STM32L5 MCU series

Excellence in ultra-low-power with more security

Colin Ramrattan
Microcontroller Marketing Americas

life.augmented

Technology Tour 2019
Toronto, Canada | May 29

IoT Security

- **Security**
  - Is a requirement **NOT** a nice to have
  - Can be and should be implemented now and not later
  - Money, Money, Money, this means either losing it now from security breaches or later from customers not purchasing your solution due to security concerns

- **Available Today**
  - PSA Certification of a device
  - Software package examples to build your application from
  - Reference Designs from ST Microelectronics

life.augmented

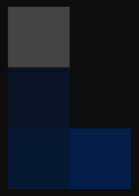
STM32 L5

IoT Security

The Cost of Security Inaction is Significant

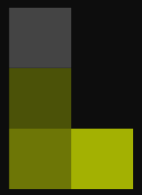
>300%

Increase in malware loaded onto IoT devices[2]



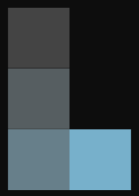
29%

Increase in industrial control system vulnerabilities[1]



600%

Increase in IoT device attacks[1]



$6 trillion

Cost of damage related to cybercrime by 2021[3]

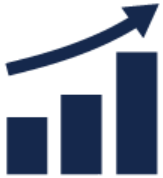
life.augmented

- 1 – Symantec Internet Security Threat Report 2018
  2 – Kaspersky Labs, New Trends in the World of IoT Threats 2018
  3 – Annual Cyber Crime Report, Cyber Security Ventures 2019

Main Concerns for Embedded Design

- **Security**
  - Protection from hackers

- **Low power consumption**
  - Long life time, small battery size



- **Integration, size, performance**
  - Best fit versus the application requirements

life.augmented

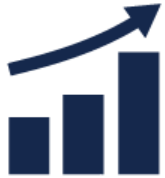
First STM32 Based on Cortex-M33

STM32L5 is the answer

- More security with TrustZone and ST security implementation
  - **HW to resist to Logical and board level attack**

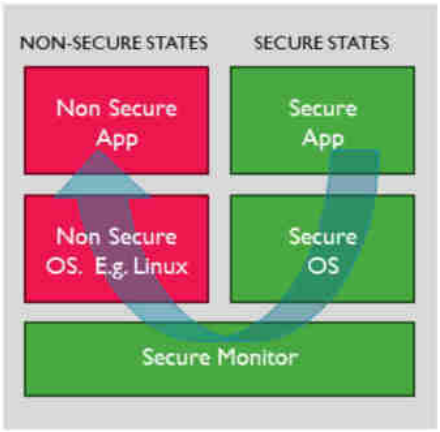
- Lower Power consumption
  - **STM32 ultra-low-power technology**

- Integration, Size, performance
  - **More performance, high memory size and wide portfolio**

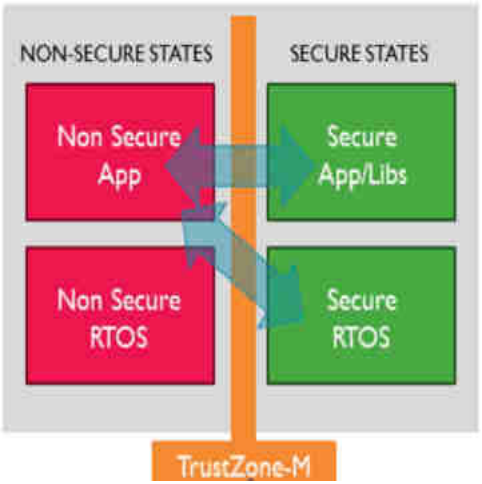


life.augmented

TrustZone-M versus TrustZone(-A)



Cortex A



- Conceptually TrustZone for ARMv8-M is similar to the TrustZone technology found in ARM Cortex-A Processors.
- Operations of TrustZone for ARMv8-M are however very different as they are optimized for embedded systems that requires real-time responsiveness

Security: Type of Attacks

- **Logical attack**
  - Malicious code injection
  - Malware replacing genuine program
  - Man-in-the-middle attack

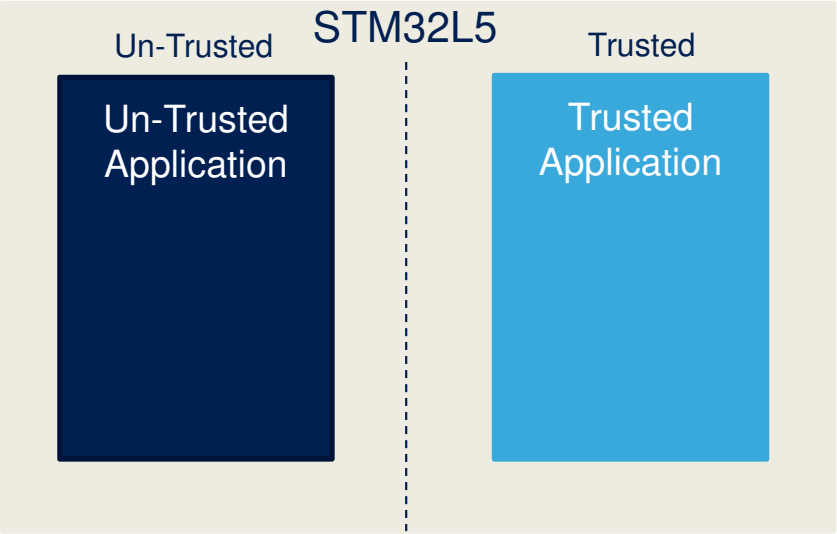
- **Board level attack**
  - Cloning attack
  - Fault injection
  - Side channel attack

Features to combat attacks

- **Hardware Isolation**
- **Secure Key storage**
- **Encryption**
- **Authentication**
- **IP Protection**
- **Read-out Protection**
- **Active tampering**
- **Certified Crypto library**

Security: TrustZone for Isolation

ST implementation provides high granularity of isolation

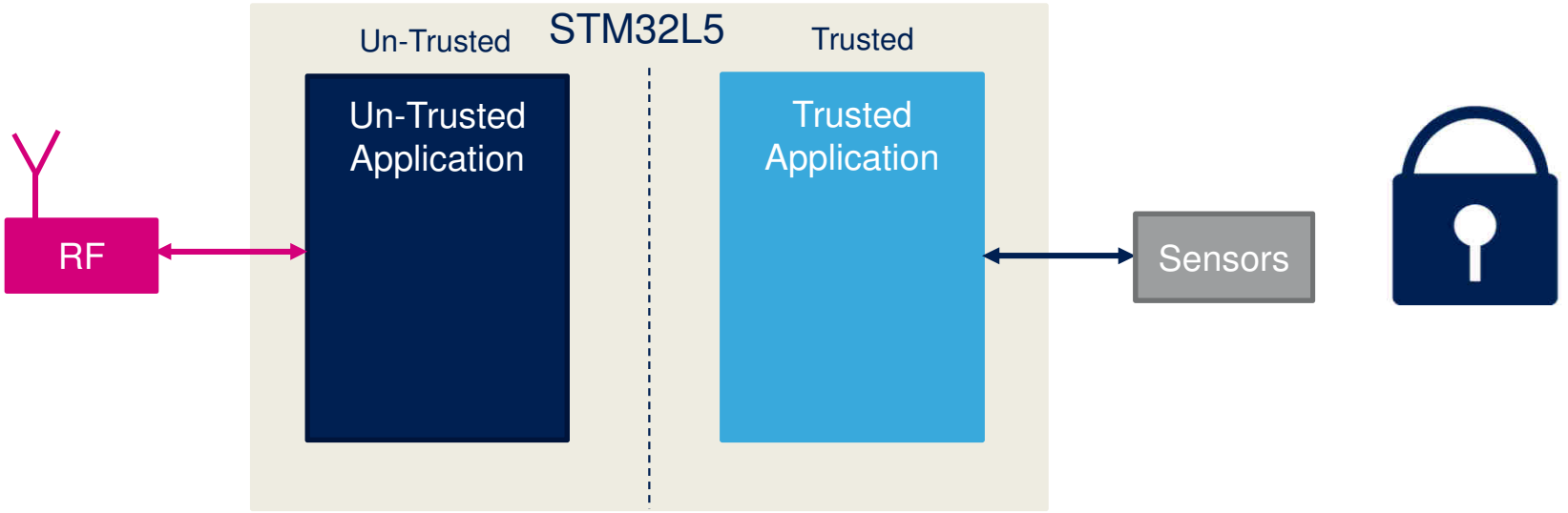


- **Each** GPIO or peripheral, DMA channel, clock configuration register, ART or small part of Flash or SRAM can be configured as **Trusted or un-Trusted**
- **ST** is the **ONLY** manufacturer to implement this high-granularity in TZ.
- **Full isolation** of trusted and non-trusted world

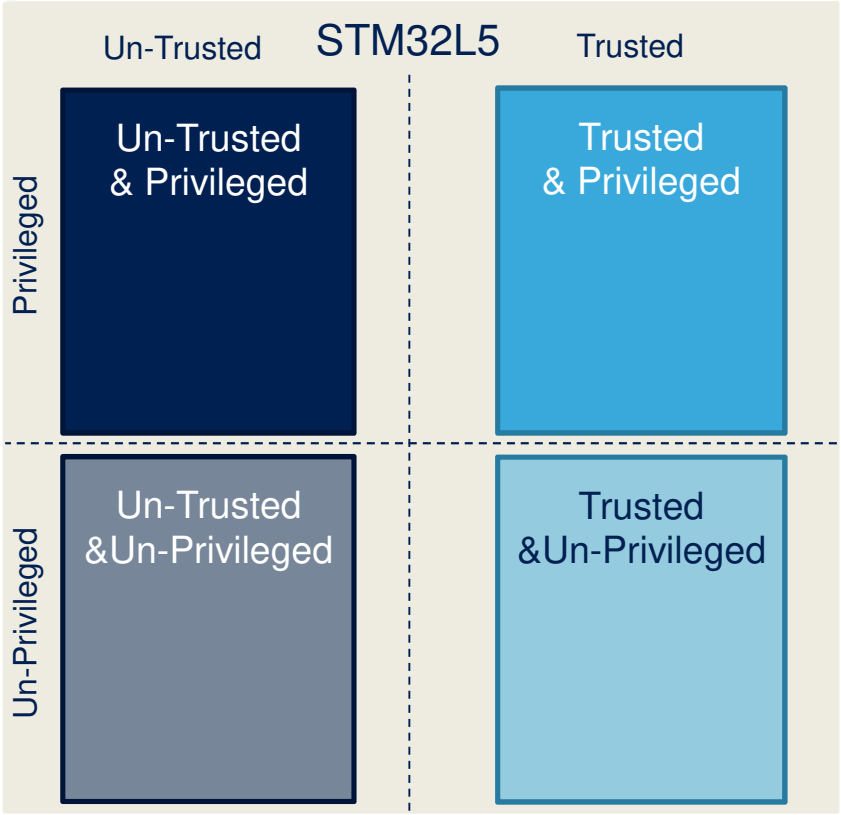
Security: TrustZone for Isolation

TrustZone provides full isolation

Example of IoT application implementation

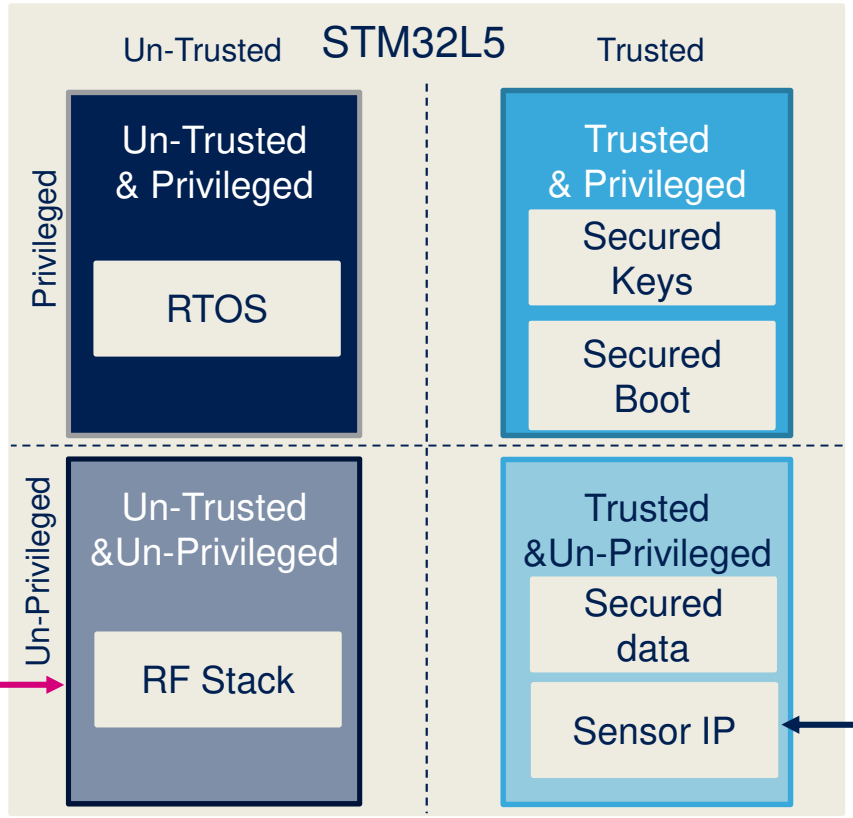


Security: TrustZone and Privileged



- More partitioning
- Possibility to separate the trusted and un-trusted area with **privileged and un-privileged** zone
- Strong **granularity** to define each part of memory or each peripheral, DMA channel as privileged or un-privileged

TrustZone: Example



A Full Set of Security

ENCRYPTION
DECRYPTION
AUTHENTIFICATION

- AES-128/256 Encryption
- SHA-256 Authentication
- **Public Key Acceleration (PKA): for RSA, Diffie-Hellmann or ECC (Elliptic Curve Cryptography)**
- Certified Crypto library
- True Random Number Generator
- Unique ID
- OTP Zone

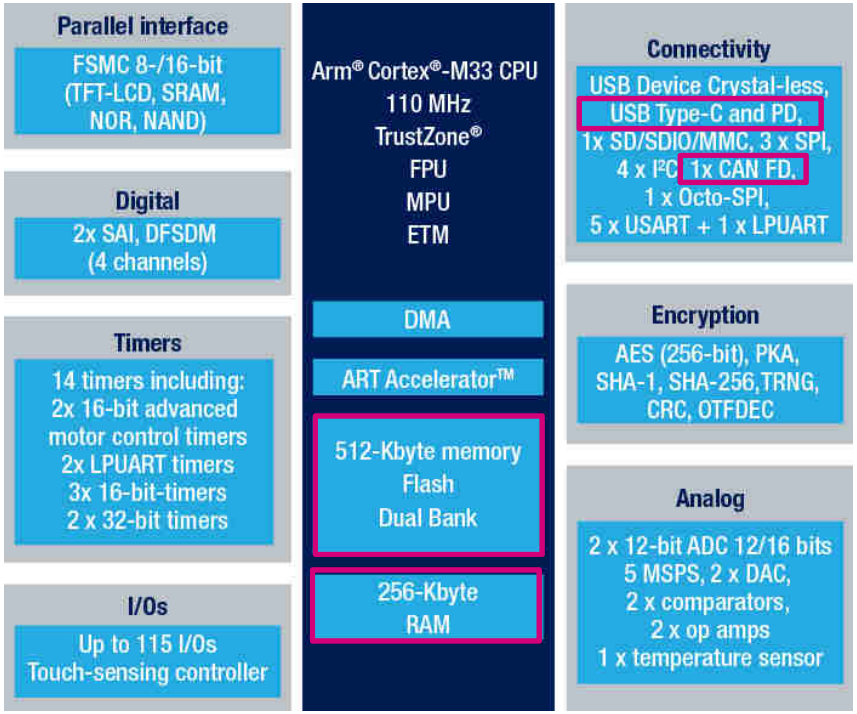
MEMORY and IP PROTECTION

- **Active and static Anti-tamper detection**
- Memory Protection Unit (MPU)
- Secure Boot
- Read and Write Protection
- **HDP (Hide Protect)**
- **OTFDEC (On-the-fly decryption) on Octo SPI to protect external memory**
- JTAG fuse
- **TrustZone**
- **Unique Boot Entry**

life.augmented

High Integration and Innovation

Large memory, USB Type-C™ w/ power delivery controller, CAN FD

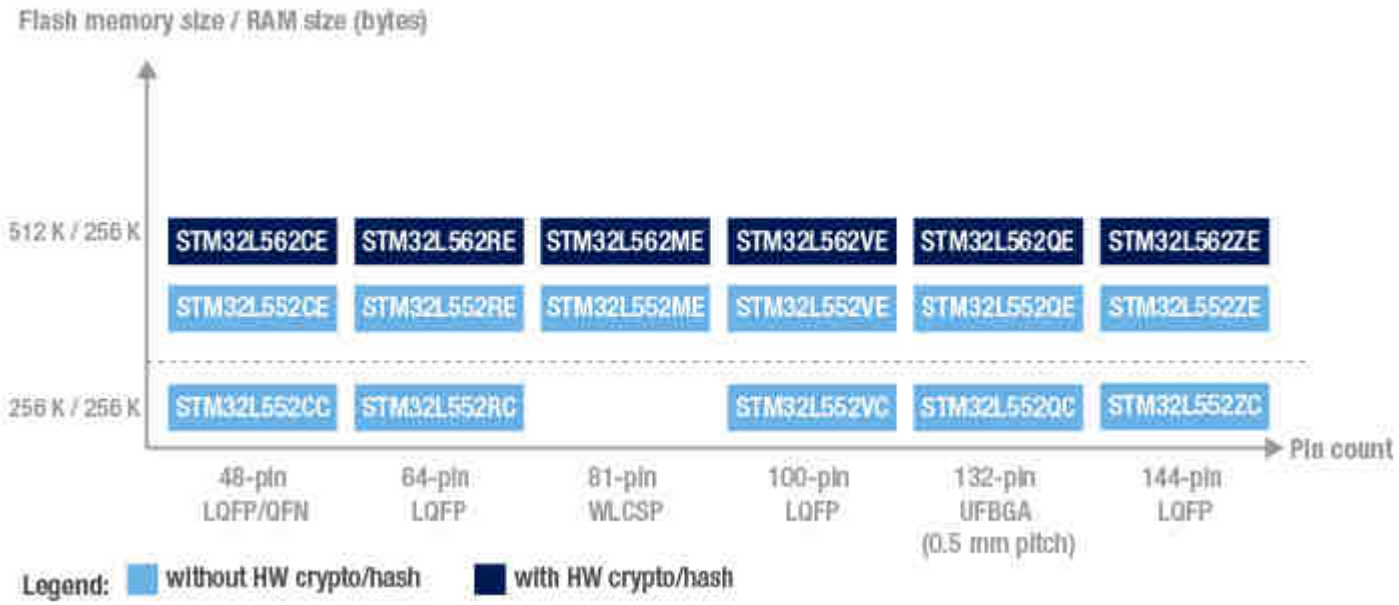


STM32 L5

life.augmented

Large Portfolio

7 packages, several options



Extend the Battery Life Time

- STM32L5 reuses the STM32L4/L4+ technology achieving **best-in-class** power consumption
- STM32L5 integrates an optional **SMPS** (DC/DC buck voltage regulator) which can be enabled/disabled on the fly to optimize the energy.
- Proven by EEMBC test results:
  - ULPBENCH™ An EEMBC Benchmark **402 ULPMark-CP**
  - ULPBENCH™ An EEMBC Benchmark **59.5 ULPMark-PP**

Ultra-low-power Modes

Best power consumption numbers with full flexibility

Wake-up time			
	V_{BAT}	3 nA / 225 nA*	Tamper detection: 3 I/Os, RTC
250 µs	Shutdown	33 nA / 300 nA*	Wake-up sources: reset pin, 5 I/Os, RTC
14 µs	Standby	110 nA / 385 nA*	Wake-up sources: + BOR, IWDG
14 µs	Standby + 4-Kbyte RAM	190 nA / 465 nA*	
5 µs	Stop 2 (full retention: 256-Kbyte RAM)	3.3 µA / 3.6 µA*	Wake-up sources: + all I/Os, PVD, COMPs, I²C, LPUART, LPTIM
6 cycles	Sleep	38 µA / MHz	Wake-up sources: any interrupt or event
	Run up to 110 MHz	Down to 60 µA / MHz	

Note : * without RTC / with RTC

More Performance

Better responsiveness of the application

- **New** Arm® Cortex®-M33 performance: **+20%** versus Cortex-M4

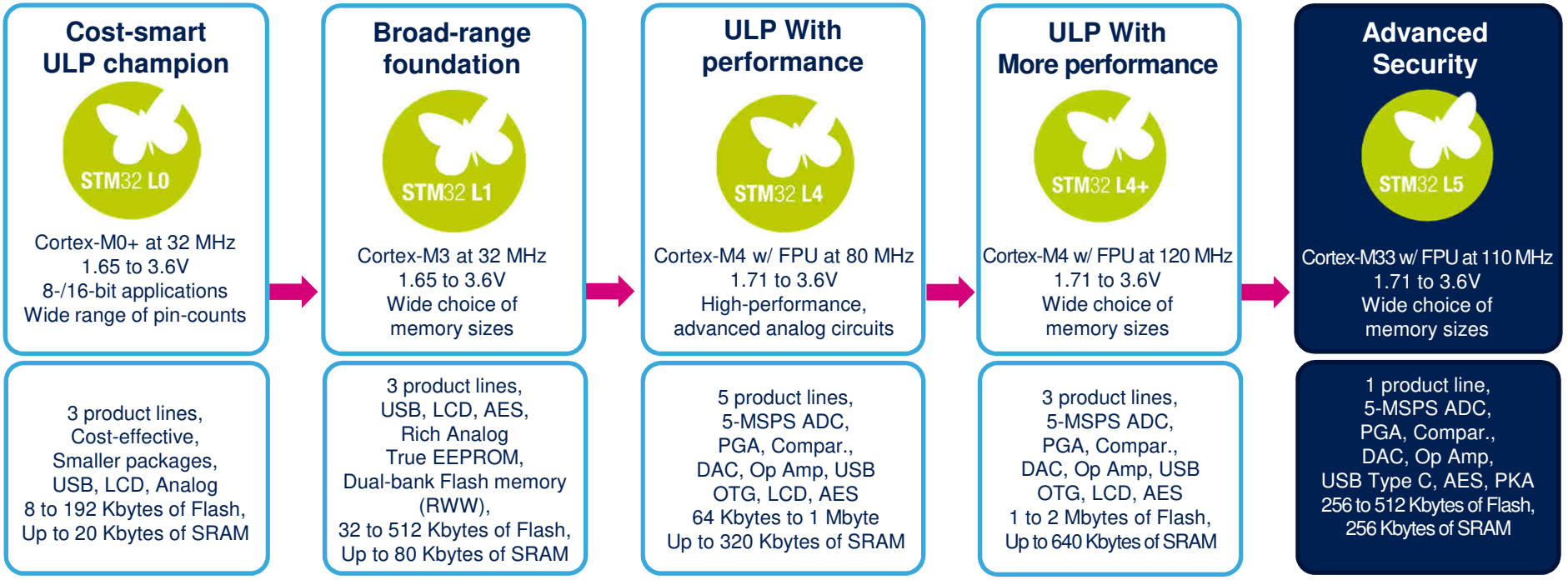
1.5 DMIPS/MHz 3.88 CoreMark/MHz	→	165 DMIPS 427 CoreMark

- **New** ST ART Accelerator™: working both on internal and **external** Flash
  - 8 Kbytes of instruction cache
- **STM32L5 Outperforms Competition**
  - With onboard flash and caching schemes, the STM32L5 can outperform other similar competitor devices.

life.augmented

STM32L ULP Portfolio

STM32L5 completes the ultra-low-power subclass

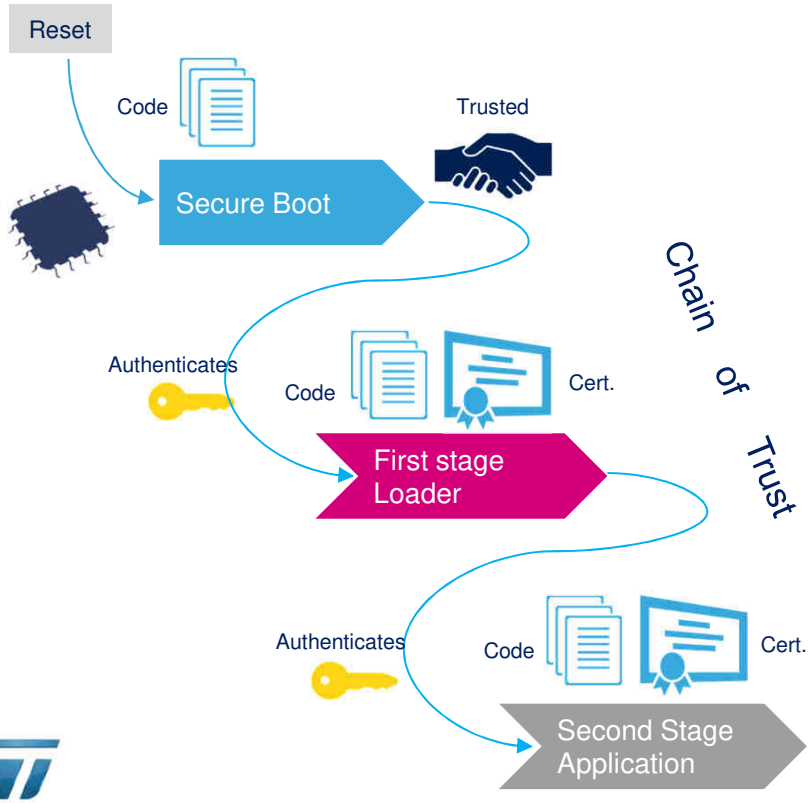


life.augmented

Secure Boot Secure Firmware Upgrade

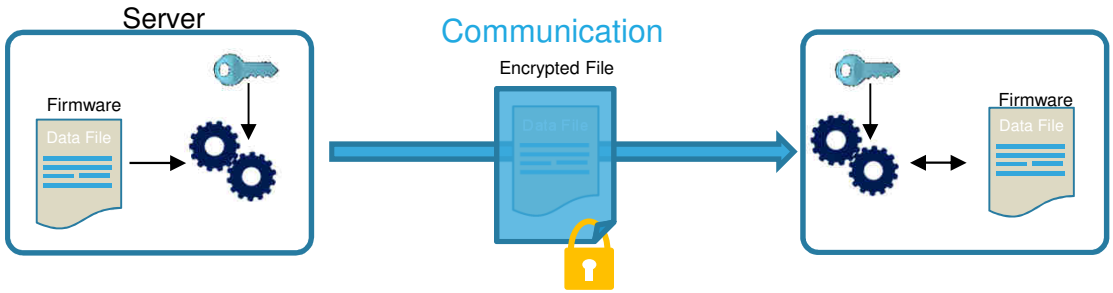
- Problem: How can I be sure only my code/firmware is used during boot, or when updating
  - Protection against malicious firmware installations during boot or updating
  - Prevent unauthorized updates
- Answer: **STM32 Secure Boot and Secure Firmware Update (SBSFU)**
  - Root of Trust Service
  - Immutable code
  - Application authentication before execution
  - Firmware version management
  - Error management for image rollback and anti-rollback
  - HOW
    - Utilize HW Anti-Tamper in STM32 (RDP, WRP, MPU, Anti-Tamper, DAP, IWDG)
    - X-CUBE-SBSFU – STM32Cube software expansion

Secure Boot



- At RESET, verify platform integrity
- Start secure boot from trusted immutable code
- All components are authenticated and integrity verified
- Next stage code is executed ONLY when components are authenticated and verified

Secure Firmware Update



- A new encrypted firmware image is created and stored in the server
- New firmware image is sent through an untrusted channel
- Server is authenticated, new firmware image is downloaded, checked and installed

STM32 SBSFU Strategy

STM32 Code Execution
Single Entry Point

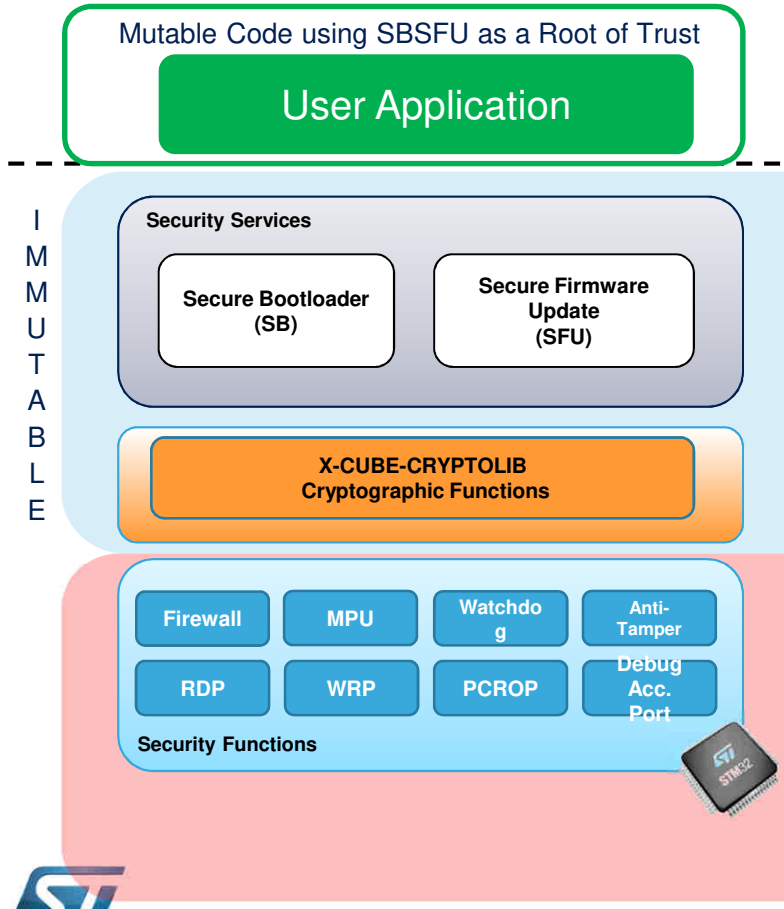
SBSFU Code is
Secret and Immutable

STM32 Protected Enclave

STM32 Debug Lock

STM32 System Monitoring

SBSFU Architecture



- Secure Boot and Secure Firmware Update
  - Using Security Features offering multiple layers of protection
- Cryptographic Functions
  - Ensures Confidentiality, Integrity and Authenticity
- STM32 Security Functions
  - Used to establish a robust platform on which trusted processes and associated cryptography can be performed

life.augmented

X-CUBE-SBSFU Features Overview

- Secure Boot (SB) module
  - Execution with Root of Trust service (STM32 Security Functions)
  - Application authentication and Integrity check before execution
- Secure firmware Update (SFU) module
  - Detect new FW version to install
    - From local download service
    - Pre-downloaded OTA via User application from previous execution…
  - Manage FW version (check unauthorized updates or unauthorized installation)
  - Secure FW upgrade:
    - FW Authentication, integrity check, decryption and installation.
  - In case of any error occurring during new image installation rollback to the previous valid version
  - Execute new installed FW (once Authenticated and integrity checked)

- STSAFE (Secure Element) module
  - Code isolated from main Firmware → Secure execution
  - Dedicated HW crypto accelerator
  - Manage secure key storage
  - Manage secure user data

X-CUBE-SBSFU Features Overview

- X-CUBE-SBSFU is provided as **reference code to demonstrate state-of-the-art usage of the STM32 security protection mechanisms**.
- It is a **starting point** for OEMs to develop their own Secure Boot and Secure Firmware Update applications as a function of their product security requirement levels.

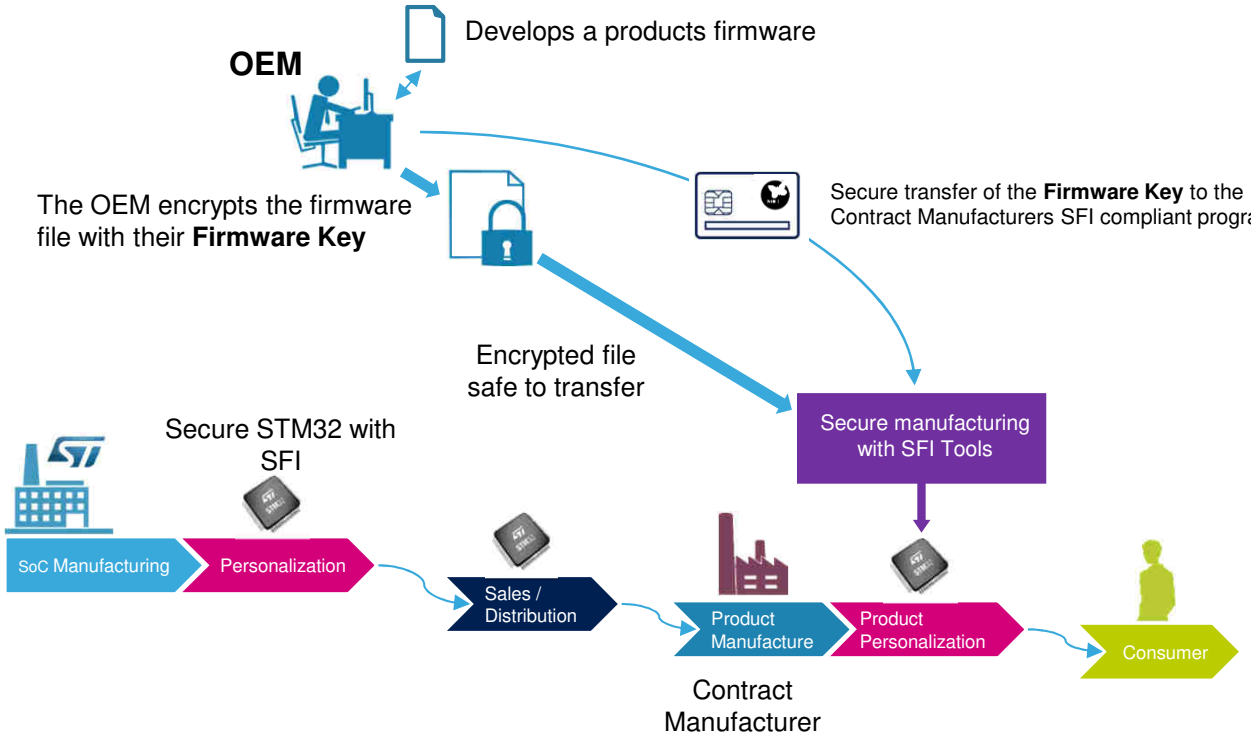
SBSFU Example Code Use Cases

- Industrial Firmware Update
  - Operated by a human action
  - Physical connection between the updater tool and the STM32:
    - UART, SPI, USB, ….. Wired connection
  - Allowed to stop the running application during the update
  - In case of update error, retry is manually managed
- Over The Air Firmware Update (FOTA)
  - Stand alone update operation
  - Wireless device connectivity to receive and manage the update
    - Wifi, LPWan, BT/BLE, ….
  - Running application shall manage its own firmware update
  - Retry may be difficult to support

Secure Firmware Install

- Problem: I do not want my code/firmware to be accessible by any body
  - Firmware protection against copying or tampering with
  - Production line management
    - Like controlling how many boards are manufactured
- Answer: STM32 **Secure Firmware Install (SFI)**
  - It uses a SFI enabled STM32 with embedded certificate – allowing it to be authenticated
  - SFI supports the loading of encrypted firmware files using :
    - STM32 Boot loader + Secure Firmware Install (SFI) services
    - Firmware is decrypted and programmed into the STM32 User FLASH
  - HOW
    - Firmware encryption tool – **Trusted Package Creator**
    - Firmware programming tools – **STM32 CubeProgrammer** and ST partners programming tools
    - A special SmartCard – STM32HSM

Secure Firmware Install (SFI)



STM32 Built-in Secure Firmware Install

Feature Overview

STM32
Secure Loader

Provides Firmware
Confidentiality / Authenticity

ST Provisioned
Device Certificate

Strong Cryptography
AES, ECC

UART / SPI / USB
Loading Protocols

life.augmented

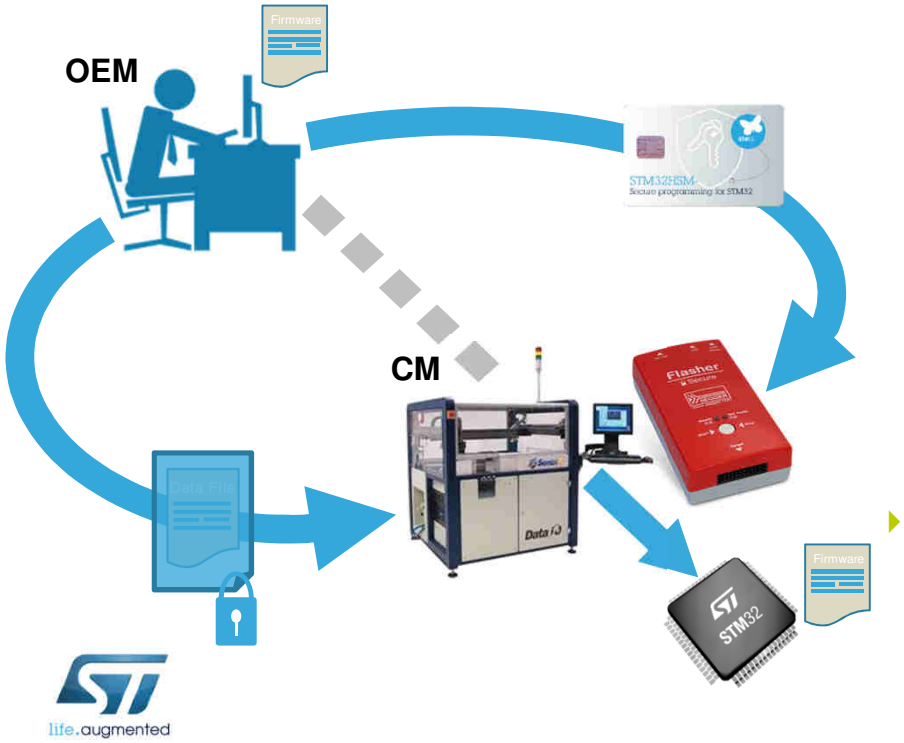
STM32HSM

Used to securely transfer OEM information

- Secure Microcontroller
  - Supports the SFI HSM functions
  - Support ISO7816 T=0 / T = 1 API command format
- Used to Store and Transfer
  - Firmware Key
  - Use Count Limit
    - to control the number of boards made
    - Max limit up to 1 million
  - Firmware Identifier

SFI Ecosystem

The Complete ST SFI Tool Chain Options



For development

Use ST tool chain

TrueSTUDIO for STM32

STM32 CubeProgrammer

For mass production

Partner tool chain

Secure Thingz / DataIO

SECURE THINGZ

Segger Flasher Secure

SEGGER

PSA Certified

STM32L5 is PSA Certified Today!

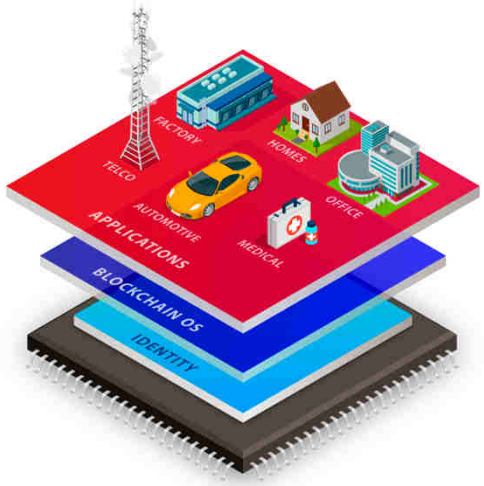
- PSA Certified: Building Trust in IoT with low power consumption
- Why should you care about PSA Certified?
  - It is based published threat models, specs and open source reference code, allowing for MCUs to be tested against
  - ‘Security by design’ approach
  - Industry wide initiative on IoT security
  - Secure devices will drive IoT business
- Level 1: The foundation of PSA Certified
  - STM32L5 is Level 1 certified today
- Level 2: Lab-based evaluation
  - STM32L5 soon to be Level 2 certified

PSA Implemented Today

Four phases of identity

1. **Phase One:** Centralized Identity (administrative control by a single authority or hierarchy)
2. **Phase Two:** Federated Identity (administrative control by multiple, federated authorities)
3. **Phase Three:** User-Centric Identity (individual or administrative control across multiple authorities without requiring a federation)
4. **Phase Four:** Self-Sovereign Identity (individual control across any number of authorities)

Autonomous Security allows a PSA certified Chip such as STM32L4 or STM32L5 to create its own Identity and PKI in the Trusted Execution Environment along with key exchange and management through digital ledger for secure end-to-end encryption.



NXM's Autonomous Security Software Platform spans multiple industries and commercial sectors

Conclusion

STM32L5 helps designers to answer to IoT challenges

STM32 L5

- More security
- Lower power consumption
- Integration, size, performance

life.augmented

Important Links

STM32L5 helps designers to answer to IoT challenges

- www.st.com/stm32l5
- X-CUBE-SBSFU, https://www.st.com/en/embedded-software/x-cube-sbsfu.html
- https://www.researchgate.net/publication/330696364
  - Demystifying Trust Zone
- https://www.psacertified.org/
  - PSA Certification
- https://www.nxmlabs.com/

Thank You - Questions

life.augmented

www.st.com/stm32l5