STM32Trust

Marketing Presentation

V1.2

Agenda

# Overview

# 6 Customer examples

# 12 Security functions

Overview security functions versus STM32 portfolio

Security functions and ST offer

Evaluations and certifications

# Focus on SFI and SBSFU

STM32Trust overview

- STM32Trust offers a robust multi-level strategy to enhance security in new product designs, using our STM32 microcontrollers augmented with STSAFE secure elements.
- STM32Trust is the security framework combining our knowledge, ecosystem and security services.
- The STM32Trust solution offers a complete toolset for code and execution protection.
- STM32Trust ensures IP protection, data security, implements validated credentials, and safeguards firmware authenticity and secure firmware update.

Customer example (1/6)
Focus on Secure Manufacturing

Bob is CEO of a company designing toys.
He would like to make sure the firmware developed by his team is protected from theft and will only run on the hardware developed by his team.

What Bob wants to achieve ?

- No firmware stealing at production
- No over-production by manufacturer
- No mean to program other devices

- No firmware stealing in the field

- Detection of attacks in the field

The Security Functions needed by Bob

- Secure Manufacturing

- Software IP Protection
- Secure Install / Update
- Silicon Device Lifecycle

- Abnormal Situations Handling
- Audit/Log

STM32 Trust

Customer example (2/6)
Focus on Isolation and IP protection

Jon is at the head of a company selling firmware and receives royalty payments from customers.
The firmware developed by his team is very valuable to him. It features application options that can be further enabled by the user.

What Jon wants to achieve	The Security Functions needed by Jon
Isolate his firmware from customer one	Isolation Software IP Protection
Ensure that his firmware can independently be updated	Secure Install/Update
Set application macro-state in a way which cannot be altered	Application Lifecycle

Customer example (3/6)
Focus on Secure boot & Secure update

Mark sells costly equipment.
He wants to offer a firmware update service.
He wants his service to only update his equipment and would like to make sure only his firmware runs on his devices.

What Mark wants to achieve ?

- Ensure only his equipment is targeted
- Always known product state
- Ensure the update is handled with integrity and that authenticity checks are carried out
- Authenticity of firmware running on devices

The Security Functions needed by Mark

- Identification/Authentication/ Attestation
- Secure Install/Update
- Secure Boot

Customer example (4/6)
Focus on Secured communication

Oliver is selling devices that report sensitive data to a central server. Oliver needs to make sure the data cannot be exposed to people outside of his company and that it is protected.

What Oliver wants to achieve	The Security Functions needed by Oliver
• Ensure transmitted data is not exposed	• Crypto Engine
• Ensure secret on data encryption keys	• Secure storage
• Ensure data is sent from authenticated devices • Ensure data is sent to authenticated servers	• Identification/Authentication/ Attestation

STM32 Trust

Customer example (5/6)
Focus on Brand protection and Identification

Rose controls her fleet of devices from a remote server. She wants to be sure no counterfeiting or malicious devices are running with her server and would like to have full control over the devices. Rose needs to be able to check the identity and access rights of network operating devices at any time.

What Rose wants to achieve ?

- That every device shows a unique identity
- Be able to authenticate the device
- Be able to attest the device access rights

- Secure device communication

- Ensure that identities and access right secrets cannot be leaked even at the manufacturing stage

The Security Functions needed by Rose

- Identification/Authentication/ Attestation

- Crypto Engine

- Secure Storage and Secure Manufacturing (Secure Personalization)

STM32 Trust

Customer example (6/6)
Focus on data protection

Jack is collecting user data within his devices as part of a larger system.
Jack's devices and system needs to be in line with regulations (such as GDPR) to be able to promote and sell devices.

What Jack wants to achieve ?

- Ensure platform integrity
- Ensure user data is not exposed while communicating
- Ensure user data is stored securely

The Security Functions needed by Jack

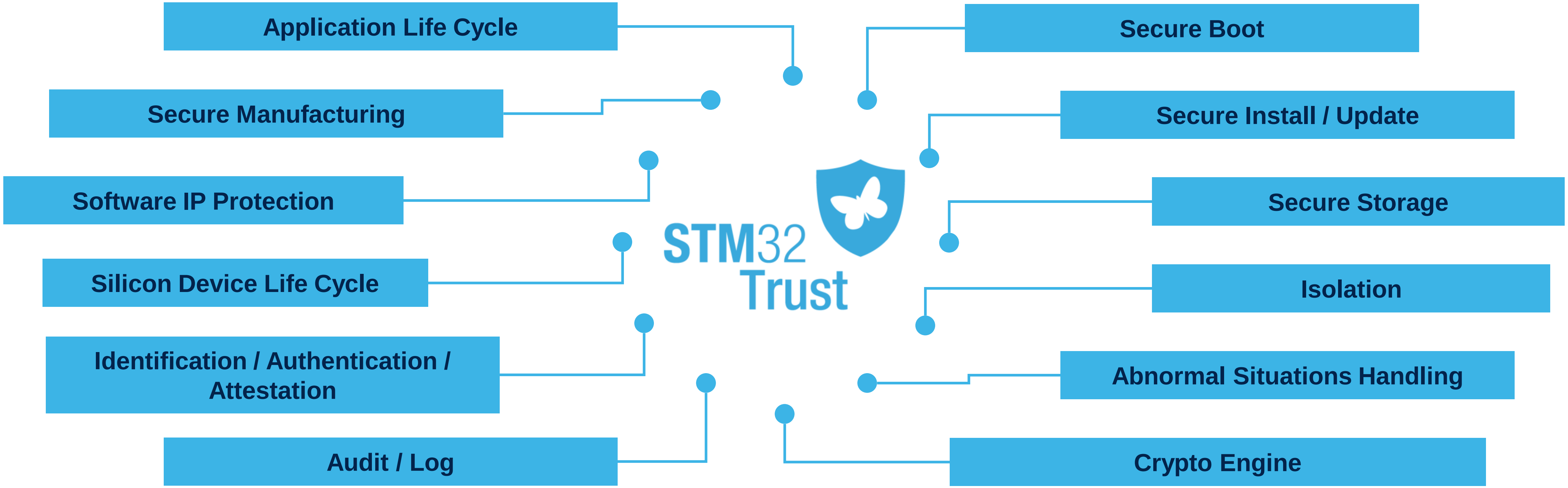
- Secure Boot
- Abnormal Situations Handling

- Crypto Engine
- Identification/Authentication/Attestation

- Secure Storage

The 12 security functions

- STM32Trust brings 12 Security Functions to align with Customer Use Cases and Security Standards
- STM32Trust brings assets (Documentation, Software, Tools…) to cover those 12 Security Functions



Application Life Cycle

Secure Manufacturing

Software IP Protection

Silicon Device Life Cycle

Identification / Authentication / Attestation

Audit / Log

Secure Boot

Secure Install / Update

Secure Storage

Isolation

Abnormal Situations Handling

Crypto Engine

STM32 Trust

The 12 security functions Summary of definitions

1- Secure Boot

Ability to ensure the authenticity and integrity of an application that is inside a device

2- Secure Install / Update

Installation or update of firmware with initial checks of integrity and authenticity before programming and executing

3- Secure Storage

Ability to securely store secrets like data or keys

4- Isolation

Isolation between trusted and non-trusted parts of an application

5- Abnormal Situations Handling

Ability to detect abnormal situations (both hardware and software) and to take adapted decisions like secrets removals

6- Crypto Engine

Ability to process cryptographic algorithms, as recommended by a security assurance level

7- Audit / Log

Keep trace of security events in an unchangeable way

8- Identification / Authentication / Attestation

Unique identification of a device and/or software, and ability to detect its authenticity, inside the device or externally

9- Silicon Device Lifecycle

Control states to securely protect silicon device assets through a constrained path

10- Software IP Protection

Ability to protect a section or the whole software against external or internal reading. Can be multi-tenant

11- Secure Manufacturing

Initial device provisioning in unsecured environment with overproduction control. Potential secured personalization

12- Application Lifecycle

Define unchangeable incremental states to securely protect application states and assets

life.augmented

STM32 Trust

Overview
Security functions versus STM32 & STSAFE

Security Function	STM32F4/F7/L1/WB/G0/G4/H7/L0/L4		STM32MP1		STM32L5 with TrustZone		+ STSAFE-A/TPM
	Silicon	Firmware	Silicon	Firmware	Silicon	Firmware	Silicon
Secure Boot	✓	✓ SBSFU	✓	✓ TF-A	✓	✓ TFM_SBSFU	✓
Secure Install/Update	✓		✓	✓ OPTEE	✓		✓
Secure Storage	✓ (L0/L4/H7/G0/G4)	✓ (WB) SBSFU KMS (L4)	✓	✓ OPTEE	✓	✓ TFM SPE	✓
Isolation	✓	🟦	✓	✓ OPTEE	✓	✓ TFM	✓
Abnormal situations handling	✓	🟦	✓	🟦	✓	🟦	
Crypto Engine	✓	✓ Crypto Libraries	✓	✓ OPTEE	✓	✓ Crypto Libraries TFM	✓
Audit/Log		🟦		🟦	✓	✓ TFM	
ID/Auth/Attestation	✓	🟦	✓	🟦	✓	✓ TFM Attestation	✓
Silicon Device LifeCycle	✓		✓		✓		
Software IP Protection	✓	🟦	✓	✓ OPTEE	✓	✓ TFM	
Secure Manufacturing	✓ SFI (H7/L4) with STM32HSM		✓ SSP with STM32HSM		✓ SFI with STM32HSM		✓
Application LifeCycle	✓	🟦	✓	🟦	✓	🟦	✓

🟦 Firmware to be developed by user
🟨 Reference firmware proposed by ST

life.augmented

Security functions and ST offer

STM32 Trust

1. Secure boot

STM32 Firmware / Tool Part Number	Benefit for Security Function	STM32 Series
X-CUBE-SBSFU	Example code implementing both a Secure Boot and a Secure Firmware Update mechanism	F4/F7/WB/G0/G4/H7/L0/L4
TFM_SBSFU Boot (Part of STM32CubeL5)	Example code implementing both a Secure Boot and a Secure Firmware Update mechanism	L5
TF-A (Part of OpenSTLinux)	First stage secure bootloader configuring STM32MP platform	MP1

STM32 Silicon Feature	Benefit for Security Function	STM32 Series
RDP (Read Protection)	Prevents a debugger from reading the secure boot	F4/F7/WB/G0/G4/H7/L0/L4/L5
WRP (Write Protection)	Prevents an application from altering the secure boot firmware	
MPU (Memory Protection Unit)	Ensures privileged access to some portion of application – task isolations	
MMU (Memory Management Unit)	Ensures privileged access to some portion of application – task isolations	MP1
UBE (Unique Boot Entry)	Ensures the silicon always boots at the secure boot location	G0/G4/L5
HDP (Hide Protect)	Temporal isolation ensuring secure boot is not seen after first execution	H7/G0/G4/L5
Secure Boot ROM code	Root of trust for loading first bootloader on STM32MP	MP1

STSAFE Feature	Benefit for Security Function
X509 certificate	Allow attest of executed firmware
One-way counter (decrement)	Supporting version control management using STSAFE-A

STM32 Trust

2. Secure install / update

STM32 Firmware / Tool Part Number	Benefit for Security Function	STM32 Series
X-CUBE-SBSFU	Example code implementing both a Secure Boot and a Secure Firmware Update mechanism	F4/F7/WB/G0/G4/H7/L0/L4
TFM_SBSFU Boot (Part of STM32CubeL5)	Example code implementing both a Secure Boot and a Secure Firmware Update mechanism	L5
OP-TEE (Part of OpenSTLinux)	Trusted Execution Environment for STM32MP, embedding trusted application installation/update	MP1

STM32 Silicon Feature	Benefit for Security Function	STM32 Series
RDP (Read Protection)	Prevents a debugger from reading the secure install/update	F4/F7/WB/G0/G4/H7/L0/L4/L5
MPU (Memory Protection Unit)	Ensures privileged access to secure install/update	
MMU (Memory Management Unit)	Ensures privileged access to secure install/update	MP1
UBE (Unique Boot Entry)	Ensures the silicon always boots at the secure install/update location	G0/G4/L5
HDP (Hide Protect)	Temporal isolation blocking access to secure install/update code after execution	H7/G0/G4/L5
Trustzone	Runtime isolation technology allowing 2 distinct worlds, secure and non-secure	L5/MP1
Secure FSBL (First Stage Boot Loader)	Secure Boot loader, loaded and authenticated by secure boot rom code	MP1

STSAFE Feature	Benefit for Security Function
X509 certificate	Attest new firmware authenticity
One-way counter (decrement)	Supporting version control management using STSAFE-A

3. Secure storage

STM32 Firmware / Tool Part Number	Benefit for Security Function	STM32 Series
X-CUBE-SBSFU	Example code implementing both a Secure Boot and a Secure Firmware Update mechanism. Specific version of STM32L4 includes a Key Management service, i.e. Secure Key Storage	L4
TFM (Part of STM32CubeL5)	Trusted Execution Environment over Cortex-M, featuring Secure Storage service	L5
OP-TEE (Part of OpenSTLinux)	Trusted Execution Environment for STM32MP, featuring Secure Storage service	MP1

STM32 Silicon Feature	Benefit for Security Function	STM32 Series
TrustZone	TrustZone is a complete set of hardware mechanisms to isolate two main security application domains: one trusted (ensuring the Secure Storage) and one non-trusted	L5/MP1
Firewall	Simple isolation in two domains for RAM and flash. Permits to isolate Secure storage firmware from application	L0/L4
AES Key Storage	Write-only key registers in AES engine	L5
OTFDEC (On The Fly Decryption)	Decryption of encrypted content stored on external flash	L5/H7
HDP (Hide Protect)	Temporal isolation ensuring keys stored there are not accessible afterwards	H7/G0/G4/L5

STSAFE Feature	Benefit for Security Function
Storage	Secured storage in secure element
Data packet encryption/decryption	Packets of data can be AES encrypted / decrypted with secret keys using STSAFE-A

4. Isolation

STM32 Firmware / Tool Part Number	Benefit for Security Function	STM32 Series
TFM (Part of STM32CubeL5)	Trusted Execution Environment over Cortex-M, adding further software handling for application portions sandboxing	L5
OP-TEE (Part of OpenSTLinux)	Trusted Execution Environment for STM32MP, adding further software handling for application portions sandboxing	MP1

STM32 Silicon Feature	Benefit for Security Function	STM32 Series
MMU (Memory Management Unit)	Ensures privileged access to some portion of application – task isolations	MP1
MPU (Memory Protection Unit)	Ensures privileged access to some portion of application – task isolations	F4/F7/WB/G0/G4/H7/L0/L4/L5
HDP (Hide Protect)	Temporal isolation ensuring a portion of code is not seen after first execution	H7/G0/G4/L5
TrustZone	Runtime isolation technology allowing 2 distinct worlds, secure and non-secure	L5/MP1
Firewall	Simple isolation in two domains for RAM and flash. Permits to isolate portion of an application from the rest	L0/L4
PcRoP (Proprietary code Read out Protection)	Ability to set some flash sectors as execute-only, thus preventing other sectors to read them	F4/L0/L4/H7/G0/G4
TZC (Trust Zone Controller)	Ability to isolate in particular Cortex-A cores from Cortex-M one	MP1

STSAFE Feature	Benefit for Security Function
Crypto Services	Crypto services isolated from STM32

5. Abnormal situations handling

STM32 Silicon Feature	Benefit for Security Function	STM32 Series
Anti tamper / Active tamper / Backup registers	Protect against a wide range of physical attacks on HW system outside the MCU. Erases backup registers information when tamper is detected	F4/F7/WB/G0/G4/H7/L0/L4/L5/MP1
RTC (Alarm timestamp)	Timestamp on tamper events, or internal events	
GPIO Locking	Lock of selected GPIO. Impossible to unlock until next reset. Ability to lock communication channels after tamper detection	
CSS (Clock Security System)	Internal clock available for secured program execution independently from external source clock	F4/F7/WB/G0/G4/H7/L0/L4/L5/MP1
ECC (Error Correction Code)	Robust memory integrity. Hardened protection against fault injection attacks thanks to error detection	
Temperature Sensor	Check if device is operating in expected temperature range. Hardened protection against temperature attacks	
Watchdogs	Independent watchdog and window watchdog for software timing control.	
PVD (Power Voltage Monitoring)	Monitors changes on power	

6. Crypto engine

STM32 Firmware / Tool Part Number	Benefit for Security Function	STM32 Series
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…)	All, except MP1
DPA Resistant Crypto Library* (FIPS-140)	DPA resistant version of Cryptographic library. Available on specific part numbers after on demand adaptation	L4*
TFM (Part of STM32CubeL5)	Trusted Execution Environment over Cortex-M, featuring Crypto algorithms	L5

STM32 Silicon Feature	Benefit for Security Function	STM32 Series
Symmetric Hardware Crypto Accelerators	Implements a given algorithm by hardware implementation, like AES for instance	F4/F7/WB/G0/G4/H7/L0/L4/L5/MP1
HASH	Hash algorithms implemented by hardware, like SHA	F4/F7/WB/G0/G4/H7/L0/L4/L5/MP1
PKA (Public Key Accelerator)	Asymmetric algorithms (Public key), implemented by hardware, for RSA/ECC/DH	WB/L5
OTFDEC (On The Fly Decryption)	Decryption of encrypted image on external flash	L5/H7
RNG (Random Number Generator)	True RNG done entirely by hardware	F4/F7/WB/G0/G4/H7/L0/L4/L5/MP1

STSAFE Feature	Benefit for Security Function
ECDH key pair generation and share secret generation	Assist device to establish TLS secure connections
RNG (Random Number Generator)	True RNG done entirely by hardware
Data packet encryption	AES encryption/decryption using hardware secret keys by the STSAFE-A

*: Contact your nearest sales office

7. Audit / Log

STM32 Firmware / Tool Part Number	Benefit for Security Function	STM32 Series
TFM (Part of STM32CubeL5)	Trusted Execution Environment over Cortex-M, featuring Audit/Log	L5
Customer can implement his software to handle this Security Function		All

STM32 Silicon Feature	Benefit for Security Function	STM32 Series
GTZC (Global TrustZone Controller)	Illegal access tracking and internal log/action	L5

8. Identification / authentication / attestation

STM32 Firmware / Tool Part Number	Benefit for Security Function	STM32 Series
TFM (Part of STM32CubeL5)	Trusted Execution Environment over Cortex-M, featuring Attestation	L5

STSAFE Service	Benefit for Security Function
STSAFE-A pre-personalization (MOQ 5K)	Pre-loading of customer secret in STSAFE-A at ST secure manufacturing site

STM32 Silicon Feature	Benefit for Security Function	STM32 Series
Device 96-bit Unique ID	Enables product traceability. Can be used for security key diversification	F4/F7/WB/G0/G4/H7/L0/L4/L5/MP1
Certificate (unique per chip)	Enables to authenticate a genuine STM32	H7/WB/L5/MP1
SSP (Secure Secret Provisioning)	Secure provisioning of OTP Secret values	MP1

STSAFE Feature	Benefit for Security Function
Device 7Byte Unique ID	Enables product traceability.
ECDSA signature/verification based authentication	Allow device identity verification
X509 certificate	Allow attest device access rights

9. Silicon device lifecycle

STM32 Firmware / Tool Part Number	Benefit for Security Function	STM32 Series
STM32CubeProgrammer	Software tool able to control the RDP cycle	All

STM32 Silicon Feature	Benefit for Security Function	STM32 Series
BSEC & BootRom	Device life cycle managed through OTP and BSEC	MP1
RDP (Read Protection)	Ability to gradually choose accessible / modifiable features (like ability to debug, or ability to access Flash content) depending on RDP level	F4/F7/WB/G0/G4/H7/L0/L4/L5
WRP (Write Protection)	Flash sector becomes not writeable anymore when write protected and RDP2 is set	
HDP (Hide Protect)	Temporal isolation	H7/G0/G4/L5
PcRoP (Proprietary code Read out Protection)	Ability to set some flash sectors as execute-only	F4/L0/L4/H7/G0/G4

10. Software IP protection

STM32 Firmware / Tool Part Number	Benefit for Security Function	STM32 Series
TFM (Part of STM32CubeL5)	Trusted Execution Environment over Cortex-M, adding further software handling for application portions sandboxing	L5
OP-TEE (Part of OpenSTLinux)	Trusted Execution Environment for STM32MP, adding further software handling for application portions sandboxing	MP1

STM32 Silicon Feature	Benefit for Security Function	STM32 Series
RDP (Read Protection)	Prevents the reading of a software stored in flash	F4/F7/WB/G0/G4/H7/L0/L4/L5
TrustZone	TrustZone is a complete set of hardware mechanisms to isolate two main security application domains: one trusted and one non-trusted. A software IP can be put in trusted area, becoming non-accessible from non-trusted one	L5/MP1
Firewall	Simple isolation in two domains for RAM and flash. Permits to protect a software IP	L0/L4
PcRoP (Proprietary code Read out Protection)	Ability to set some flash sectors as execute-only	F4/L0/L4/H7/G0/G4
MMU (Memory Management Unit)	Ensures privileged access to some portion of application – task isolations	MP1
MPU (Memory Protection Unit)	Ensures privileged access to some portion of application – task isolations	F4/F7/WB/G0/G4/H7/L0/L4/L5

11. Secure manufacturing

STM32 Firmware / Tool Part Number	Benefit for Security Function	STM32 Series
STM32HSM-V1 and V2	Hardware security module (HSM) used to secure the programming of STM32 products, and to avoid product counterfeiting at contract manufacturers' premises	STM32 series with SFI or SSP
STM32CubeProgrammer	Software tool able to program an HSM with encryption key and counter of permitted programming occurrences	NA
FastROM Programming Services	Pre-loading of customer software in STM32 done by ST manufacturing	All, except MP1

STSAFE Service	Benefit for Security Function
STSAFE-A pre-personalization (MoQ 5K)	Pre-loading of customer secret in STSAFE-A at ST secure manufacturing site

STM32 Silicon Feature	Benefit for Security Function	STM32 Series
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	H7/L4/L5
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	MP1

*: Special part numbers on demand. Contact nearest sales office

12. Application lifecycle

STM32 Firmware / Tool Part Number	Benefit for Security Function	STM32 Series
TFM (Part of STM32CubeL5)	Trusted Execution Environment over Cortex-M, featuring Secure Storage service. Application LifeCycle can be stored within such storage	L5
Customer can implement his software to handle this Security Function		All

STM32 Silicon Feature	Benefit for Security Function	STM32 Series
OTP (One Time Programmable) Memory	OTP zones where application credentials or life cycle state can be stored.	F4/F7/WB/G0/G4/H7/L0/L4/L5/MP1

STM32 Trust

Certifications

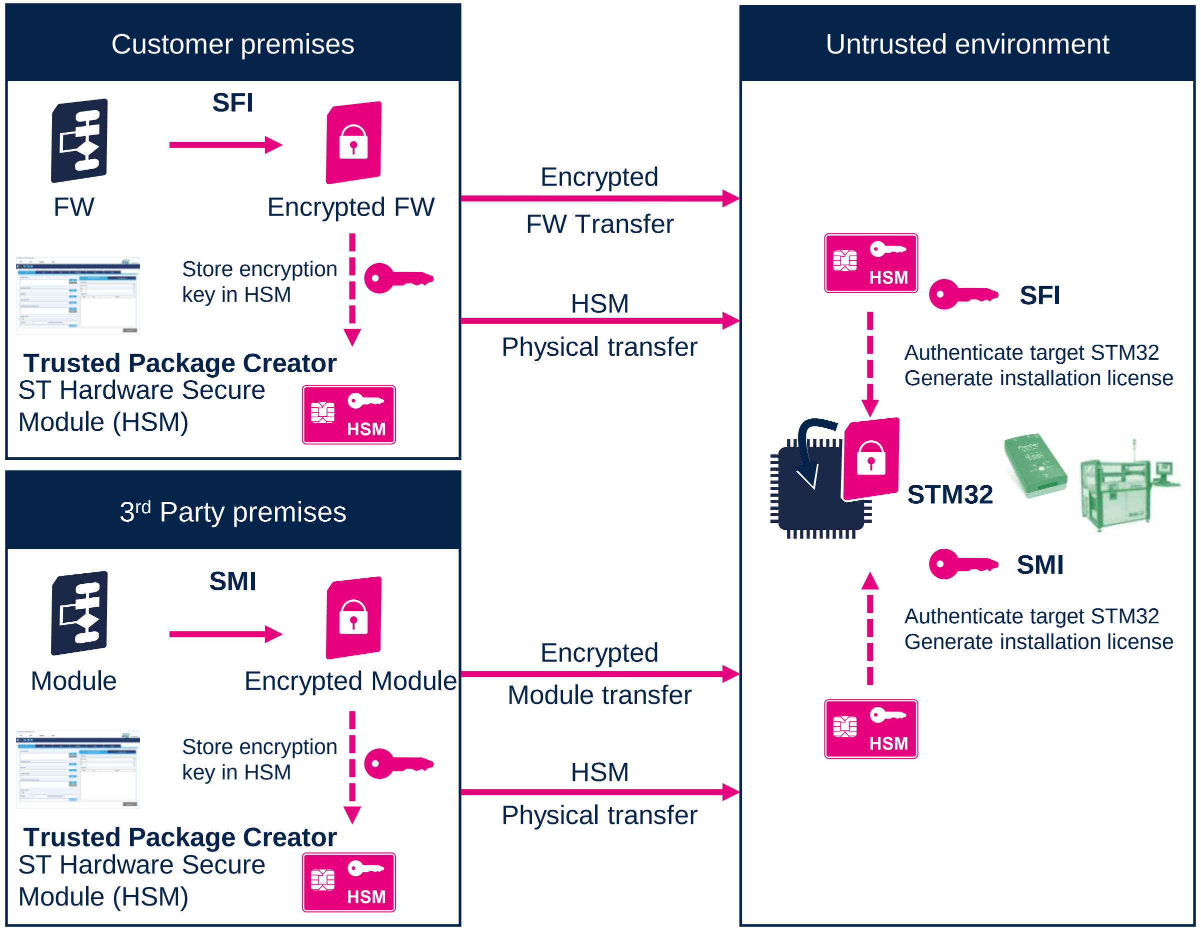
Certifications	Available Now	
ARM PSA - Level 1 (Self Assessment) - Level 2 (White box – Time Limited) - Level 3 (Smartcard-like)	ARM PSA Level 1 - STM32L4 - STM32L5	ARM PSA Level 2 - STM32L5 (TFM) ARM PSA API Compliant - STM32L5 (TFM)
SESIP **SESIP** - Level 1 (Self Assessment) - Level 2 (Black box) - Level 3 (White box – Time Limited) - Level 4 (White box) - Level 5 (Smartcard-like EAL4+)	SESIP Level 1 - STM32L4 (SBSFU)	SESIP Level 3 - STM32L4 (SBSFU)
Common Criteria **COMMON CRITERIA** - EAL5+ Smartcard	CC EAL5+ - STSAFE-A110 - STSAFE-TPM	
Evaluations	**Available Now**	
PCi **PCI POS** Point of Sale application	- STM32L4	

- Certification documents and links available at www.st.com/stm32trust
- Evaluations material is not public

life.augmented

Focus
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)
HSM
3rd Party premises
SMI
Module
Encrypted Module
Store encryption key in HSM
Trusted Package Creator
ST Hardware Secure Module (HSM)
HSM
Encrypted FW Transfer
HSM Physical transfer
Encrypted Module transfer
HSM Physical transfer
Untrusted environment
HSM
SFI
Authenticate target STM32
Generate installation license
STM32
SMI
Authenticate target STM32
Generate installation license
HSM

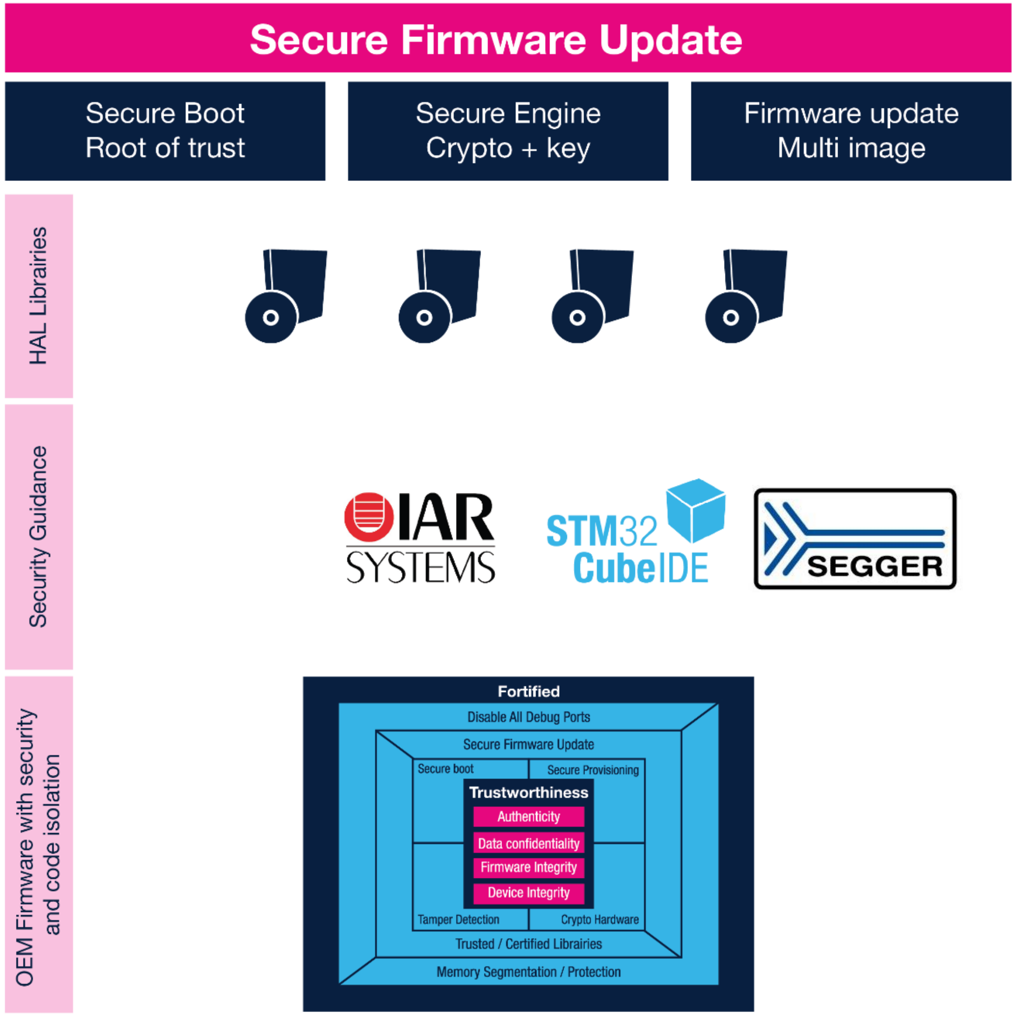
Secure Loader
embedded services provisioned by ST
➔ Mass Market approach

ST ecosystem
with
Encryption, HSM and programming tools

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

Protect 3rd party
Software IP
(SMI)

Focus
Secure boot secure FW update - SBSFU



Secure Firmware Update

Secure Boot Root of trust	Secure Engine Crypto + key	Firmware update Multi image

Reference library source code for In-application Programming

Demonstrate SW modules for:

- Secure Boot
- Secure Engine for Crypto and key
- Firmware Update image management

Ensure authentication and secure programing of in the field products

Reference implementation of STM32 hardware memory protections

Thank you

Up-to-date information available at www.st.com/stm32trust

life.augmented