Securing IoT devices with STM32 & STSAFE Products family

Fabrice Gendreau

Secure MCUs Marketing & Application Managers – EMEA Region

Application Strategic Focus

The leading provider of products and solutions for Smart Driving and the Internet of Things

Internet of Things

Smart Driving

Smart Things

Smart Home & City

Smart Industry

Smart Driving

Secure market & applications

Banking, ID

ST31 – STS3921/22- ST53

PayTV, Transport &
Banking, ID

Authentication

STSAFE & Custom

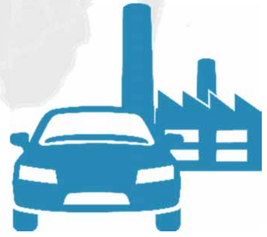
Smart World &
Internet of things

Mobile security

ST33 - ST21NFC – ST54

Mobile &
Secure NFC

M2M &
Automotive

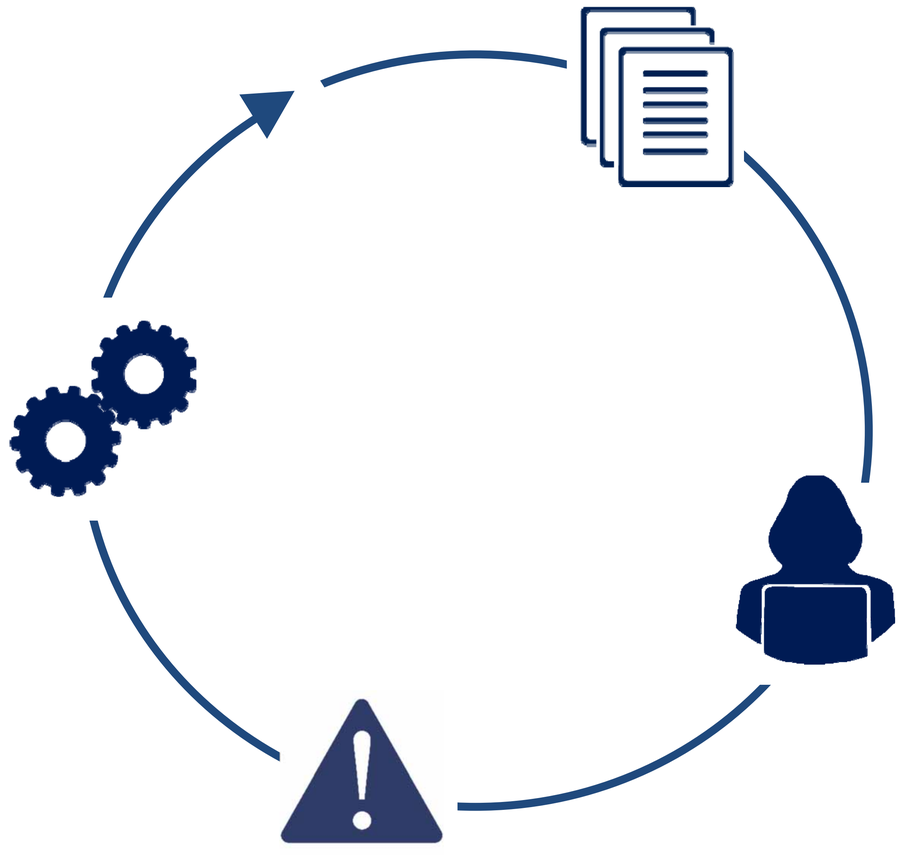


Wearable

life.augmented

Building a fortified solution
is all about risk management

- Understand the value of the Assets you are going to protect, taking into account all stake holders
- Understand your Threats and Vulnerabilities
- Develop a security strategy to reduce Risk, using right level of security for the value of the Assets being protected
- Make use of the integrity and cryptographic tools available



life.augmented

Internet of Things – Threats and Needs

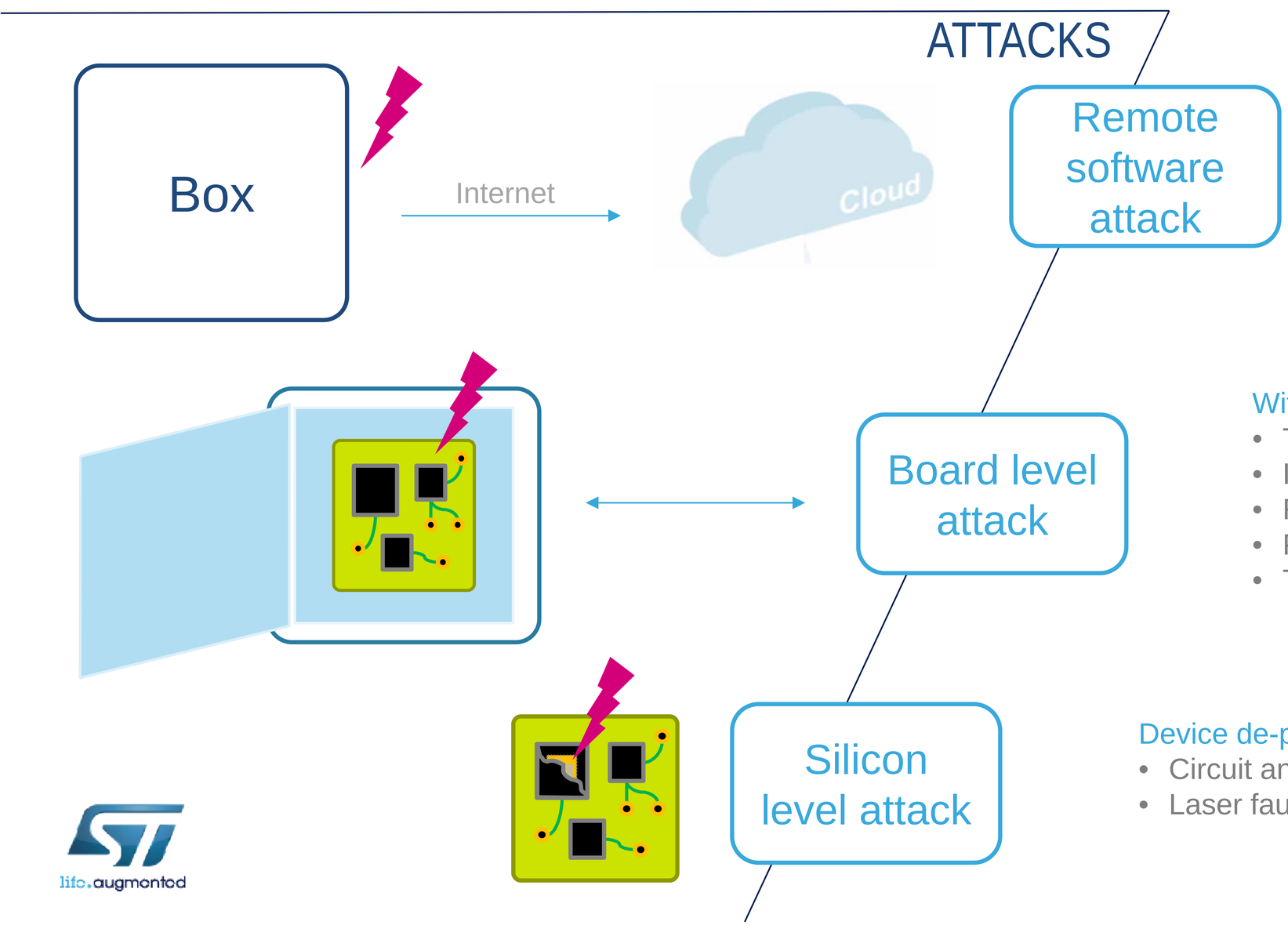
Threats	Needs	Answer
Device Cloning & Counterfeiting • A cloned device compromises OEM revenues • A counterfeited device compromises OEM brand • IoT network or cloud application is polluted by fake devices sending erroneous data	Resistance against cloning, hacking	**Device authentication** Device to device Device to server
User data corruption & eavesdropping • Data travel in clear over the network and expose some personal data • An corrupted measurement is sent to the cloud	Data privacy & confidentiality	**Secure Data storage** **Secure Data communication** Encryption & signature
Device malfunction • An erroneous command is sent to an actuator by a fake server • A malware is injected in a device to modify its behavior	Prevent denial of service	**Platform Integrity** Secure Boot Secure Firmware Upgrade

Secure MCU

life.augmented

Authentication and Encryption strength depends on how well keys are protected

Identify the classes of Attacks



Misuse of network protocols
- Exploit communication protocol errors
- Flaws in software design / implementation

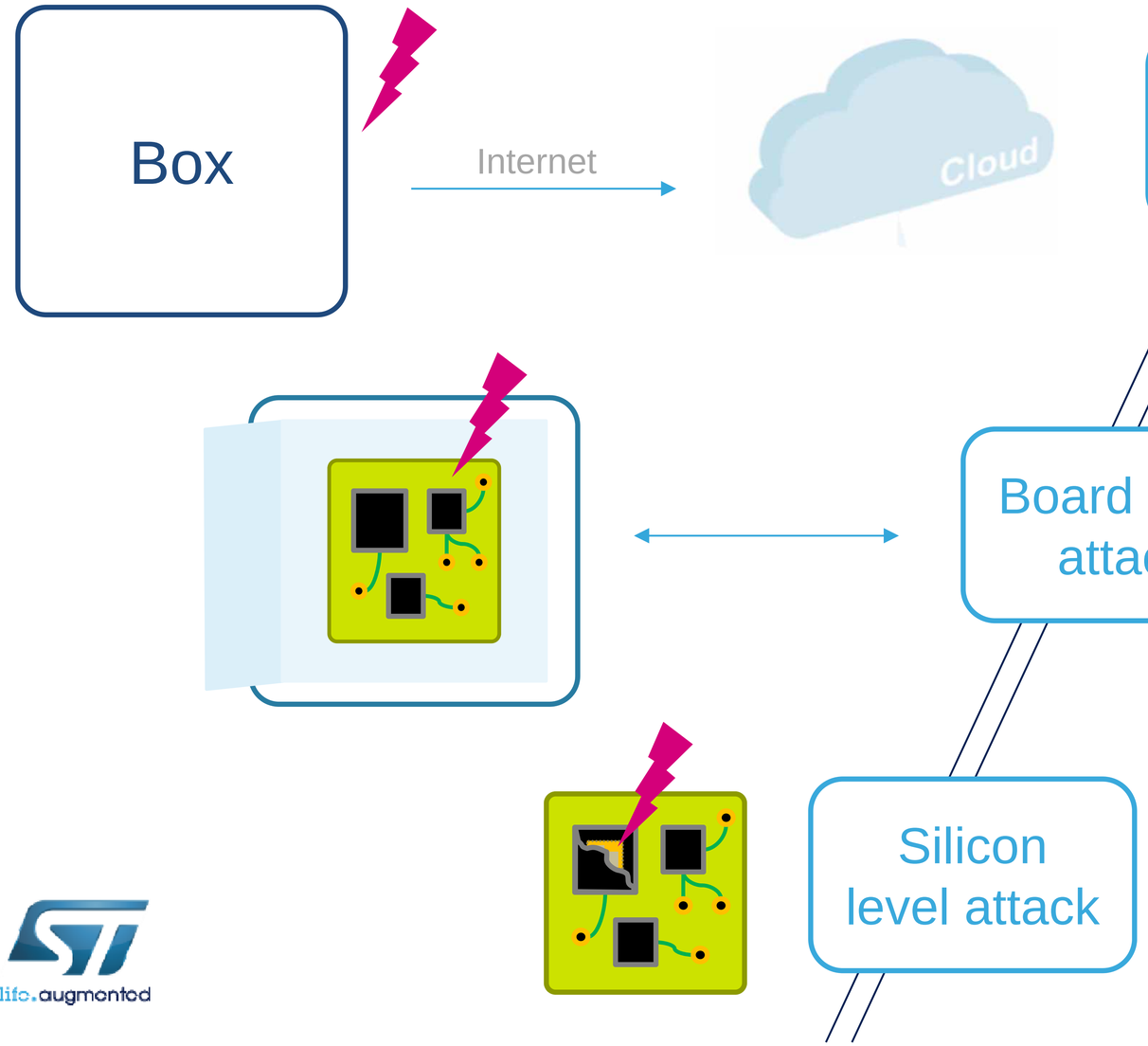
With the case opened / removed
- Test / debug port access
- Inter device bus and IO probing
- Reset, clock attacks
- Power analysis
- Temperature / electrical attacks (glitch, overvoltage)

Device de-packaged
- Circuit analysis and probing
- Laser fault injection

life.augmented

Identify the classes of Attacks

ATTACKS / SOLUTIONS



Adding Secure Element

Add a Certified (CC EAL5+) Secure Element for security improvements

which guaranties optimum security against Remote, Board and Silicon level attack

- Protection against faults injection
- Protection against side-channel attacks
- Monitoring of environmental parameters
- Memory obfuscation, Active shields
- Strong authentication / crypto services
- Secure key storage and handling
- Secure code storage and execution
- Secure key provisioning

Solution with GP MCUs

Use a MCU's security features offering various security levels linked to FW security development knowhow by customers

- Read out protection level
- Write protection
- Execute only PCROP
- Memory Protection
- Firewall
- Crypto accelerator engine
- Secure Firmware install
- Backup RTC RAM memory

life.augmented

Make use of Cryptographic tools

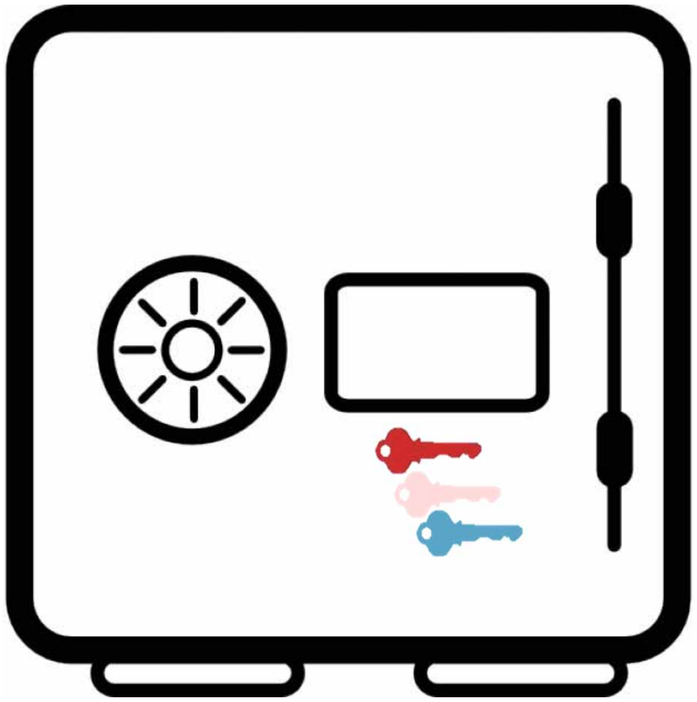
Cryptography is the mathematical toolbox providing security services to build secure systems

Whatever Symmetric (AES) or Asymmetric (RSA, ECC) cryptography

Security mechanism rely on secrets

Secrets are keys 

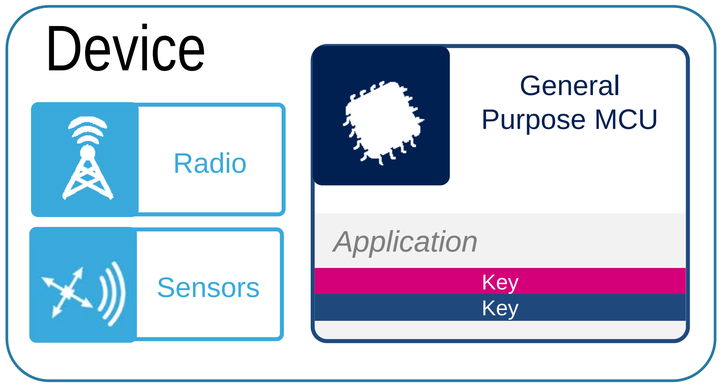
Level of Security depends on how secrets are generated, stored, and handled



life.augmented

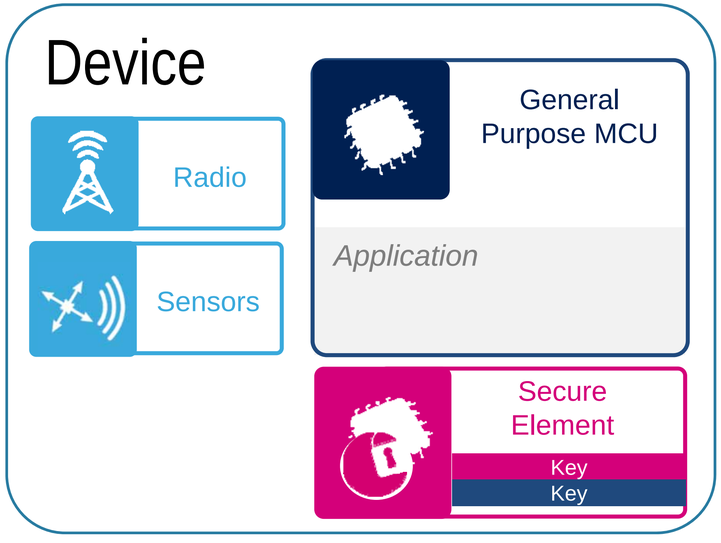
MCU-based devices : possible architectures

Keys stored in General Purpose MCU or in a key container as a Secure Element



Use MCU's embedded security features offering protection against non-invasive attacks

OR



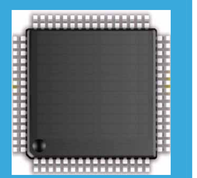
Add a Certified (CC EAL5+) Secure Element which guarantees state of the art security protection against physical and logical attacks

life.augmented

GP MCU’s embedded security features

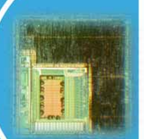
Software Attacks

- Memory Protection Unit (MPU)
- Firewall
- Read Out memory protection
- Write memory protection
- Proprietary Code Read-Out Protection (PCROP)
- RNG, Crypto accelerator, CRC
- Memory ECC, Parity check
- Read while write
- Secure Firmware Install



Non-Invasive Attacks

- JTAG Read out protection
- BOOT from Flash only
- Tamper pads
- RTC alarm, registers, SRAM mass erase
- Power supply integrity monitor
- Clock security system
- Temperature sensor



Invasive Attacks

- GP MCUs not designed to resist against advanced security attacks

life.augmented

Secure Element – Definition

A Secure Element (SE):

- is a tamper-resistant platform (typically a one chip secure microcontroller)
- capable of securely hosting applications and storing their confidential and cryptographic data
- in accordance with the rules and security requirements set forth by a set of well-identified trusted authorities

Secure Element – Trusted Security
Development, Production and Personalization

Non-Invasive attacks
Material & IP Theft

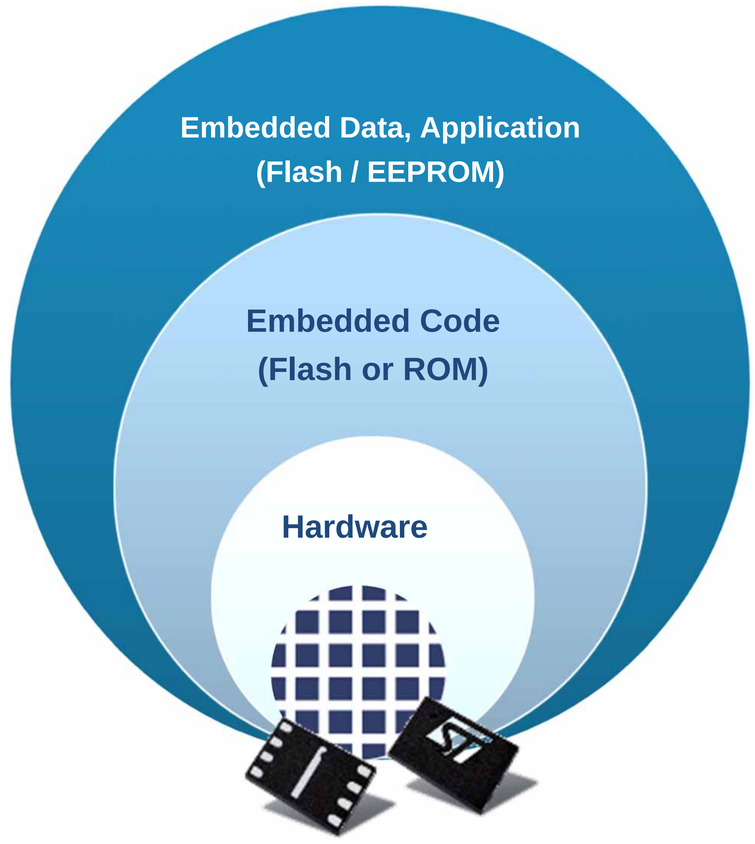
- Secure manufacturing and development environments
- Product lifecycle management

Semi-Invasive attacks
Fault Injection

- Dedicated architecture and design
- Hardware and Software countermeasures

Invasive
Physical Attacks

- Shields
- Intrusion detectors
- Obfuscation



Security evaluated by independent 3rd party laboratories according to defined rules and rankings


PREMIER MINISTRE

Schéma français d'évaluation et de certification de la sécurité des technologies de l'information

CERTIFICAT ANSSI-CC-2014/46

Microcontrôleur sécurisé ST33G1M2 révision F, Firmware révision 9, incluant optionnellement la bibliothèque cryptographique Neslib 4.1 et la bibliothèque MIFARE® DESFire® EV1 3.7 ou 3.8

Développeur : STMicroelectronics

Commanditaire : STMicroelectronics

Paris, le 21 juillet 2014

Common Criteria

EMVCo

life.augmented

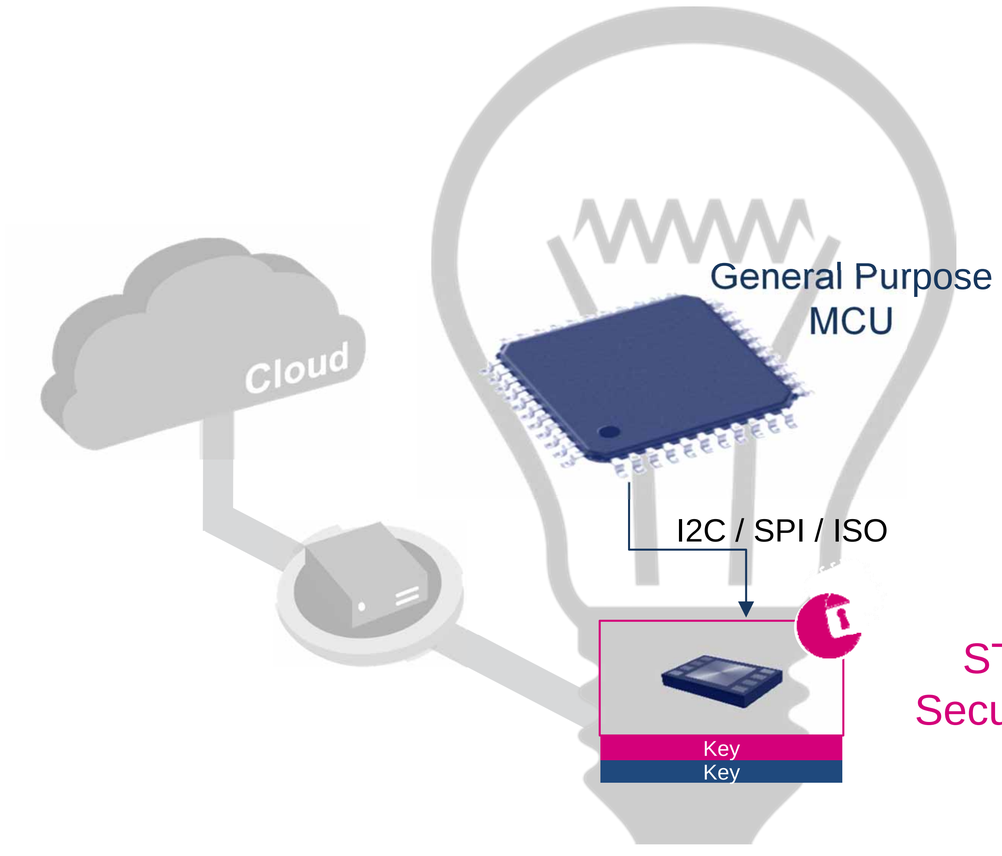
Different kinds of Secure Element

	STSAFE-A Optimized SE	STSAFE-TPM Standardized SE	STSAFE-J Flexible Java Card SE
Key Function	Authentication, Encryption, Signature, Secure Storage	Platform integrity measurement and reporting	Running Specific Applications
Firmware	Native OS Providing dedicated Crypto Services	TCG compliant OS TPM 1.2 or 2.0 commands set CC EAL4+ certified FIPS 140-2 certified	Java Card OS 3.0.4 Global Platform 2.1.1 CC EAL5+ certified
Hardware	Secure Microcontroller Secure Core CPU / ROM or FLASH memory / Hardware Crypto Accelerators RSA, ECC, DES, AES CC EAL5+ or EAL6+ certified		

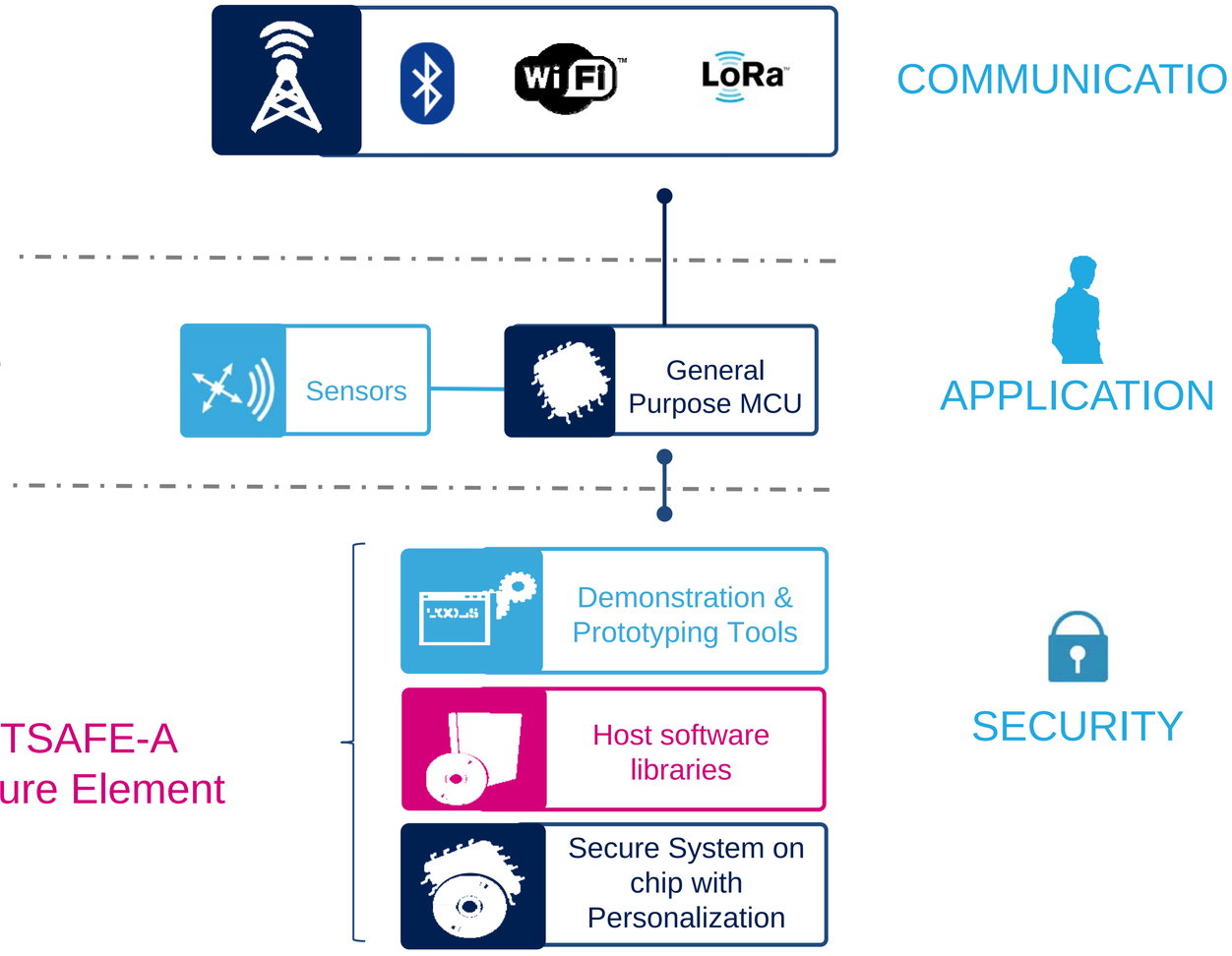
life.augmented

Combining Secure Element with local Host MCU

Enabling easy of use security services for IoT developers



STSAFE-A
Secure Element



life.augmented

Combining STSAFE-A to local Host MCU

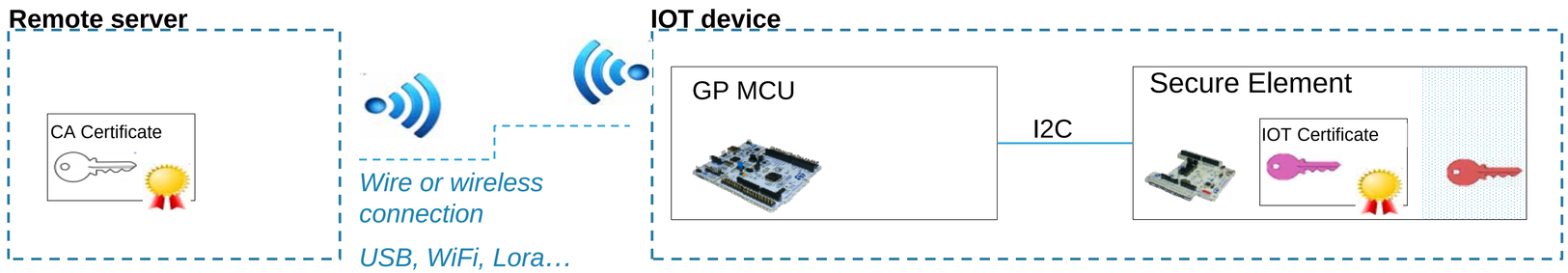
Highly secure & cost optimized solution for connected devices

EAL5+ Common Criteria certified chip

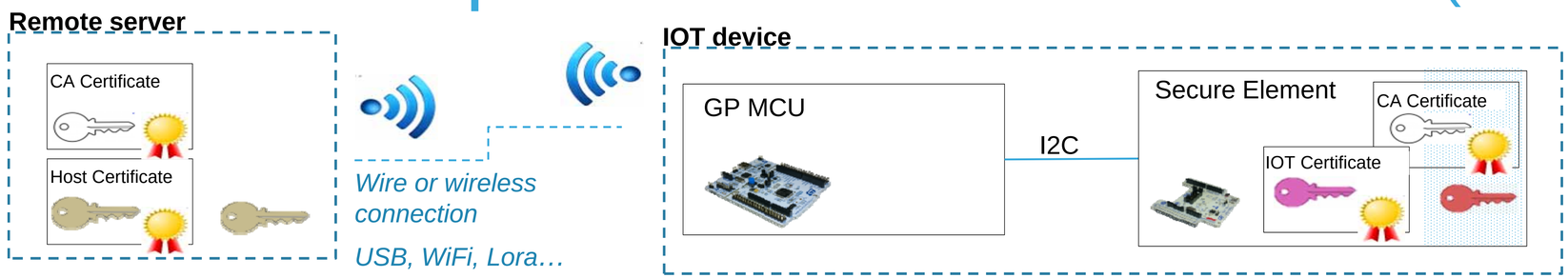
- Authentication (devices to servers)
- Secure communication (Integrity & Confidentiality)
- Secure Data storage
- Signature verification (Secure Boot & Secure Firmware update)
- Secure key provisioning service
- Seamless integration with GP MCU

life.augmented

1st Use case example : Peripheral authentication



2nd Use case example : TLS Handshake V1.2 (RFC 5246)



Client Hello (client random)

Client provides supported TLS version, algorithms and a random

Replies algorithms choices

Server Hello (server random)

Provides X509 certificate and signed random

Certificate (), signed client random

Request IOT device X509 certificate

Certificate Request ()

Provides EC public key and the curve to use

Server Key Exchange ()

Server Hello done ()

Processing
- Verify Server host certificates with CA certificate
- Authenticate server verifying signature
- Generate ephemeral EC key pairs
- Computes shared secret using Remote server public key

Verifies IOT Device certificate and authenticate IOT device

Certificate (), signed server random

Provides IOT device X509 certificate and signed random

Computes Diffie-Hellman shared secret

Client Key Exchange ()

Provides ephemeral public key

Certificate Verify ()

Change Cipher Spec ()

Starts exchange ciphering

Client Finished ()

Change Cipher Spec ()

Starts exchange ciphering

Server Finished ()

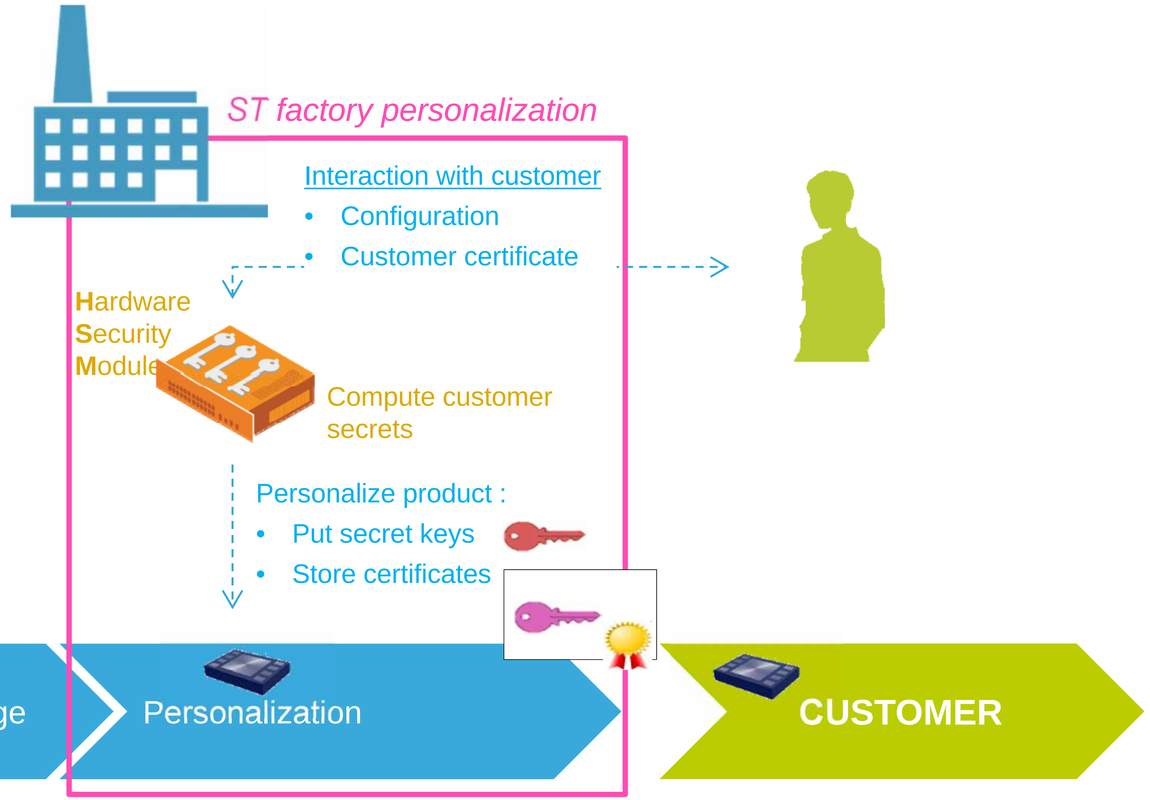
life.augmented

Secure Element personalization service

Securing IoT devices manufacturing

CERTIFICATIONS

VISA · MasterCard · American Express · GSMA Association · ISO 9001 · IQNet · Common Criteria · Consorzio Bancomat · ISO 27001



life.augmented

Approved by Common Criteria · EMVCo

Secure Element seamless integration

A comprehensive set of tools and services

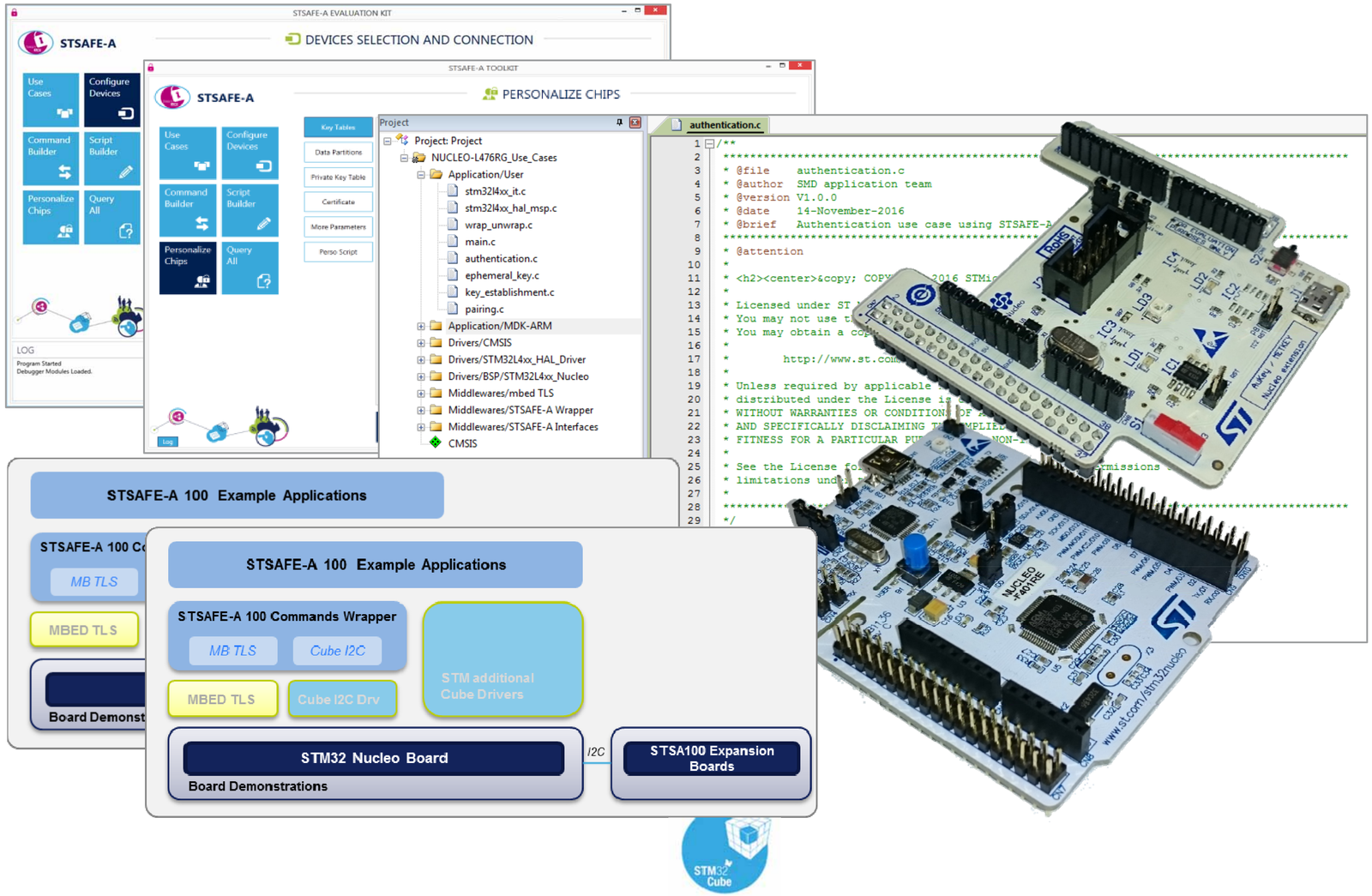
STSAFE Nucleo Expansion

STSAFE Toolkit PC application

Personalization service

Host library

Example codes



Scalable Security Platform for IoT Devices

powered by STSAFE, ProvenCore-M & STM32

Ensuring platform integrity

STM32L4 MCU

For faster, reliable and robust applications development

ProvenCore™-M Secure Operating System

For application isolation, stability and integrity of the platform

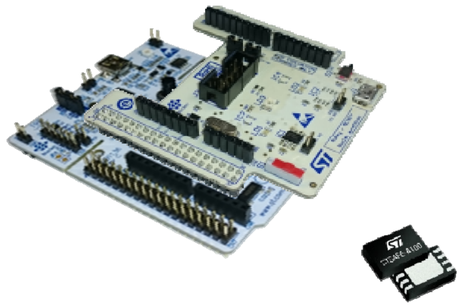
STSAFE™-A Secure Element

Providing secure storage, crypto-services to strengthen secure boot & firmware update

Secure Cloud Connectivity with STSAFE-A

STSAFE-A100 secure and ease devices registration to Amazon Web Services

Device by device registration with STSAFE-A100 standard personalization for evaluation



STSAFE-A100 evaluation Kit
Security for Amazon Web Services

Devices JIT(just in time) registration to AWS with STSAFE-A100 preconfigured for AWS
Allow mass devices automatic registration to AWS

STSAFE-A100 TLS secure connection establishment

life.augmented

Secure Sigfox Ready™ Connectivity
powered by STSAFE-A, S2-LP & STM32

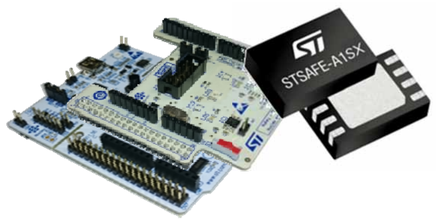
Ultra-low-power Sensor-to-Cloud Connectivity out-of-the-box

S2-LP evaluation Kit

STEVAL-FKI868V1(*) – 868MHZ

STEVAL-FKI915V1(*) - 915MHz + PA

(*) SIGFOX End Product certified



STSAFE-A1SX evaluation Kit

Security for Sigfox Ready™

S2-LP

Ultra-low power, high performance,
Sub-1GHz RF transceiver

STSAFE-A1SX

Plug and play certified security
HW CC EAL5+

STM32L

Ultra-low-power MCU portfolio

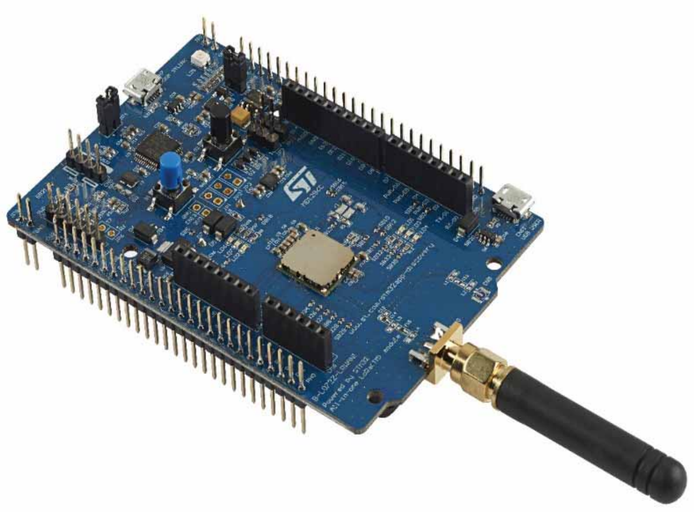
life.augmented

Secure LoRaWAN™ Connectivity
powered by STSAFE-A1LR & STM32L

G+D, Murata, and STMicroelectronics Bring Flexible and Efficient Security Solutions to LoRaWAN™ devices

http://www.st.com/content/st_com/en/about/media-center/press-item.html/t3957.html

Flexible solutions for IoT security



G+D Mobile Security

muRata INNOVATOR IN ELECTRONICS

The solution consists of :

- G+D's Key Management System
- STM's STSAFE-A secure element attached to STM32 general-purpose microcontroller
- MURATA's LoRaWAN module

Conclusion

- Security is becoming a major concern for IoT devices makers
  - A security breach could lead to loss of consumer confidence, loss of brand reputation and loss of businesses !
- Start with your own risks assessment, understanding the value of assets for all the stake holders
  - Perform a Threats analysis to better understand your Risks
  - Remember Confidentially, Availability and Integrity
- Define your security policy in order to reduce the risks
  - Hackers will go after the weakest links in the system not necessarily directly to their target
- Develop your solution resilient against attacks through out its whole life-cycle
  - By using MCU’s embedded security features for protection against non-invasive attacks
  - And adding a companion Secure Element which guaranties state of the art security protection

life.augmented

Secure Solutions

Ensuring your peace of mind

http://www.st.com/en/secure-mcus/authentication-secure-iot.html

life.augmented