STM32Trust

STM32 Trust

an embedded security framework

- Code Protection
- Execution Protection
- Ecosystem
- Partners

life.augmented

Code Protection

Ensure code confidentiality and integrity on authentic STM32 devices

Hardware features are embedded on certain STM32 MCU models for tamper detection and firewall code-isolation mechanisms. Arm® TrustZone® technologies are implemented to ensure IP protection

Services such as SFI and FastROM are available to ensure IP is protected in unsecure manufacturing locations

Part Number	X-CUBE-SBSFU	X-CUBE-CRYPTOLIB	SFI	STM32HSM-V1	FASTROM
STM32F4	✔	✔			✔
STM32F7	✔	✔			✔
STM32H7	✔	✔	✔	✔	✔
STM32G0	✔	✔			✔
STM32G4	✔	✔			✔
STM32L0	✔	✔			✔
STM32L1	✔	✔			✔
STM32L4	✔	✔	✔	✔	✔
STM32L5*	✔	✔			
STM32WB	✔	✔			✔

life.augmented

X-CUBE-SBSFU

Application code is most vulnerable when being transferred into boot memory or updated in the field

The X-CUBE-SBSFU Secure Boot and Secure Firmware Update is a set of software reference source code for secure firmware and upgrade of STM32 microcontroller built-in applications

The update process is performed in a secure way to prevent unauthorized updates and access to confidential on-device data

The X-CUBE-SBSFU shows how to set up all STM32 memory-protection mechanisms to isolate Secure Boot and Firmware Update functions from the main application

There is also a reference implementation of ST's secure element STSAFE, which maximizes the security level of the final application

Part Number	Status	Type	Category	Description
X-CUBE-SBSFU	ACTIVE	Embedded Software	MCU MPU Embedded Software	Secure boot & secure firmware update software

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

The X-CUBE-CRYPTOLIB is ready to use in all STM32 microcontrollers

- AES-128, AES-192, AES-256 bits:
  - ECB (Electronic Codebook Mode)
  - CBC (Cipher-Block Chaining with support for ciphertext stealing)
  - CTR (Counter Mode)
  - CFB (Cipher Feedback)
  - OFB (Output Feedback)
  - CCM (Counter with CBC-MAC)
  - GCM (Galois Counter Mode)
  - CMAC
  - KEY WRAP
  - XTS (XEX-based tweaked-codebook mode with ciphertext stealing)
- ARC4
- DES, TripleDES:
  - ECB (Electronic Codebook Mode)
  - CBC (Cipher-Block Chaining)
- HASH functions with HMAC support:
  - MD5
  - SHA-1
  - SHA-224
  - SHA-256
  - SHA-384
  - SHA-512
- ChaCha20
- Poly1305
- CHACHA20-POLY1305
- Random engine based on DRBG-AES-128
- RSA signature functions with PKCS#1v1.5
- RSA encryption/decryption functions with PKCS#1v1.5
- ECC (Elliptic Curve Cryptography):
- Key generation
- Scalar multiplication (the base for ECDH)
- ECDSA
- ED25519
- Curve25519

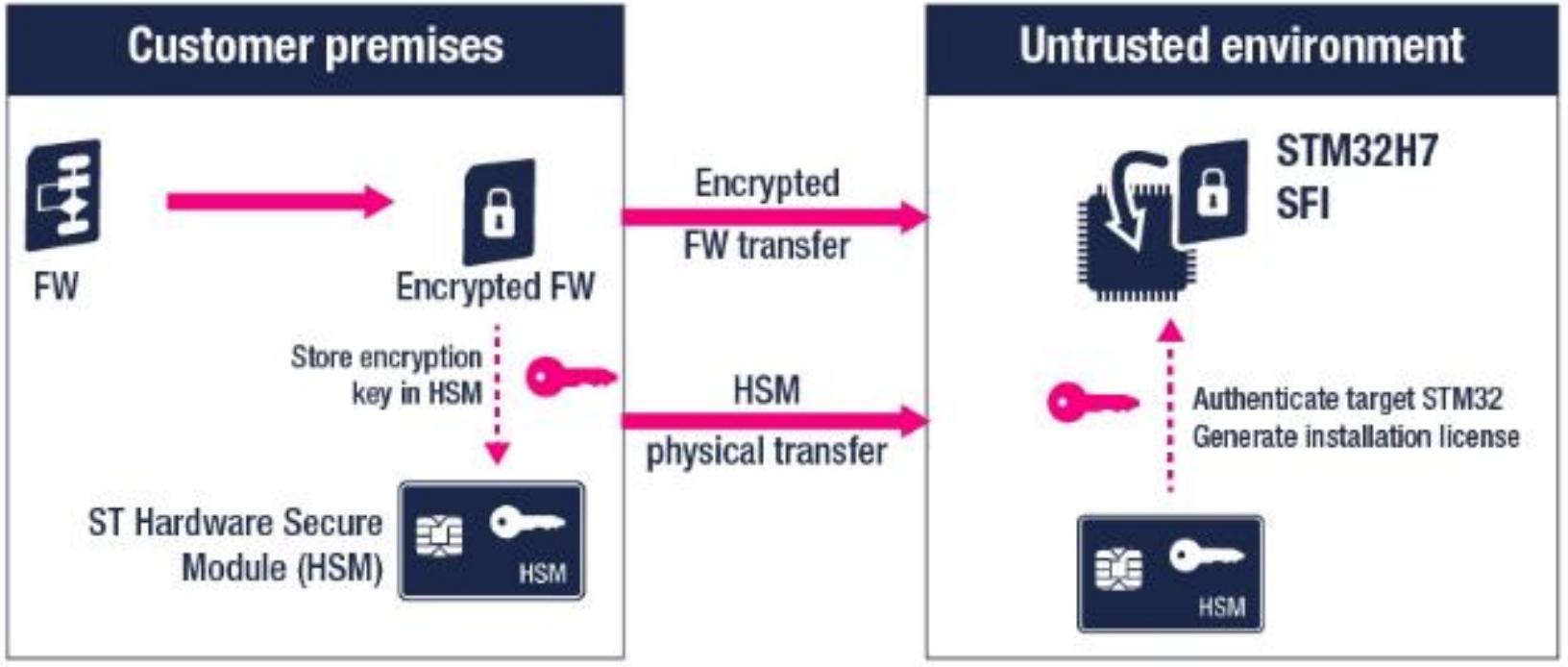
Part Number	Status	Type	Category	Description
X-CUBE-CRYPTOLIB	ACTIVE	Embedded Software	MCU MPU Embedded Software	STM32 cryptographic firmware library software

Secure Firmware Install (SFI)

The Secure Firmware Installation service provides protection when devices are being programmed for the first time

SFI is available on STM32L4 and STM32H7 series, soon to be extended to additional STM32 platforms

The solution offers a complete toolset to encrypt OEM binaries with the Trusted Package Creator software, the CUBE Programmer to securely flash the STM32 and the STM32HSM to transfer OEM credentials to the programming partner



life.augmented

FastROM

FASTROM (Factory Advanced Service Technique Read Only Memory) MCUs are Flash devices which are pre-programmed with the customer’s code and selected options

FASTROM MCUs improve programming efficiency for large quantities (10,000+) and compared to traditional ROM, have the advantage of shortening production leadtimes and allow devices to be reprogrammed

life.augmented

www.st.com/stm32trust

life.augmented

Execution Protection

Ensure code confidentiality, authenticity, isolation and execution with STM32 functions

Cyber security measures need to be set up to make sure firmware IPs are protected and credentials and data are secured by the application.

Execution Protection is a set of STM32 functions to ensure proper runtime isolation and execution of OEM code.

Part Number	Debug	Secure boot	MPU	Dual core	TrustZone	Firewall
STM32F4	✔	✔	✔			
STM32F7	✔	✔	✔			
STM32H7	✔	✔	✔			
STM32G0	✔	✔	✔			
STM32G4	✔	✔	✔			
STM32L0	✔	✔	✔			✔
STM32L1	✔	✔	✔			
STM32L4	✔	✔	✔			✔
STM32L5*	✔	✔	✔		✔	
STM32WB	✔	✔	✔	✔		

life.augmented

Execution Protection

Debug: The debug port provides access to all the device's resources from the outside. Used for application development, it is the first vulnerability breach to be accessed by the attacker on the device. STM32 debug function should be locked to ensure owner code confidentiality and authenticity.

Secure boot: Executed after each reset, the secure boot, as shown in the X-CUBE-SBSFU software package, checks the integrity of the STM32 platform configuration and verifies each embedded firmware signature for authentication.

MPU: The Memory Protection Unit mechanism protects different processes from each other and allows them to run independently. The resulting software isolation ensures that individual processes keep their code and data safe from each other. STM32 provides MPU solutions and is supported by several operating systems.

Execution Protection

Dual-core architecture: Dual-core architectures allow two runtime applications to run within the same device, both isolated by the core ID.

TrustZone: TrustZone is a complete set of hardware mechanisms to ensure the proper definition and isolation of two main security application domains: one so-called trusted domain (for critical applications with their affected resources) and one non-trusted domain for the main firmware application.

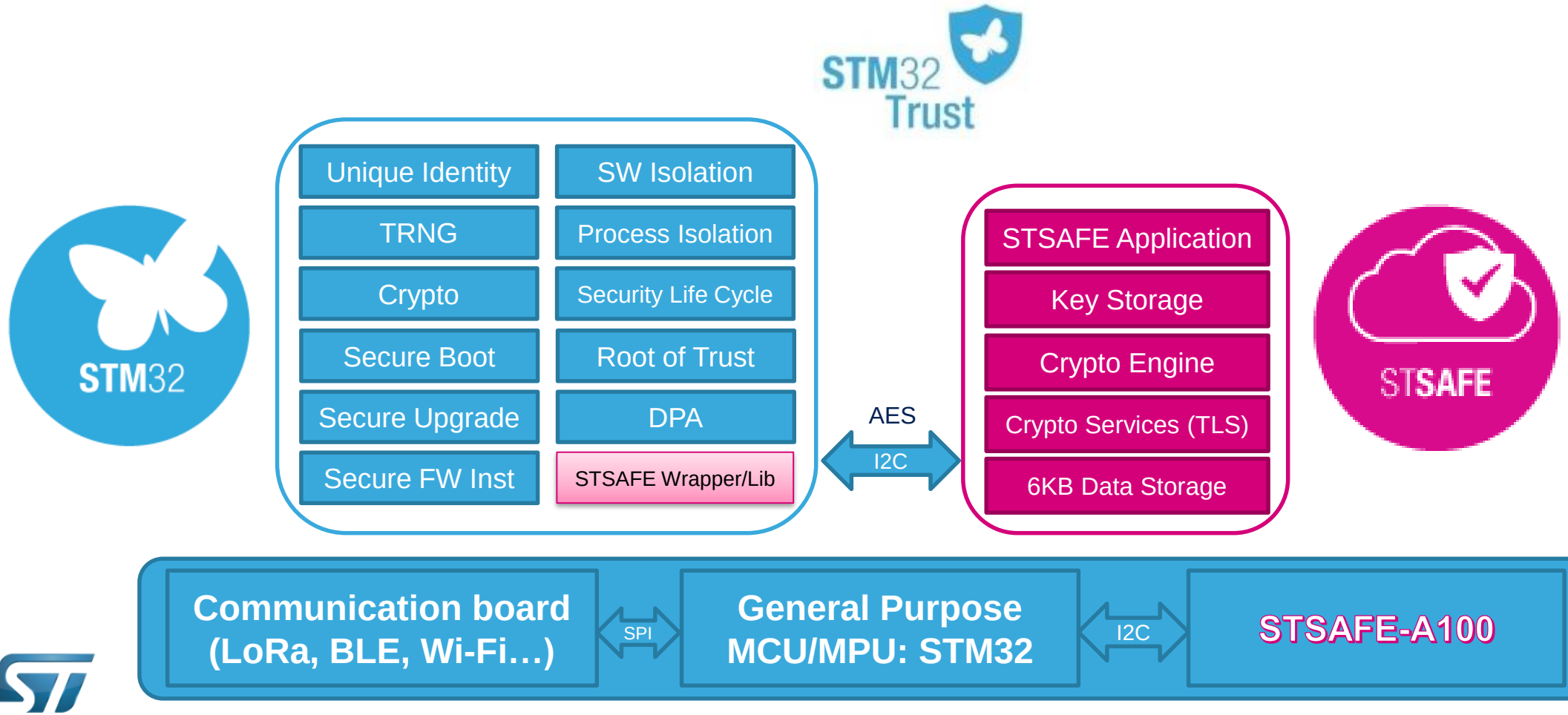
Firewall: The firewall is a hardware protection peripheral which controls the bus transactions and filters accesses to three particular areas: a code area (Flash), a volatile data area (SRAM), and a non-volatile data area (Flash). It allows users to simply set the critical code execution apart from the main application firmware.

www.st.com/stm32trust

life.augmented

Ecosystem

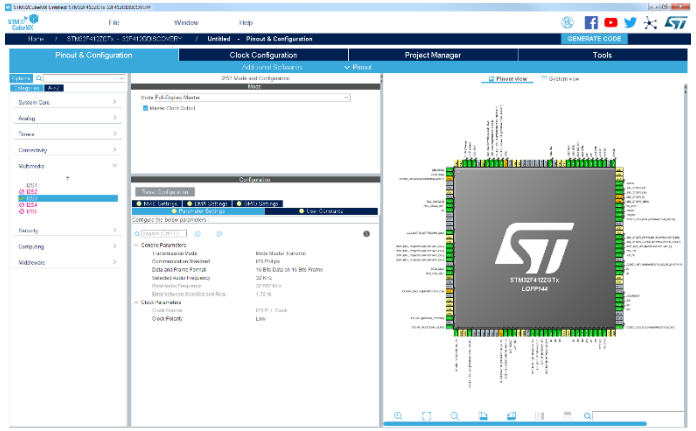
STM32Trust offers a complete framework for code and execution protection



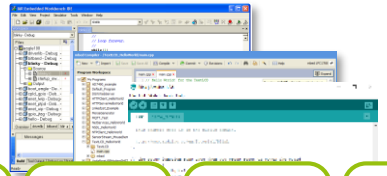
life.augmented

Ecosystem

STM32 CubeMX



STM32 CubeIDE

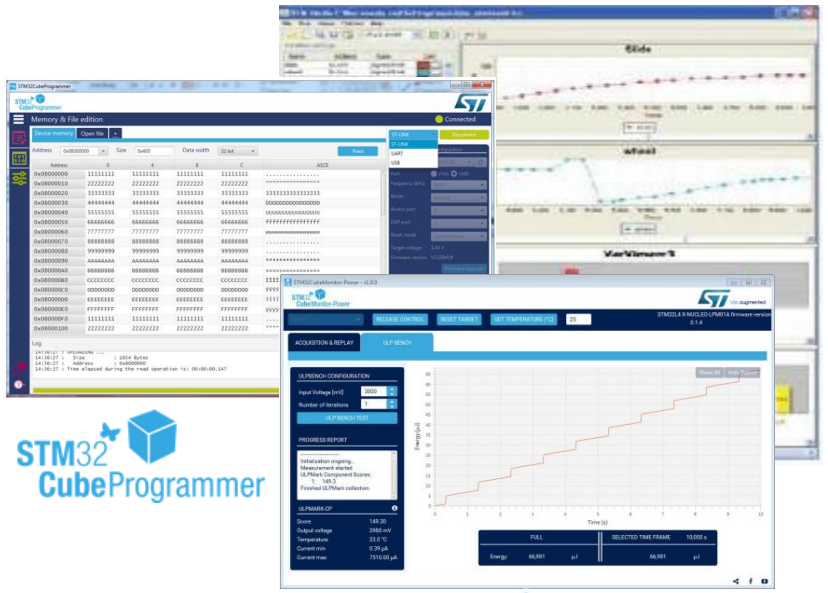


FREE IDE's

IAR SYSTEMS | arm KEIL | AC6 Assistance Conseil Systèmes | atollic | ARDUINO

arm MBED | TASKING AN ALTIUM BRAND | SEGGER | X

RAISONANCE | SysProGs | iSYSTEM | emPROG "Where Software Meets Hardware"



STM32 CubeProgrammer

STM32 CubeMonitor-Power

STM32CubeMX
Configure & Generate Code

IDEs
Compile and Debug

STM32CubeProgrammer
STM32CubeMonitor
Program & Monitor

life.augmented

Ecosystem

PRODUCT SPECIFICATIONS

00 Files selected for download

Description	Version	Size	Action
DB2641 Proprietary code read-out protection (PCROP), software expansion for STM32Cube	3.0.0	139 KB	PDF

APPLICATION NOTES

Description	Version	Size	Action
AN5056 Integration guide for the X-CUBE-SBSFU STM32Cube Expansion Package	3.0.0	3MB	PDF
AN5156 Introduction to STM32 microcontrollers security	2.0.0	3MB	PDF

USER MANUAL

Description	Version	Size	Action
UM2262 Getting started with the X-CUBE-SBSFU STM32Cube Expansion Package	4.0	2.8 MB	PDF
UM2237 STM32CubeProgrammer software description	7.0	3.2 MB	PDF
UM2238 STM2 Trusted Package Creator tool software description	3.0	1.7 MB	PDF

Ecosystem

Trainings

STM32L4 Security Firewall		PDF
STM32L4 Security Advanced Encryption Standard (AES) HW accelerator		PDF
STM32L4 peripheral HASH		PDF
STM32L4 Security memories protections		PDF
STM32L4 Security Random Number Generator (RNG)		PDF
STM32L4 Real Time Clock		PDF

X-CUBE-PCROP firmware

Proprietary code read-out protection (PCROP) software expansion for STM32Cube (AN4701, AN4758 and AN4968)

STM32 online training about “Security & Safety

Full range of STM32 training courses (STM32G4, STM32F7, STM32L4, STM32L4+, STM32G0, STM32WB, STM32H7 and STM32MP1) available on line

STM32 MOOC - Basics of security in STM32

STM32 security basics MOOC with hands-on exercises

www.st.com/stm32trust

life.augmented

Partners

Work with STM32Trust and our trusted partners

Segger

Prove & run

Express Logic

Wolf SSL

Cypherbridge

Electric imp

ClevX

Mocana

Kudelski Group

life.augmented

YouTransactor

Fast track to design your POS terminal

Secure PCI Chip

- Patented microcontroller
- STM32L4 architecture
- Adjust key Chip parameters

- PCI PTS Secure Core
  (PIN entry, Key storage, Right Management)

STM32LP452

PCI/EMV Module

- Fit in any Hardware
- Fast track integration
- Module PCI/EMV ready

- Communication chip
- Contact Card Reader
- Payment Application
  (SRED, Display, PIN…)

uCube Core

EMV / PCI ready

Pre-Certifications:
- PCI PTS 5.x
- EMV L1/L2 contactless

Certifications:
- EMV L1/L2 contact

Ultimate Security

- Crypto Libraries
- Application Loader
- Secure Boot
- Hardware & Software Tamper
- RTC – Real Time clock integrity

Key Benefits

- Low cost - no need to buy an expensive chip
- Long component availability
- Fraud attempts stopped in few microseconds
- Possibility to have a POS reference design

life.augmented

YouTransactor

Mobility

- Transportations (Ticket, Fines, Control)
- Events & Hospitality
- Street Merchants
- Professionals in Mobility

Retail & Shops

- Sales staff in Shops
- Cashier and POS solutions
- Instant Payment

Payment reinvented

- ✓ EMV L1/L2 Contact & Contactless
- ✓ PCI 5.x certified
- ✓ Bluetooth, WIFI, 2G/4G
- ✓ Android / iOS SDK
- ✓ QR code display
- ✓ Chip & PIN acceptance

life.augmented

ClevX

Hardware Solutions for Portable Data Storage

- Award-winning DataLock® Secured and FoldIT® USB drives.
- Easy to use hardware encrypted solutions.
- Remote Management available.
- OS-agnostic, self-encrypting, self-authenticating, bootable secure drives. FIPS 140-2 Level 3 Certified.
- Implemented for various types of external data storage devices (Flash, HDD, SSD).

Keypad-access hardware encrypted portable drives

Phone-access hardware encrypted portable drives

The world's thinnest USB drive. Fun and Practical

Software Solutions for Portable Data Storage

- Easy to use and deploy.
- Portable – no host Installation required.
- Designed for all external data storage devices (Flash, HDD, SSD).
- Visual user interface with OEM / rebranding options.
- Remote license management. A license is tied to the unique hardware ID of the drive.

Protect your USB drives with EncryptUSB

Back up your USB drive to a cloud with USBtoCloud

Keep your USB drives free of viruses with DriveSecurity

life.augmented

SecureData

SecureDrive® KP

SecureUSB® KP

SecureDrive® BT

life.augmented

www.st.com/stm32trust

life.augmented