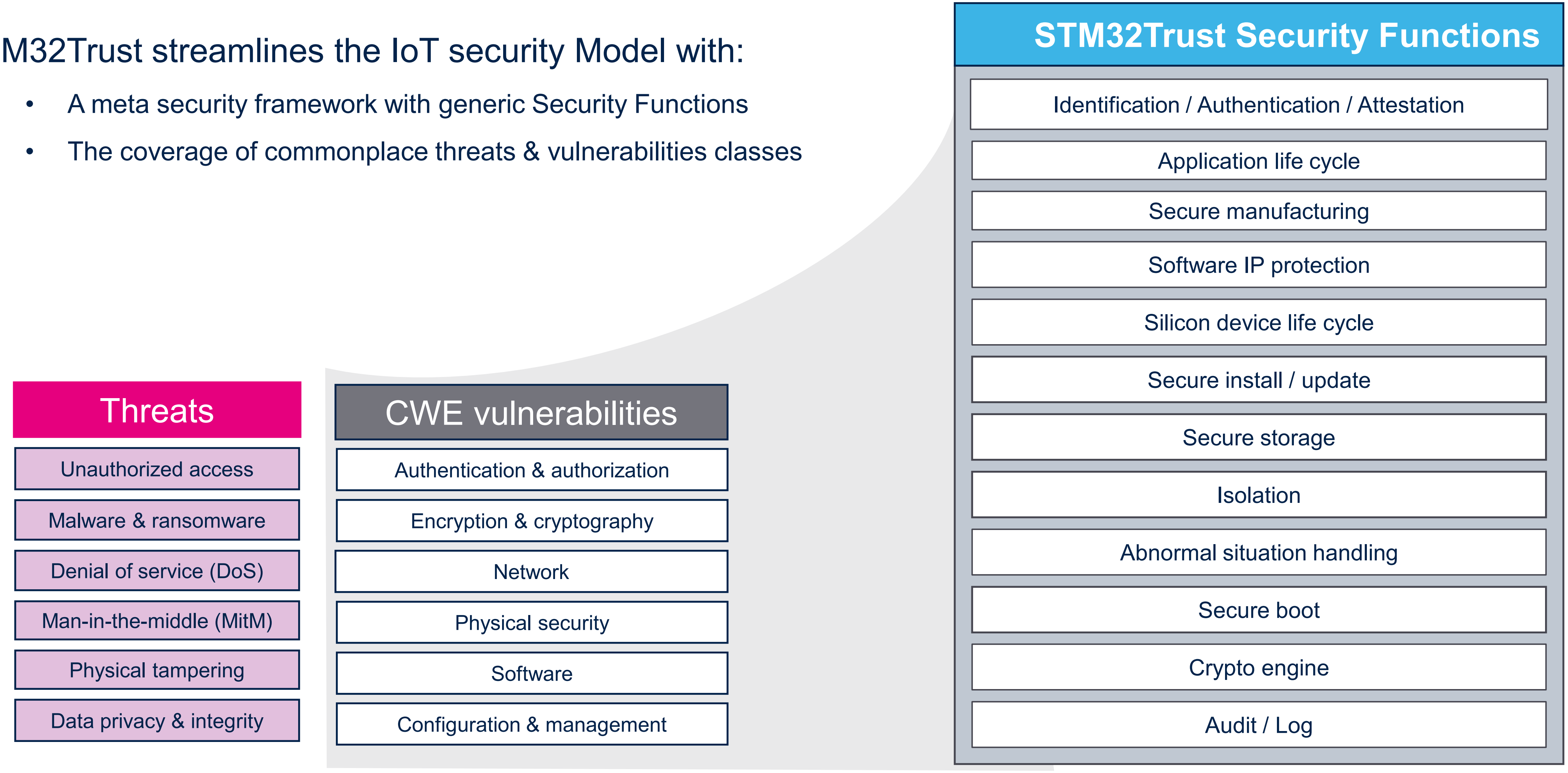
STM32Trust Security Functions

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

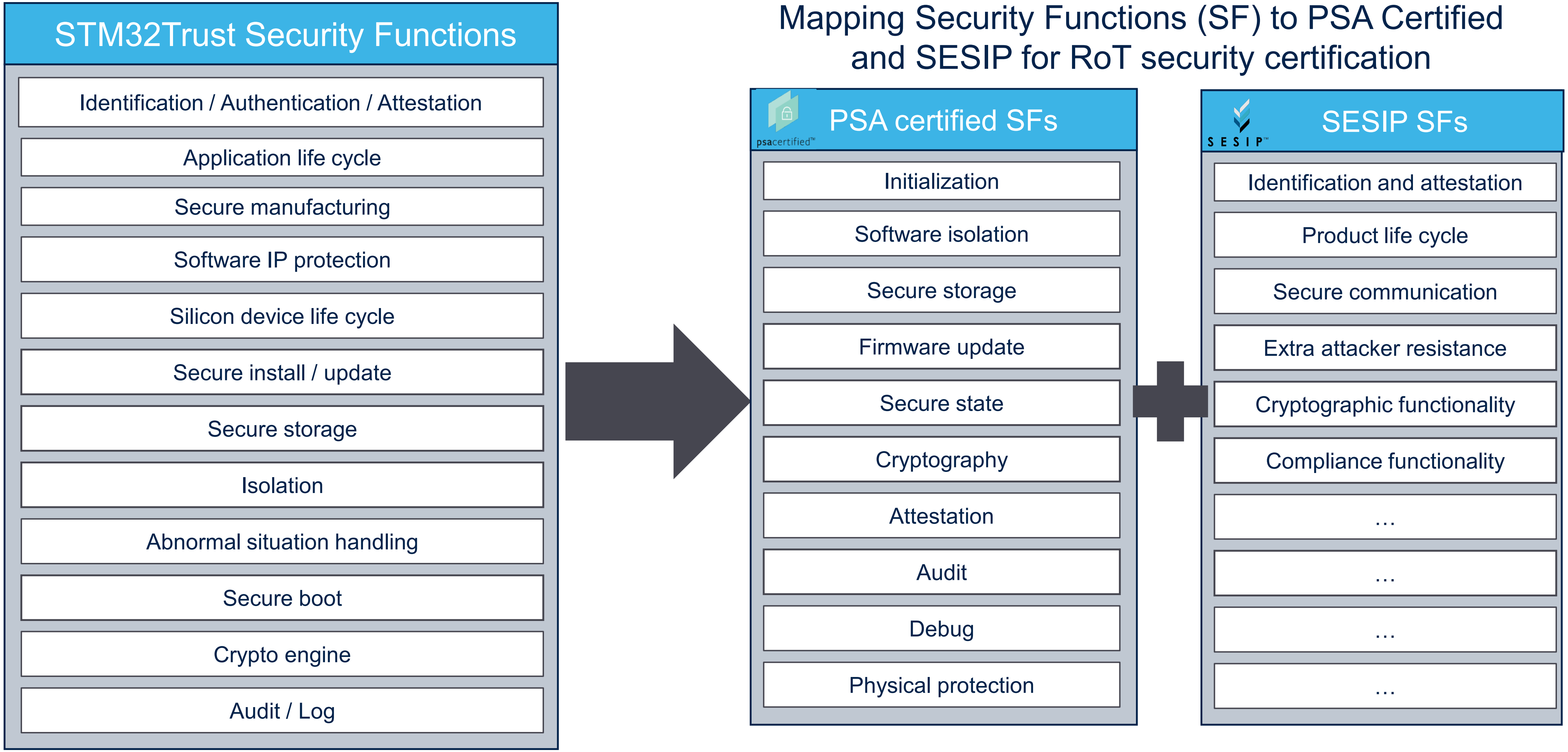
CWE vulnerabilities

- 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

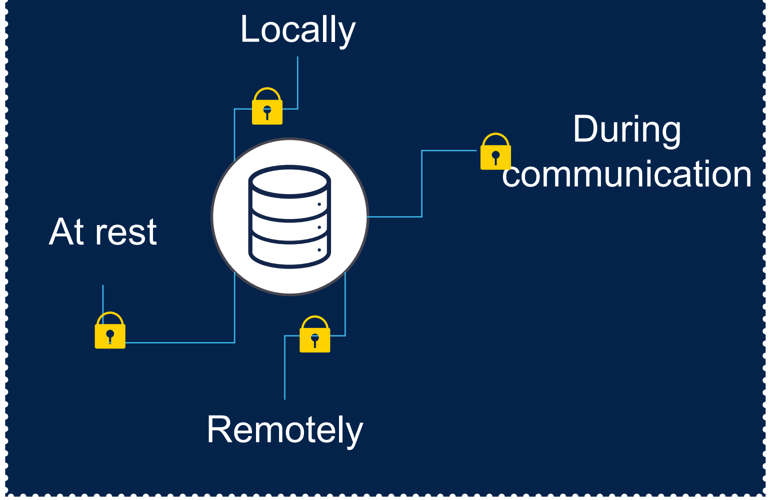
MPU		PSA Certified Level 1 STM32**MP15**	PSA Certified Level 1 SESIP3 STM32**MP13**
High perf MCUs		PSA Certified Level 1 STM32**H7**	PSA Certified Level 1 SESIP3 STM32**H5**
Mainstream MCUs	PSA Certified Level 1 STM32**G0**	PSA Certified Level 1 STM32**G4**	PSA Certified Level 1 STM32**C0**
Ultra-low-power 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**

STM32Trust TEE Secure Manager

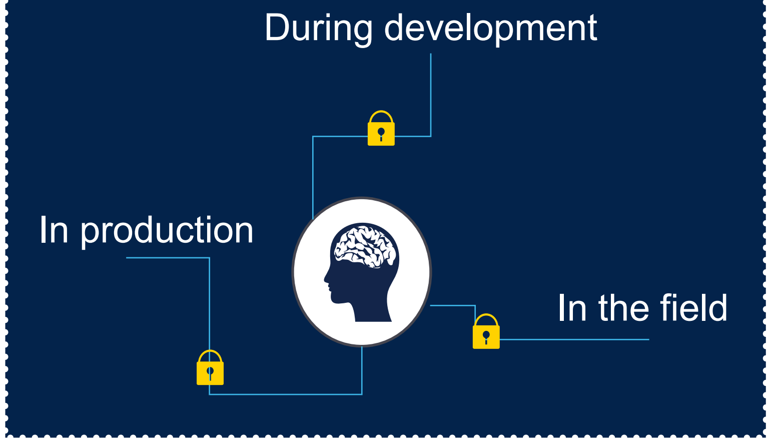
life.augmented

Embedded security
What are developers typically trying to achieve?

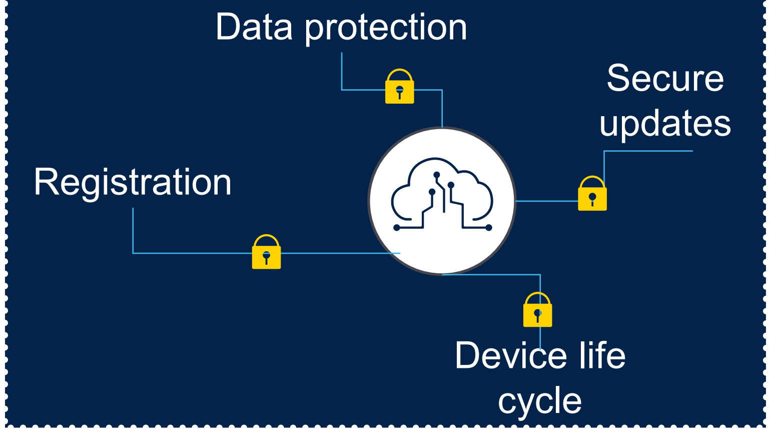
Easily protect my critical data & secrets and those of my end customers



Easily protect my IP and my partner's IP in a strong and effective way



Easily & securely connect to clouds & servers without painful digital identities management



STM32 Trust TEE

Introducing the STM32Trust TEE Secure Manager

Secure Manager

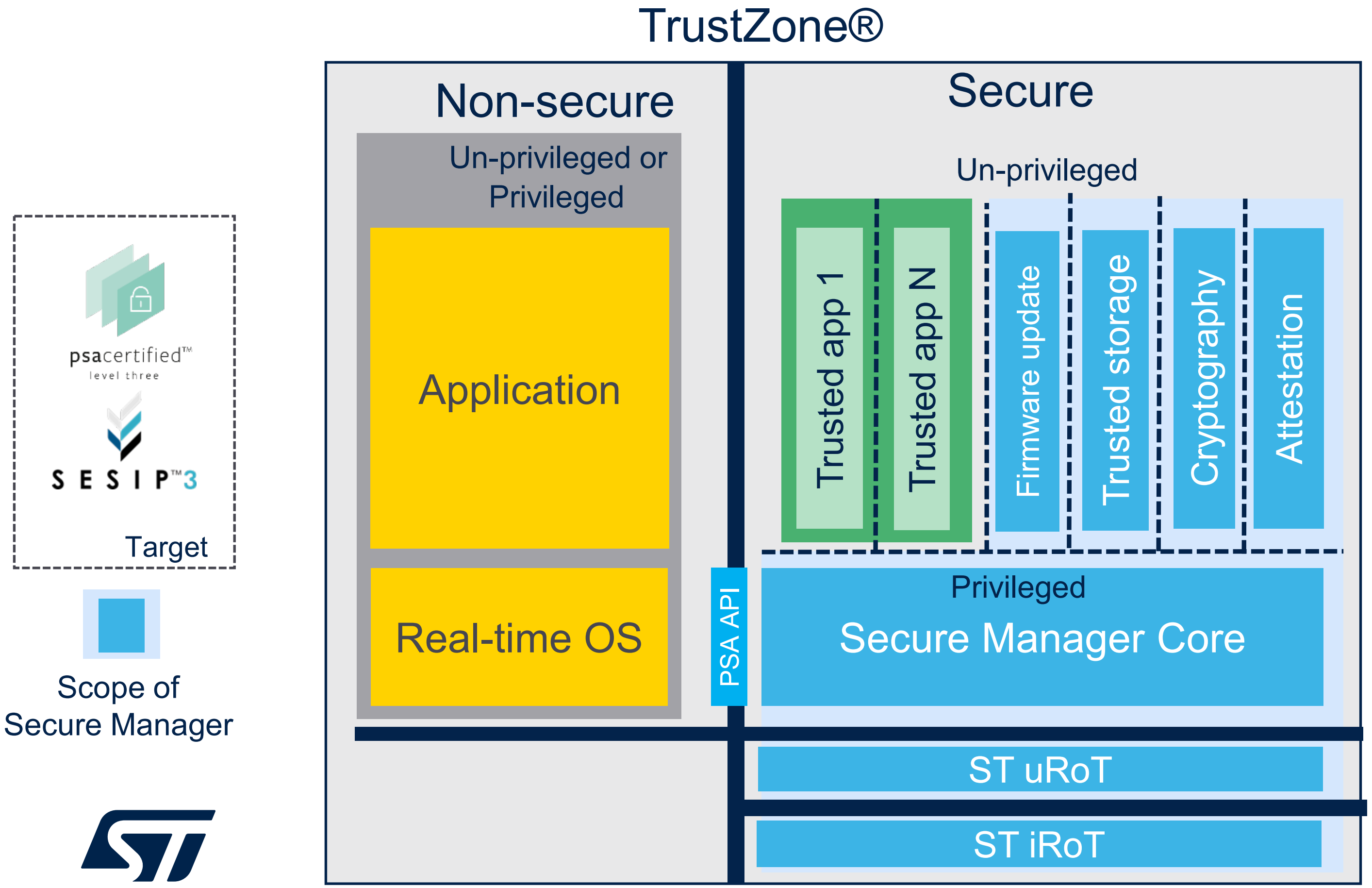
A **trusted execution environment (**TEE) integrating core security services

A set of turnkey security services developed, maintained, and certified by ST

life.augmented

Secure Manager
First used in the STM32H5 platform

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

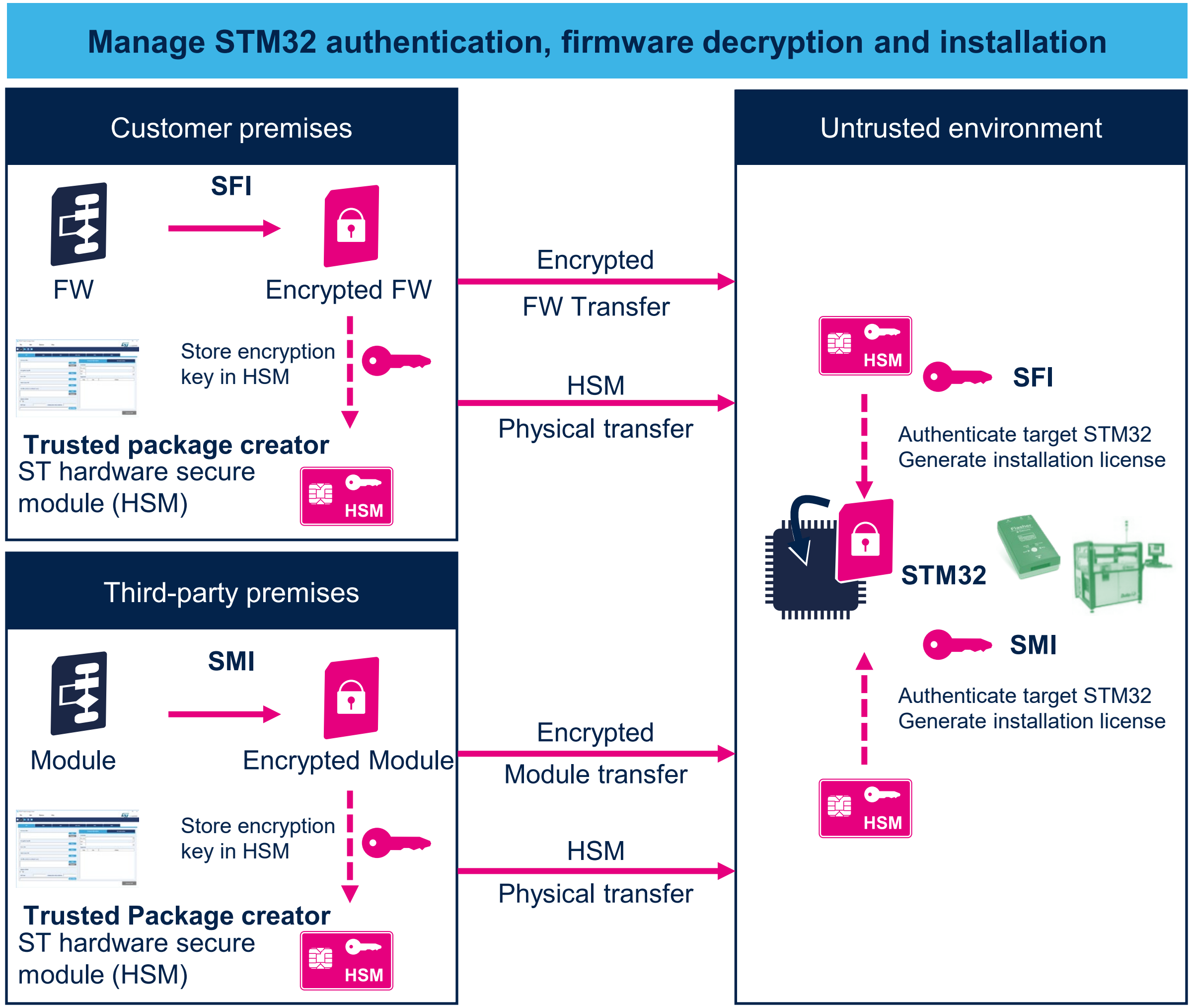


- ST platform ownership
- Turnkey set of security services
- Secure Manager Core to handle isolation
- Multitenant software IP protection
- Arm® PSA API compatible
- Designed for long-term-support (LTS)
- Modular secure update capable
- Optimized certification properties
- Certified and maintained by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

Secure firmware and secret installation

life.augmented

Embedded secure firmware install - SFI



Manage STM32 authentication, firmware decryption and installation

Customer premises

SFI

FW

Encrypted FW

Store encryption key in HSM

Trusted package creator
ST hardware secure module (HSM)

Encrypted FW Transfer

HSM Physical transfer

Third-party premises

SMI

Module

Encrypted Module

Store encryption key in HSM

Trusted Package creator
ST hardware secure module (HSM)

Encrypted Module transfer

HSM Physical transfer

Untrusted environment

SFI

Authenticate target STM32
Generate installation license

STM32

SMI

Authenticate target STM32
Generate installation license

Secure Loader embedded services provisioned by ST
➔ mass market approach

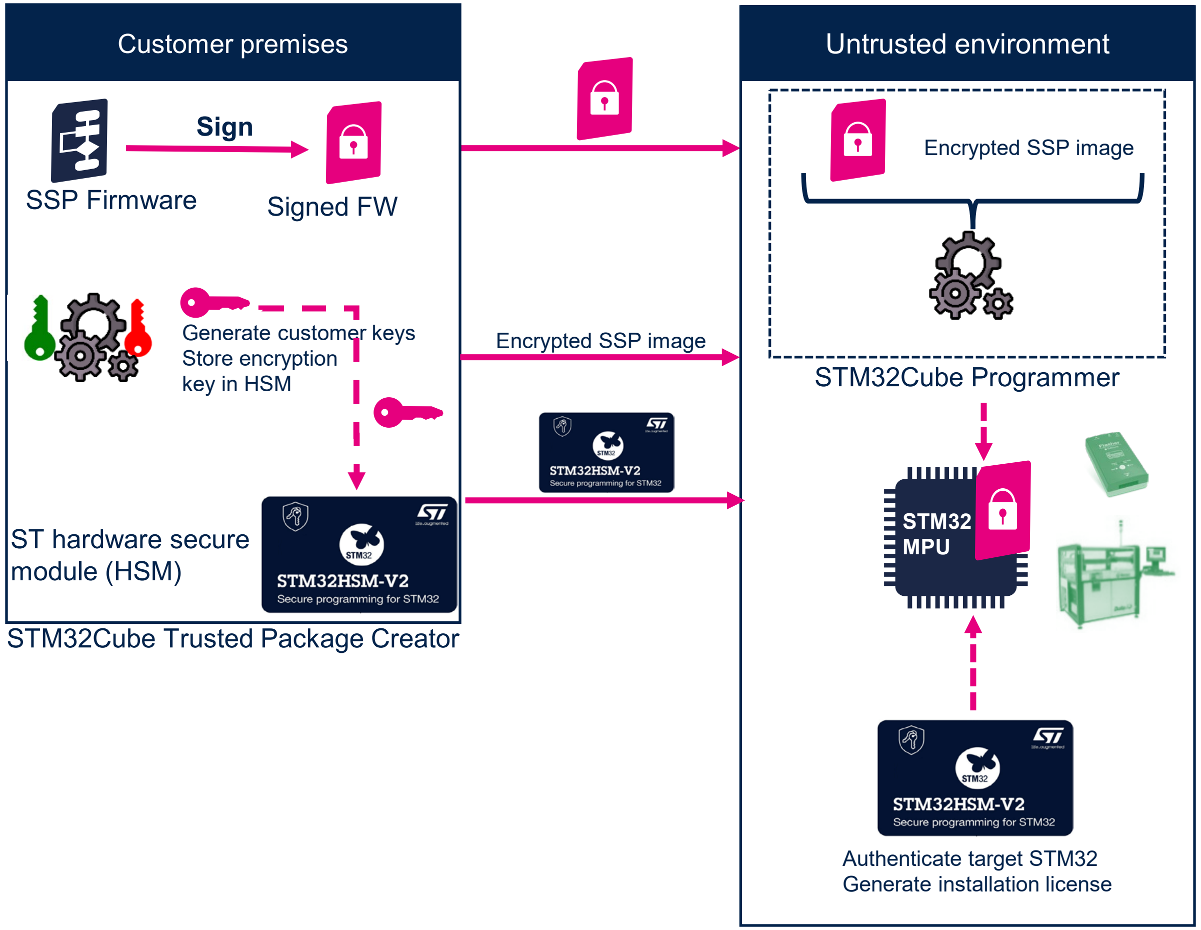
ST ecosystem
with
Encryption, HSM, and programming tools

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

Protect third-party software IP
(SMI)

Embedded secure secret provisioning - SSP

Manage STM32 authentication, license generation and secure key transfer



Customer premises

SSP Firmware → Sign → Signed FW

Generate customer keys
Store encryption key in HSM

ST hardware secure module (HSM)

STM32Cube Trusted Package Creator

Encrypted SSP image

Untrusted environment

Encrypted SSP image

STM32Cube Programmer

STM32 MPU

Authenticate target STM32
Generate installation license

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

Security in practice

STM32 Trust

Customer example (1/6) 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

IP protection

Required Security Functions

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

Customer example (2/6) 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

Customer example (3/6) focus on secure maintenance & update

Asset

Product trustability

Mark’s company sells costly equipment.
He plans to offer remote maintenance and updates.
He wants to ensure that the remote updates are only performed on the equipment sold by his company and that only his firmware pack runs on the devices.

.

What Mark wants to achieve

- Ensure only his equipment benefits from remote updates
- Access to information on product state
- Ensure that the firmware update is carried out in a secure way

Secure connectivity

- Firmware authentication and integrity

System integrity

Required Security Functions

- Identification/Authentication/ Attestation
- Secure Install/Update
- Secure boot
- Memory protections

STM32 Trust

Customer example (4/6) focus on data management

Asset

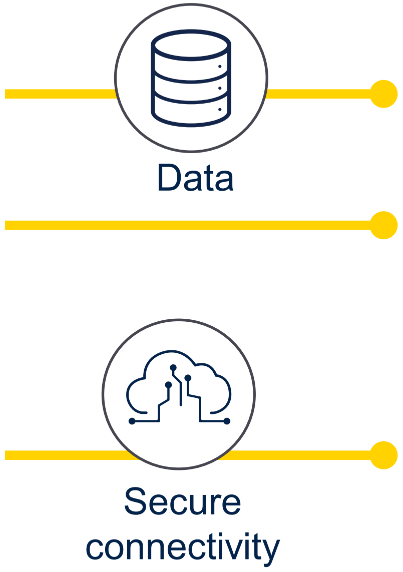
Company data

Oliver sells devices that report sensitive data to servers. Oliver needs to make sure the data cannot be exposed outside of his company.

What Oliver wants to achieve

- Ensure the data transmitted is not exposed
- Secrecy in data encryption keys
- Ensure data is sent from authenticated devices
- Ensure data is sent to authenticated servers

Required Security Functions



- Crypto engine
- Secure storage
- Identification/Authentication/ Attestation

STM32 Trust

Customer example (5/6)
focus on remote access & control

Asset

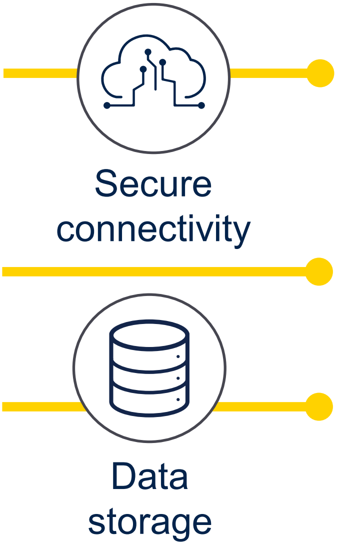
Device integrity

Rose controls her device fleet remotely.
She wants to make sure her devices have not been hacked and have full control over the devices at any time.

What Rose wants to achieve

- Unique identity for each device
- Device authentication
- Attest device access rights
- Secure device communication
- Ensure that identities and access rights cannot be hacked, even at the manufacturing stage

Required Security Functions



- Identification/Authentication/ Attestation
- Crypto engine
- Secure storage and secure manufacturing (secure personalization)

Customer example (6/6) focus on data protection

Asset

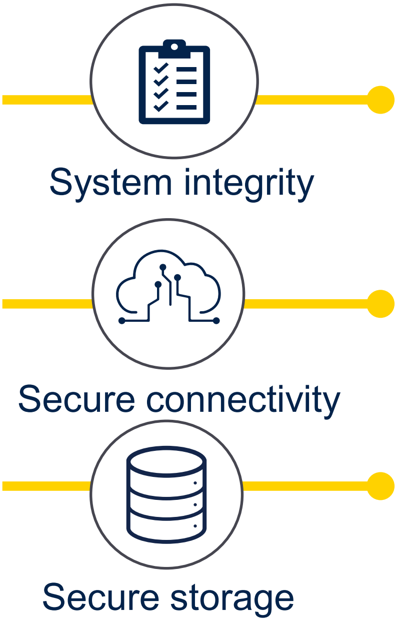
Data

Jack collects and stores user data in his devices
Jack's devices and large-scale systems need to comply with regulations (such as GDPR).

What Jack wants to achieve

- Platform integrity
- Integrity of user data
- Secure storage of user data

Required Security Functions


System integrity

Secure connectivity

Secure storage

- Secure boot
- Abnormal situation handling

- Crypto engine
- Identification/Authentication/Attestation

- Secure storage

Security Functions and services in STM32 products

life.augmented

The STM32 portfolio

STM32

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

life.augmented

MPU portfolio

MCU portfolio

Mainstream products with security functions

STM32Fx

★STM32F0

★STM32F1*

★STM32F2**

STM32Trust Security Functions	Features		
	Hardware	Software	Services
Identification / Authentication / Attestation	Unique ID	-	-
Application life cycle	OTP**	-	
Secure manufacturing	-	-	-
Software IP protection	MPU**, WRP	-	-
Silicon device life cycle	WRP	-	CubeProgrammer
Secure install / update	-	-	-
Secure storage	-	-	-
Isolation	-	-	-
Abnormal situation handling	Tamper, RTC		-
Secure boot	-	-	-
Crypto engine	-	-	-
Audit / Log	-	-	-

Certification targets

STM32 Trust

Mainstream products with security functions

STM32Cx	STM32Trust Security Functions	Features		
		Hardware	Software	Services
★STM32C0	Identification / Authentication / Attestation	Unique ID	-	-
	Application life cycle	-	-	
	Secure manufacturing	-	-	-
	Software IP protection	MPU, WRP	-	
	Silicon device life cycle	WRP	-	CubeProgrammer
	Secure install / update	-	-	-
	Secure storage	-	-	-
	Isolation	MPU	-	-
	Abnormal situation handling	Tamper, RTC		-
	Secure boot	-	-	-
	Crypto engine	-	-	-
	Audit / Log	-	-	-

Certification targets

psacertified™
level one

life.augmented

Mainstream products with security functions

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	-	-	-

Mainstream products with security functions

STM32Gx

STM32G0

STM32G4

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	-	-	-

Certification targets

psacertified™
level one

STM32 Trust

Ultra-low-power products with security functions

STM32Lx

★STM32L0

★STM32L4

★STM32L5

Certification targets

STM32Trust Security Functions	Features		
	Hardware	**Software**	**Services**
Identification / Authentication / Attestation	Unique ID		-
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	-		-

life.augmented

STM32 Trust

Ultra-low-power products with security functions

STM32Lx

- ☆ STM32L0
- ★ STM32L4
- ☆ STM32L5

STM32Trust Security Functions	Features		
	Hardware	Software	Services
Identification / Authentication / Attestation	Unique ID		-
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

life.augmented

Ultra-low-power products with security functions

STM32Lx

- STM32L0
- STM32L4
- STM32L5

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	-

Certification targets

psacertified™ level one

SESIP™3

STM32 Trust

Ultra-low-power products with security functions

STM32Ux	STM32Trust Security Functions	Features		
		Hardware	Software	Services
★STM32U5	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

life.augmented

STM32 Trust

High performance products with security functions

STM32Fx

★STM32F3

★STM32F4

★STM32F7

Certification targets

STM32Trust Security Functions	Features		
	Hardware	Software	Services
Identification / Authentication / Attestation	Unique ID	-	-
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	-	-	-

life.augmented

STM32 Trust

High performance products with security functions

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 PCL : Protected Crypto Library

High performance products with security functions

STM32Fx

★ STM32F3

★ STM32F4

★ STM32F7

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	-	
Silicon device life cycle	WPR, RDP	-	CubeProgrammer
Secure install / update	HDP, WPR, RDP, UBE	X-CUBE-SBSFU	CubeProgrammer (digest, signature)
Secure storage	HDP, OTFDEC	-	-
Isolation	MPU	-	-
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	-	-	-

Certification targets

Notes: (1) side channel PCL : Protected Crypto Library

STM32 Trust

High performance products with security functions

STM32Hx

★ STM32H5

★ STM32H7

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	-

Certification targets

psacertified™ level three

SESIP™3

Certificate includes physical protections

life.augmented

STM32 Trust

High performance products with security functions

STM32Hx

★ STM32H5

★ STM32H7

STM32Trust Security Functions	Features		
	Hardware	Software	Services
Identification / Authentication / Attestation	Unique ID, device certificate	-	STSAFE support
Application life cycle	OTP	-	-
Secure manufacturing	RSS	SFI	XCUBE-SFI, FastROM
Software IP protection	RDP, MPU, PCROP	SFI	XCUBE-SFI
Silicon device life cycle	HDP, WPR, RDP, PCROP	-	CubeProgrammer
Secure install / update	HDP, WPR, RDP, UBE	X-CUBE-SBSFU	CubeProgrammer (digest, signature)
Secure storage	HDP, OTFDEC	-	-
Isolation	MPU, HDP, PCROP	-	-
Abnormal situation handling	Tamper, RTC, GPIO lock, CSS, ECC, Temp. sensor, PVD, WD, BR	-	-
Secure boot	HDP, WPR, RDP, UBE	X-CUBE-SBSFU	CubeProgrammer (digest, signature)
Crypto engine	HASH (SHA1, MD5), AES, DES/TDES, OTFDEC, TRNG	X-CUBE-CRYPTOLIB, PCL[1]	-
Audit / Log	-	-	-

Certification targets

psacertified™
level one

Notes: (1) side channel PCL : Protected Crypto Library

Wireless products with security functions

STM32Wx

★ STM32WB

★ STM32WBA

★ STM32WL5

Certification targets

STM32Trust Security Functions	Features		
	Hardware	Software	Services
Identification / Authentication / Attestation	Unique ID, 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	-	-	-

STM32 Trust

Wireless products with security functions

STM32Wx

★ STM32WB

★ **STM32WBA**

★ STM32WL5

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

Wireless products with security functions

STM32Wx

★ STM32WB

★ STM32WBA

★ STM32WL5

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

Certification targets

STM32 Trust

MPU products with security functions

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

Enhancing STM32 security assurance levels with STSECURE

life.augmented

STM32 Trust

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

STM32

MCU + Secure element

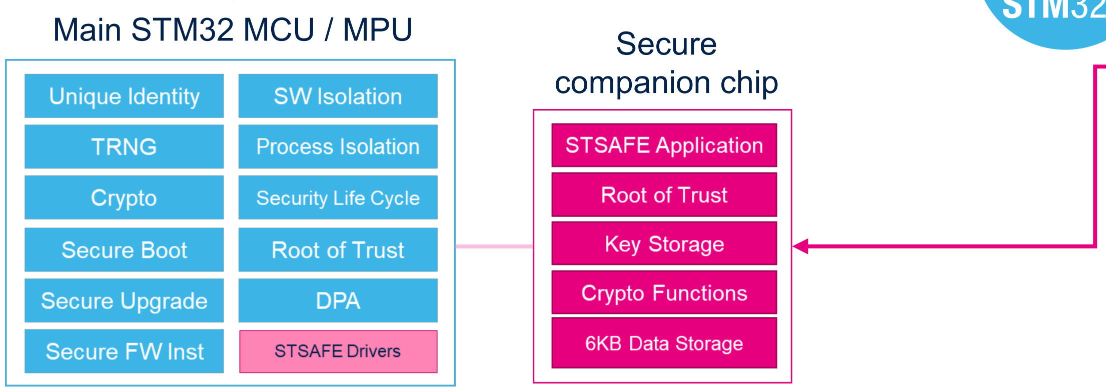
Trusted components

- 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

STSECURE



Main STM32 MCU / MPU

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

Secure companion chip

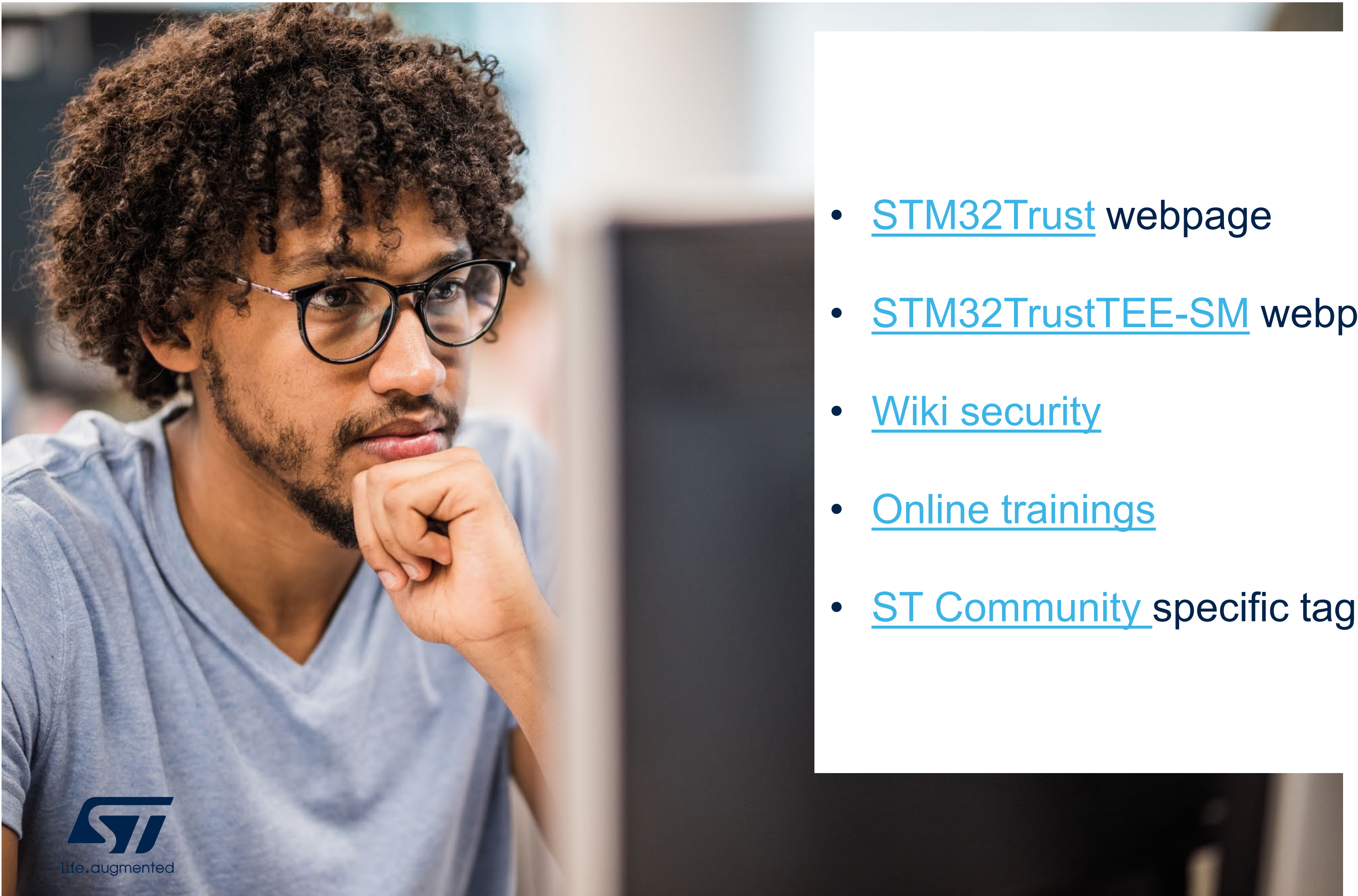
- STSAFE Application
- Root of Trust
- Key Storage
- Crypto Functions
- 6KB Data Storage

life.augmented

Where to find help

life.augmented

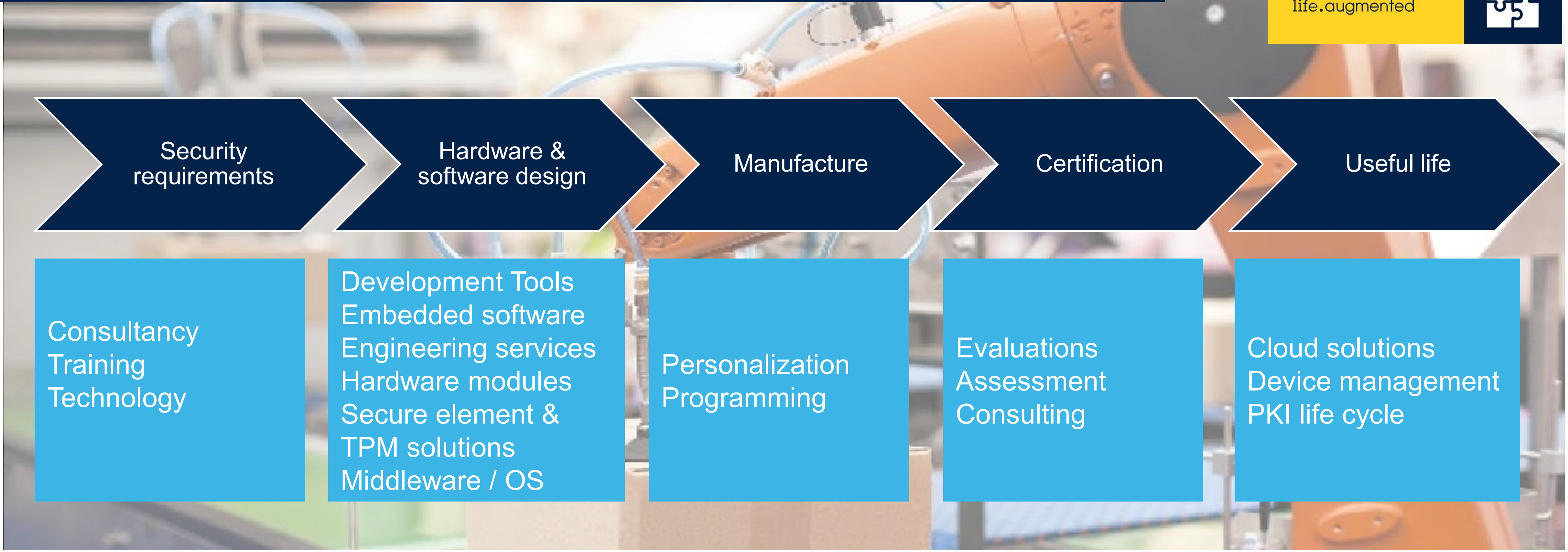
Documentation and useful links



- 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



Security requirements	Hardware & software design	Manufacture	Certification	Useful life
Consultancy Training Technology	Development Tools Embedded software Engineering services Hardware modules Secure element & TPM solutions Middleware / OS	Personalization Programming	Evaluations Assessment Consulting	Cloud solutions Device management PKI life cycle

Abbreviation glossary and definitions

life.augmented

Abbreviation glossary and definitions

Glossary	Benefit and explanation
AES Key storage	Write-only key registers in AES engine.
Antitamper / active tamper / backup registers	Protect against a wide range of physical attacks on a hardware system outside the MCU. Erases backup registers information when tamper is detected.
BSEC & boot ROM	Device life cycle managed through OTP and BSEC.
Certificate (unique per chip)	Enables to authenticate a genuine STM32.
CSS (clock security system)	Internal clock available for secured program execution independently from external source clock.
Device 96-bit unique ID	Enables product traceability. Can be used for security key diversification.
DPA Resistant Crypto Library* (FIPS-140)	DPA resistant version of Cryptographic library. Available on specific part numbers after on demand adaptation
ECC (error correction code)	Robust memory integrity. Hardened protection against fault injection attacks thanks to error detection.
FastROM Programming services	Pre-loading of customer software in STM32 done by ST manufacturing
Firewall	Simple isolation in two domains for RAM and flash. Allows to protect software IP.
GPIO locking	Lock of selected GPIO. Impossible to unlock until next reset. Ability to lock communication channels after tamper detection.
GTZC (global TrustZone® controller)	Illegal access tracking and internal log/action.
HASH	Hash algorithms implemented by hardware, like SHA.
HDP (hide protect)	Temporal isolation ensuring secure boot is not seen after first execution.

Abbreviation glossary and definitions

Glossary	Benefit and explanation
MMU (memory management unit)	Ensures privileged access to some portion of application–task isolations.
OP-TEE (Part of OpenSTLinux)	Trusted Execution Environment for STM32MP, featuring Secure storage service
OP-TEE (Part of OpenSTLinux)	Trusted Execution Environment for STM32MP, adding further software handling for application portions sandboxing
OTFDEC (on the fly decryption)	Decryption of encrypted image on external flash.
OTFDEC (on the fly decryption)	Decryption of encrypted content stored on external flash.
OTP (one time programmable) memory	OTP zones where application credentials or life cycle states can be stored.
PCROP (proprietary code readout protection)	Ability to set some flash sectors as execute-only, thus preventing other sectors to read them.
PKA (public key accelerator)	Asymmetric algorithms (public key), implemented by hardware, for RSA/ECC/DH.
PVD (power voltage monitoring)	Monitors power changes.
RDP (Read protection)	Prevents a debugger from reading the secure boot
RNG (random number generator)	True RNG done entirely by hardware.
RSS with SFI (root security services with secure firmware install)	Built-in service callable at reset, ensuring installation of an OEM firmware and option bytes, with authenticity, integrity, confidentiality, insurance to program a genuine STM32, and possibly limited overall quantity of programmed STM32.
RTC (alarm timestamp)	Timestamp on tamper events, or internal events.

Abbreviation glossary and definitions

Glossary	Benefit and explanation
Secure boot ROM code	Root of trust for loading first bootloader on STM32MP.
Secure boot with SSP (secure secret provisioning)	Built-in service callable at reset, ensuring secure provisioning of OEM credentials. Controllability of overall quantity of STM32MP1 provisioned.
Secure FSBL (First Stage bootloader)	Secure bootloader, loaded and authenticated by secure boot ROM code.
SSP (secure secret provisioning)	Secure provisioning of OTP secret values.
STM32CubeProgrammer	Software tool able to control the RDP cycle
Symmetric hardware crypto accelerators	Implements a given algorithm by hardware implementation, like AES for instance.
Temperature sensor	Checks if the device is operating in the expected temperature range. Hardened protection against temperature attacks.
TF-A (part of OpenSTLinux)	First-stage secure bootloader configuring STM32MP platform
TFM_SBSFU boot (part of STM32CubeL5)	Example code implementing both a secure boot and a secure firmware update mechanism
TrustZone®	Runtime isolation technology allowing 2 distinct worlds, secure and nonsecure. It is a complete set of hardware mechanisms to isolate two main security application domains: one trusted (ensuring secure storage) and one nontrusted.
TZC (TrustZone® controller)	Ability to isolate Cortex-A cores from Cortex-M one.
UBE (unique boot entry)	Ensures the silicon always boots at the secure boot location.
Watchdogs	Independent watchdog and window watchdog for software timing control.
WRP (write protection)	Prevents an application from altering the secure boot firmware.
X-CUBE-CRYPTOLIB	This ECCN 5D002-classified software is based on STM32Cube architecture package and includes a set of crypto algorithms based on firmware implementation (symmetric, asymmetric, hash…)
X-CUBE-SBSFU	code example implementing both a secure boot and a secure firmware update mechanism

Our technology starts with You

Find out more at www.st.com/stm32trust

life.augmented