STM32Trust
An ecosystem for embedded security

Secure Boot, Update, and Install under one roof

The STM32Trust ecosystem combines knowledge, design tools, and ready-to-use original ST software to build strong cyber-protection into new IoT devices, leveraging industry best-practices. These help designers take advantage of features built into STM32 microcontrollers to ensure trust among devices, prevent unauthorized access, and resist side-channel attacks to avert data theft and code modification.

STM32Trust integrates all available cyber-protection resources including reference material and free software for the STM32 family and offers a robust multi-level strategy to enhance security.

The STM32Trust solution offers a complete toolset for code and execution protection.

CODE PROTECTION

STM32Trust.CodeProtection includes a set of solutions to ensure owner code confidentiality and integrity programming on authentic STM32 devices.

Hardware cyber-protection features are already embedded on certain STM32 MCU models. Tamper detection, firewall code-isolation mechanisms and Arm TrustZone® technologies are also implemented to ensure the most sensitive codes benefit from extra protection.

EXECUTION PROTECTION

Devices become targets of cyberattacks when they are commercially implemented and need to be immune to these attacks. Cyber security measures need to be set up to make sure that firmware IPs are protected and that credentials and data are secured by the application and cannot be breached.

STM32Trust.ExecutionProtection is a set of STM32 functions to ensure owner code proper runtime isolation, execution and ease, and which achieves confidentiality and authenticity in the collected data. STM32 offers different architectures and isolation schemes.

Code Protection

- X-CUBE-SBSFU software library
- X-CUBE-CRYPTOLIB
- Secure Firmware Install solution
- STM32CubeProgrammer
- STM32HSM-V1
- FASTROM programming services

STM32 Trust

Execution protection

- Debug
- Secure boot
- Memory Protection Unit
- Dual core
- TrustZone
- Firewall

	CODE PROTECTION					EXECUTION PROTECTION					
Part Number	X-CUBE-SBSFU	X-CUBE-CRYPTO LIB	SFI	STM32 HSM-V1	FASTROM	DEBUG	SECURE BOOT	MPU	DUAL CORE	TRUST ZONE	FIRE WALL
STM32F4	√	√			√	√	√	√			
STM32F7	√	√			√	√	√	√			
STM32H7	√	√	√	√	√	√	√	√			
STM32G0	√	√			√	√	√	√			
STM32G4	√	√			√	√	√	√			
STM32L0	√	√			√	√	√	√			√
STM32L1	√	√			√	√	√	√			
STM32L4	√	√	√	√	√	√	√	√			√
STM32L5*	√	√				√	√	√		√	
STM32WB	√	√			√	√	√	√	√		

*available in Q4 2019

To discover this complete toolset, please visit www.st.com/stm32trust

ST COMMUNITY

Ask, learn, share, discuss, become famous and engage with the community of STM32 enthusiasts on community.st.com/stm32

© STMicroelectronics - August 2019 - All rights reserved
The STMicroelectronics corporate logo is a registered trademark of the STMicroelectronics group of companies
All other names are the property of their respective owners

life.augmented