Secure Cloud-Connected Sensor Nodes – A Modular Approach!

Security: a mandatory pillar in every new embedded design

SMART | CONNECTED | SECURE

Embedded Security Snapshot

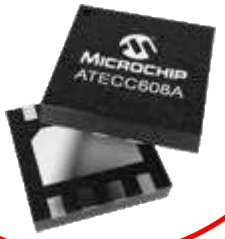
All those features require a
Crypto-ALGORITHM (the math) triggered by a KEY (the secret)

Application layer security	Leverage cryptographic capabilities of the system to further harden the implementation (access rights - privileges)
Secure Connectivity	Authenticate and encrypts the device communication
Secure update	Leverage secure communication and secure boot mechanisms to ensure safe delivery of genuine images
IP Protection	Prevents adversaries to steal IP residing in the firmware of the MCU or RTL of the FPGA
Counterfeit Protection	Prevents adversaries counterfeit disposable goods (cartridge) or protect from copies of accessories
Hardware Root of Trust	Firmware validation (aka secure boot – for all systems) **Trustable identity**

Microcontrollers
32/16/8-bit
Ex : Arm® Cortex®- M23
+

Microprocessors
Arm® Cortex®-A5

Secure Elements
Common Criteria (JIL) Rated HIGH



Network controllers
Wired & Wireless
Integrated communication stacks

FPGA
Solutions

Importance of Keys in Security

- **Security: It's All About the Key**

- A cryptosystem should be secure if everything about the system – ***except the key*** – is public knowledge

  Kerckhoff's Principle

What a private key really looks like
JVFDvdfvJvfdnjvjk543524cds9ics9cCDSCcs0dcw8eidpciswsn8934XSCDS

- The Enemy **Knows** the System

  Claude Shannon

- Why are the keys important ? With the possession of the key, critical **transactions can be impersonated**

Secure Element challenge

Notion of Personalization

The secure device needs to be personalized

- Find and learn complex tools and access expert knowledge to start prototyping
- Configuration mapping the use case(s)
- Key ceremony to “exchange secrets” and trigger provisioning process
- Manufacture the device in a secured supply chain equipped with Hardware Secure Modules (HSM)
- Results in custom part number (Today market threshold for direct support and provisioning services >100ku)

Ecosystem challenge

support Cloud solutions, MCU's, Connectivity link (Wireless / Wired), stack providers… while keeping the Secure Root of Trust

Google Cloud

amazon web services

Microsoft Azure

TLS

arm MBED

CycloneSSL

OpenSSL

wolfSSL

8-bit

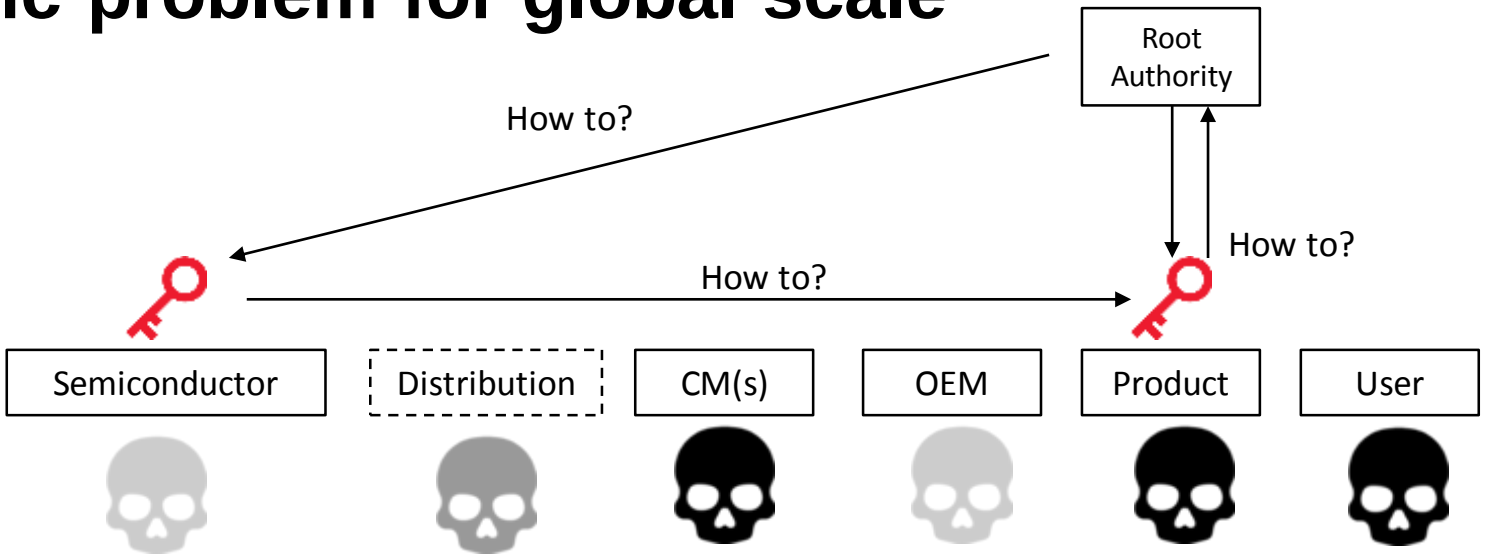
16-bit

32-bit

Wi Fi CERTIFIED

Key Distribution challenge

A logistic problem for global scale



How to ship :

- Sensitive material (the key)
- In a fragmented market
- And a complex distribution model
- While the goal is to reduce exposure to 3rd parties

Small size Customers	Medium size customers	Large size customers

How to...

Ease onboarding with
predefined use cases

Accelerate market adoption
with **simple toolsets**

Support Mass Market with
low MoQ including
provisioning and **certificates**

Architecture Agnostic with
any cloud, any PKI*, any
controller, any connectivity

*PKI : public key infrastructure

A Scalable and Adaptive Provisioning Service

	Ready-to-Go	Flexible	Custom
Pre-Configured	YES	YES	NO
Pre-Provisioned	YES	YES (flexible)	NO
Minimum Order Quantity (MOQ)	Few units	Few thousands units	Few thousands units
Development Time	Lowest	Lower	Custom
Complexity	Lowest	Lower	Custom
Secure Key Storage	JIL High	JIL High	JIL High

AWS Modular approach

AWS IoT
Greengrass HSI (Linux)
OpenSSL
Linux MPU
Secure Element

AWS IoT
FreeRTOS
mBed TLS
Wifi module
CortexM4
Secure Element

AWS IoT
a:FreeRTOS
mBed TLS
Wifi module
CortexM7
Secure Element

AWS IoT
a:FreeRTOS
mBed TLS
Wifi module
PIC32
Secure Element

Google Modular approach

Google IoT
Linux
OpenSSL
Raspberry Pi
Secure Element

Google IoT
C-SDK
mBedTLS
Ethernet
CortexM4
Secure Element

Google IoT
No RTOS
WINC TLS
Wifi module
CortexM4
Secure Element

Google IoT
No RTOS
WINC TLS
Wifi module
CortexM0+
Secure Element

Google IoT
No RTOS
WINC TLS
Wifi module
16-bit MCU
Secure Element

Google IoT
No RTOS
WINC TLS
Wifi module
8-bit MCU
Secure Element

LoRaWAN Modular approach

CortexM0+ SiP with LoRa Radio
+ Secure Element
+ LoRaWan Stack

arm MBED OS

ATSAML21-XPRO
+ LoRa Discrete Radio
+ Secure Element
+ Arm® Mbed™ OS
LoRaWAN stack

Secure Element with any MCU + LoRa radio + LoRaWAN stack

Trust Platform

Pre-Configured	YES	YES	NO
Pre-Provisioned	YES	YES (flexible)	NO
Minimum Order Quantity (MOQ)	10 units	2000 units	4000 units
Development Time	Lowest	Lower	Custom
Complexity	Lowest	Lower	Custom
Secure Key Storage	JIL High	JIL High	JIL High

Simpler Onboarding with Trust Platform Design Suite

1 Define

Map use case to configuration

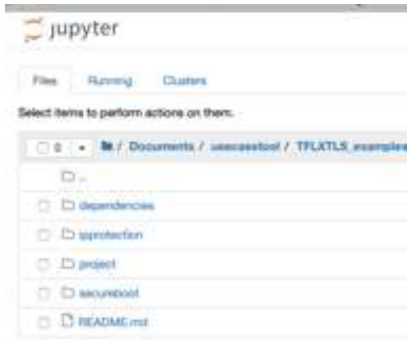
Use Case Tool

2 Prototype

Python executable tutorial

Jupyter Notebook

3 Develop



C-code projects for each use case

Any IDE

4 Release

Generates secret exchange file

Secret Exchange

Hardware Development Tools

DM320118

CryptoAuth Trust Platform USB Kit

Direct prototyping

PC Host via USB (with Python Jupyter Notebook tutorials)

Or onboard SAMD21 with debugger

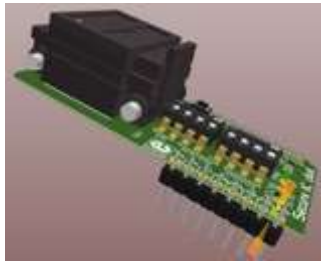
DT100104

ATECC608A Trust Platform Board

Onboard Trust&GO, TrustFLEX, TrustCUSTOM

MikroBUS male/female

Secure UDFN click



UDFN and SOIC

Same functionality as XPRO Socket Boards

MikroBUS male pinout

Sold through Mikroe.com

AT88CKSCKTUDFN

CryptoAuthentication socket kit

UDFN8 socket

SOIC8 socket

Xplain PRO form factor

Thank you for your time!

http://www.microchip.com/TrustPlatform

Contact For Further Information

Mark Korsloot

Product Specialist Embedded Component Solutions

mark.korsloot@alcom.nl

Nicolas Demoulin

EMEA Marketing Manager Secure Products Group

nicolas.demoulin@microchip.com