Firmware Verification with TrustFLEX Secure Elements

Presenter: Brett Kim – Senior Embedded Solutions Engineer

MICROCHIP

Embedded Security Snapshot

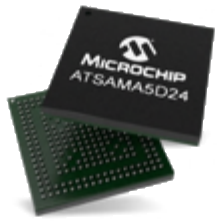
All those features require a

Crypto-ALGORITHM (the math) triggered by a KEY (the secret)

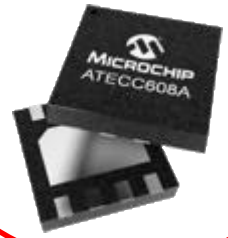
Application Layer Security	Leverage cryptographic capabilities of the system to further harden the implementation (access rights - privileges)
Secure Connectivity	Authenticate and encrypts the device communication
Secure Update	Leverage secure communication and secure boot mechanisms to ensure safe delivery 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	Trustable identity Firmware validation (aka secure boot – for all systems)

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

MICROCHIP

Save Costs, Reduce Risk, Protect Revenue

Secure your Intellectual Property

- **Brand protection and preserve quality**
  - Avoid counterfeits
  - Avoid lower quality and lower performances
  - Controlled ecosystem strategy

- **Enable service revenue streams**
  - Maintenance service strategy
  - Part replacement strategy

- **Revenue stream protection**
  - Start with authentication from the start
  - Protect user experience
  - Avoid discounted copies

- **Reduce cost**
  - Makes sure the IP in your firmware is protected
  - Reduce/mitigate warranty cost of returned products

IP Protection

The **value** is the Intellectual Property (IP) that resides **inside the code** of a system. Consequently, the signed code needs to be verified at any relevant point of time during the operation of the system.

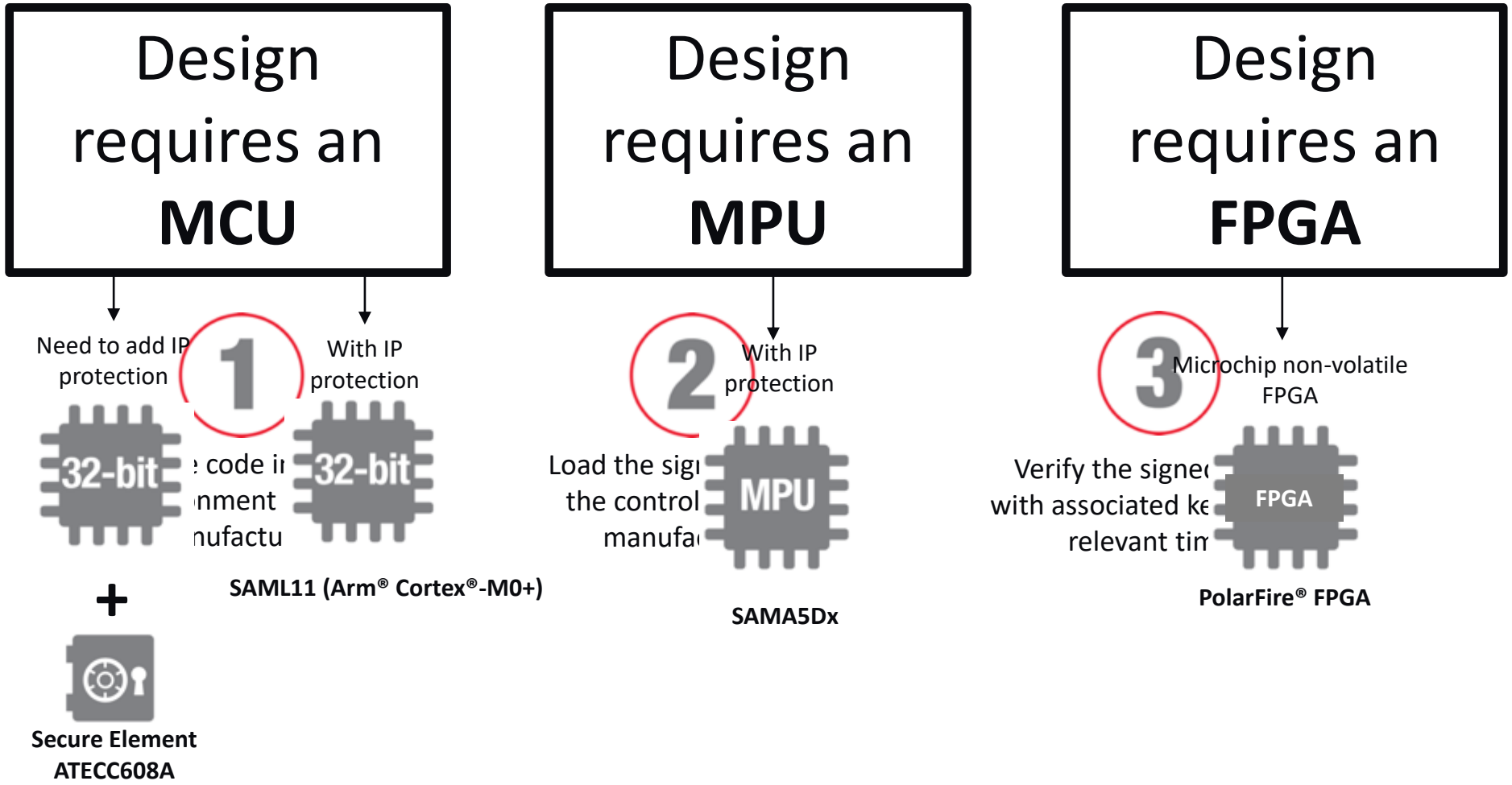
Drone

Hair Dryer

Military

Stadium Speakers

Various Ways to Add IP Protection



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**

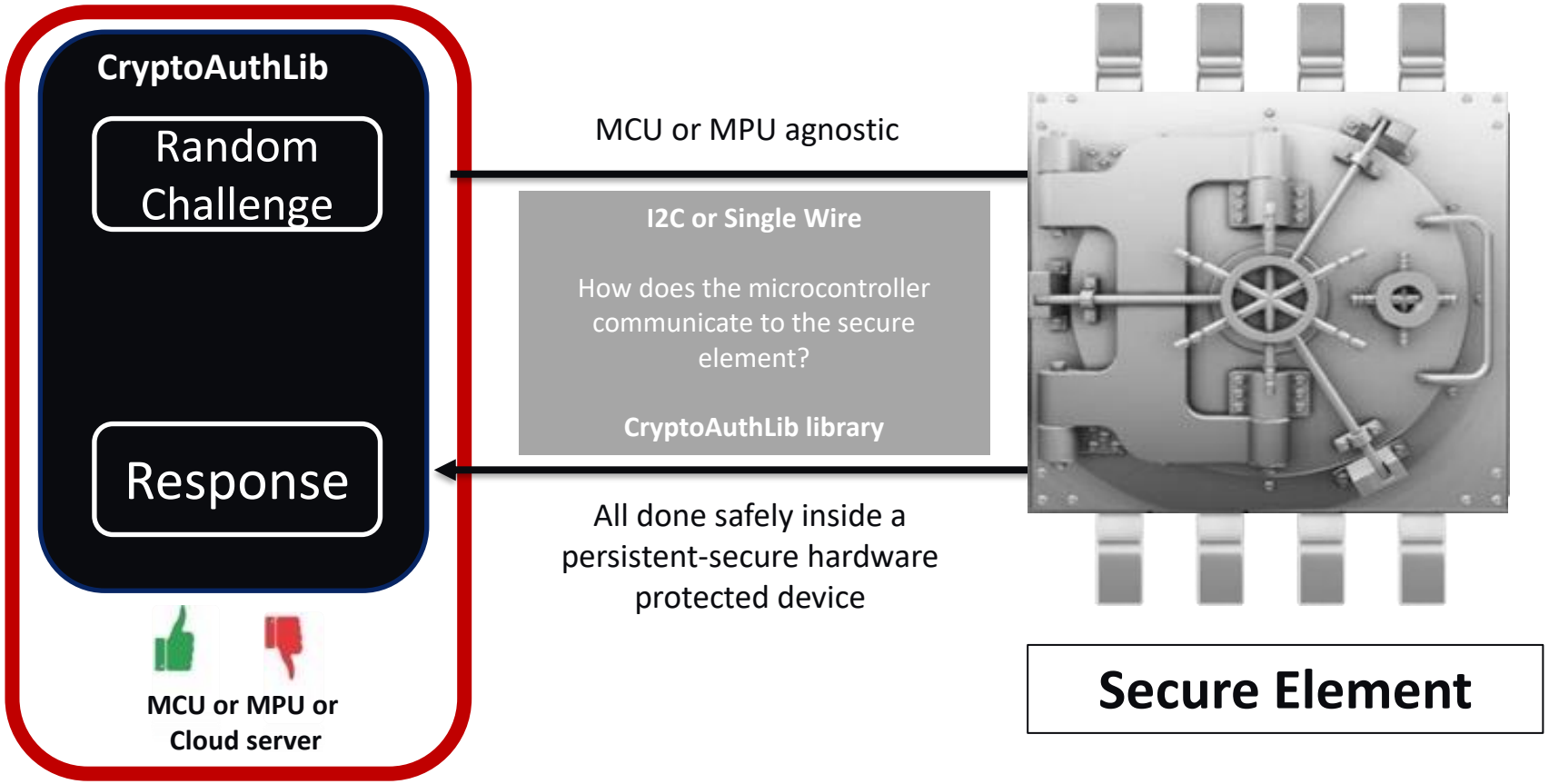
How to Protect the Keys in an IoT System?

Use a Secure Element

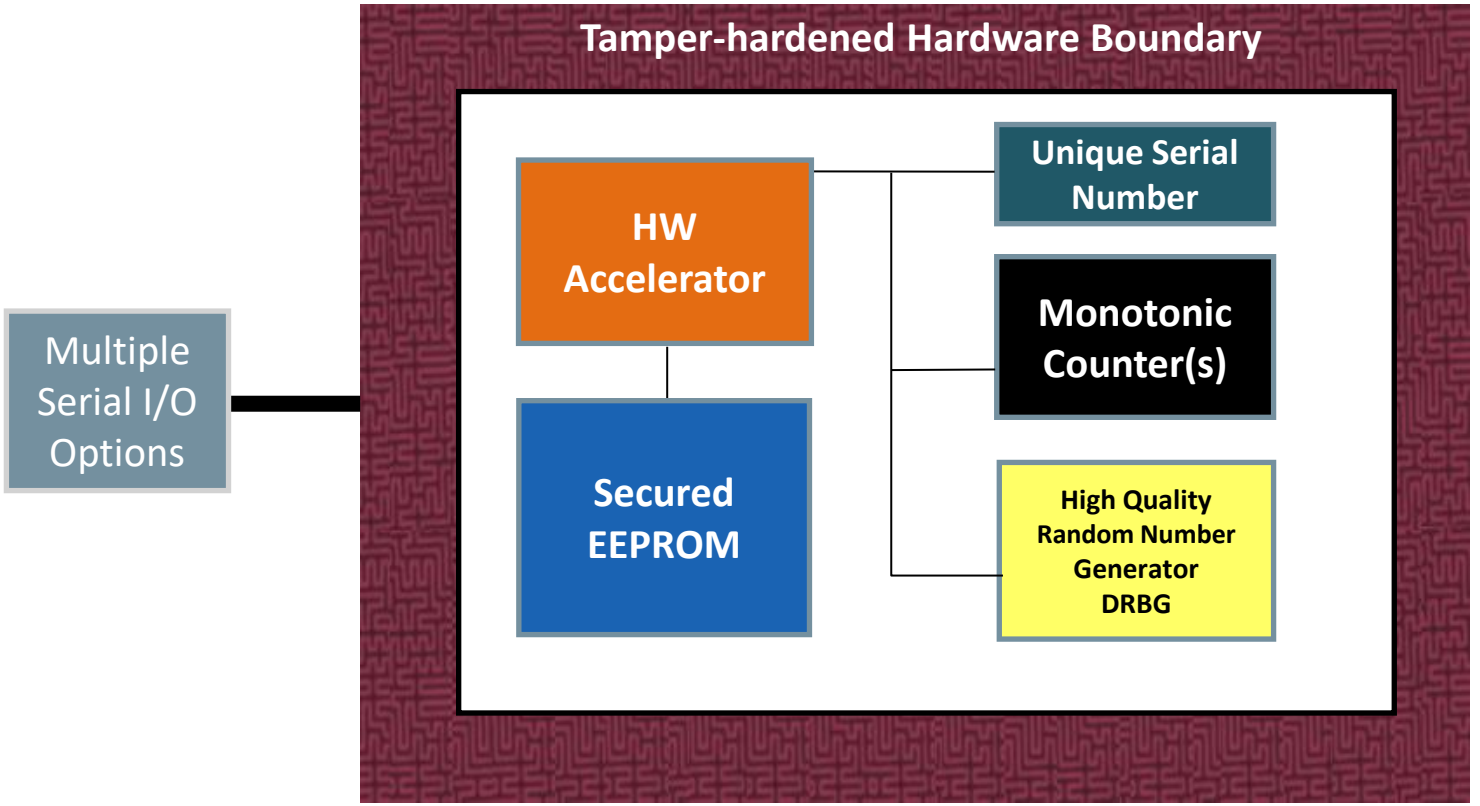
A secure element is a **vault that protects secrets**, it's a companion device to the microcontroller

Inside the vault, secrets are **generated during manufacturing** - inside Microchip secured factories

The secrets (keys, certificates) are **not exposed** and handled by Microchip **secure provisioning** process



Secure Element Basic Architecture



The Challenge

Notion of Personalization

- **Customization due to each key being unique to each product**
- **How do you handle security complexity and customization:**
  - In product development?
  - In the supply chain?

Microchip Trust Platform

		TRUST&GO	TRUST FLEX	TRUST CUSTOM
Pre-configured		YES	YES	NO
Pre-provisioned		YES	YES (flexible)	NO
MOQ	**Low MOQ flow**	10 units	2 000 units	4 000 units
	High Volume flow*	30 000 units	30 000 units	30 000 units
Development time		Lowest	Lower	Custom
Complexity		Lowest	Lower	Custom
Secure key Storage		JIL High	JIL High	JIL High
Devices		ATECC608A	ATECC608A ATSHA204A (w/o RBH) – Q4/2020	ATECC608A ATSHA204A (w/o RBH) – Q3/2020

* MOQ depending on Package / Silicon – showing here the lowest MOQ through the whole product portfolio – **Minimum Annual Business of 100 ku**

TrustFLEX: Overview

Use Cases

- **What if the customer likes Trust&GO, but their use case requires more than Trust&GO?**
- **TrustFLEX allows an overlay of Trust&GO functionality with any combination of the following use cases:**

- **Start with pre-configured only device policies**
- **Cover all the most commonly used use cases**
  - Custom certificate authentication
  - JWT authentication
  - Secure boot (with key attestation)
  - OTA verification
  - FW IP protection
  - Message encryption
  - Key rotation
  - I/O protection key
  - Host accessory authentication

- **Needs to be provisioned with customer credentials**
- **All these use cases require some customer information:**
  - Secure boot public key
  - Secure boot master public key
  - Accessory / IP protection master secret
  - PKI chain

TrustFLEX

Advantages

www.microchip.com/**TrustFLEX**

Flexible

Flexibility

Support any core, any cloud, any certificate authority providers

Accommodate customer's own secrets

Time to Market

Reduce Time to Market

Out of the box pre-defined use cases

No time spent on device configuration

Availability

Low MOQ including Provisioning

Address all types of project and company volume sizes

Security solution for the fragmented mass market

Support

Simple Engagement Model

The Trust Platform Design Suite removes friction for both development and secret exchange

Secure Download Firmware Update

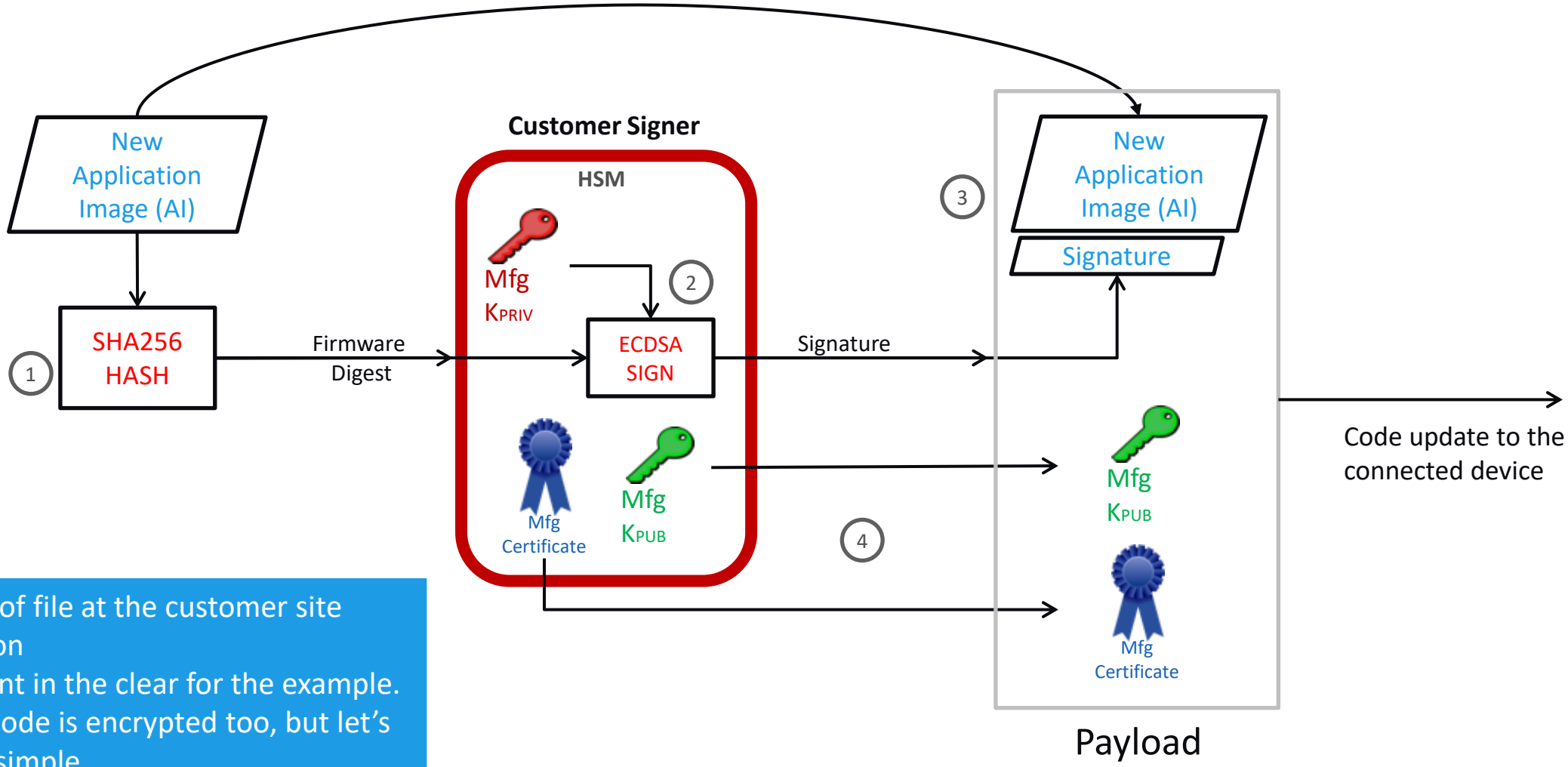
Otherwise called OTA in the World of IoT

Attestation: Secure Download Firmware Update

- **Secure DFU** or otherwise call Over-The-Air (OTA) fall under the category of ***Attestation***
  - *Attestation: To affirm to be correct, true, or genuine*
- **Requirements for Attestation:**
  - Secure Boot: Assurance only genuine code is executed (details in different session)
  - **Secure DFU**: Assurance only genuine upgrade code is accepted and programmed into the MCU/MPU
  - Local and/or remote “run-time attestation” is possible
    - In both cases, this assures the code in question is genuine
- **This presentation covers Secure DFU**

Asymmetric Secure DFU

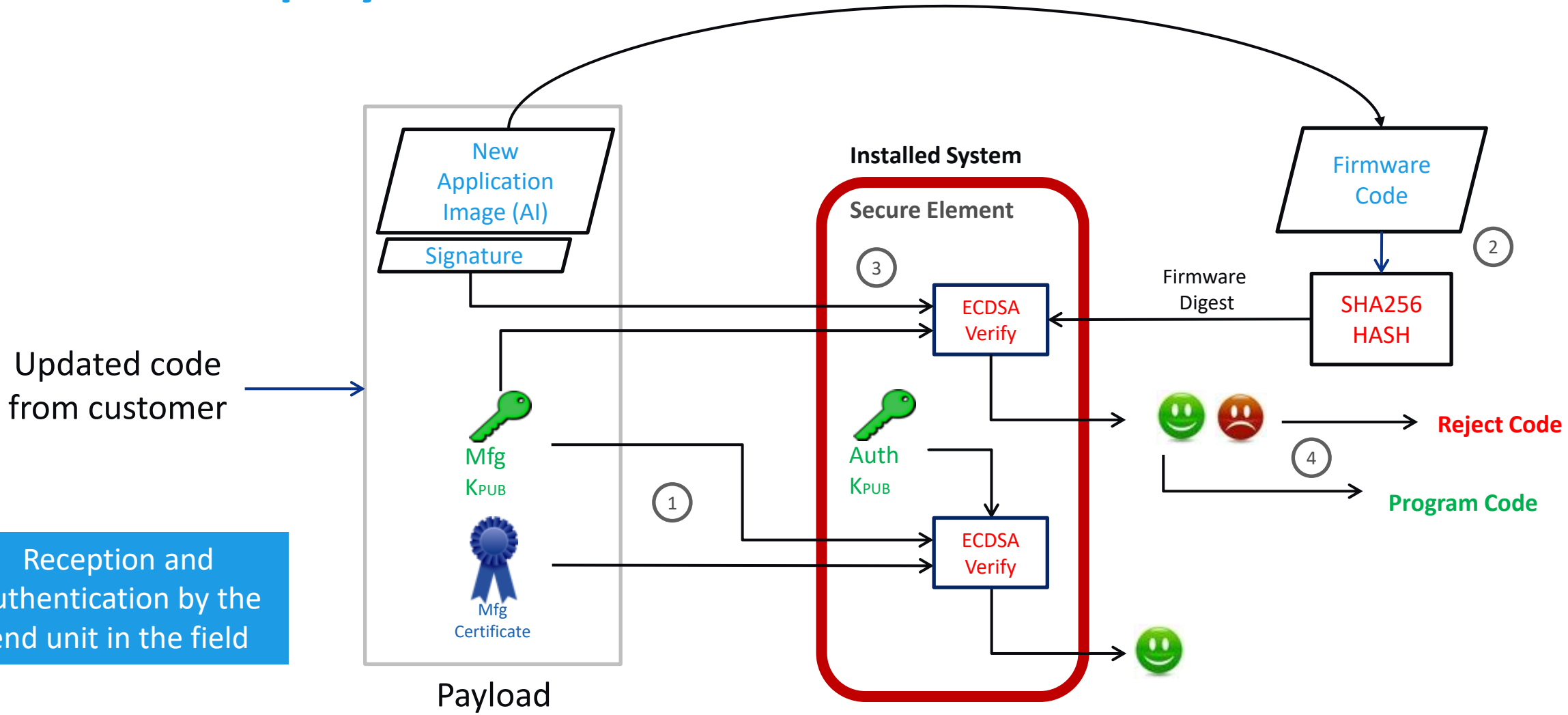
At the Customer Site



- Preparation of file at the customer site
- No encryption
- Firmware sent in the clear for the example. Ideally, the code is encrypted too, but let's keep things simple

Asymmetric Secure DFU

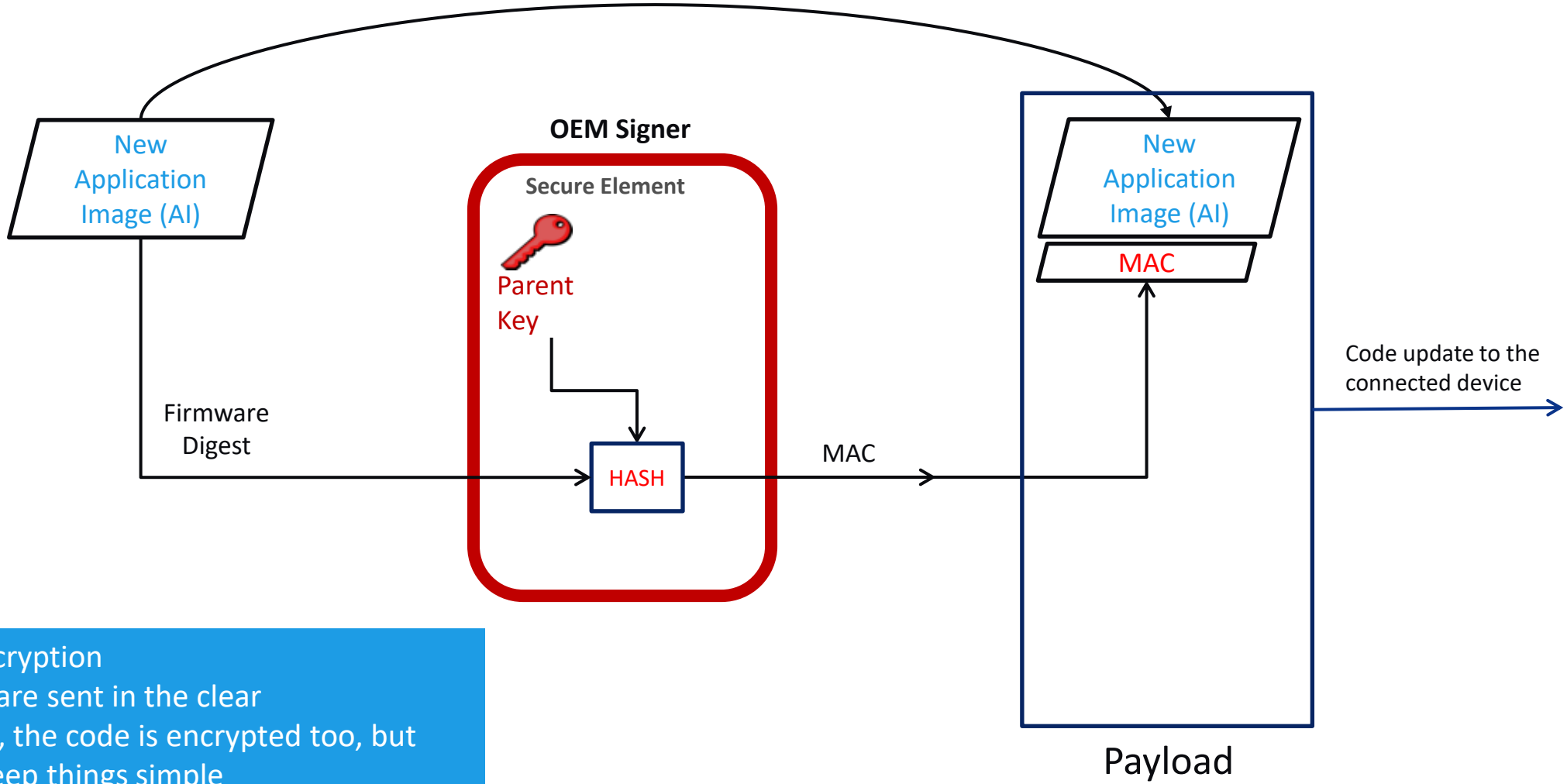
Inside the Deployed IoT Device



MICROCHIP

Symmetric Secure DFU

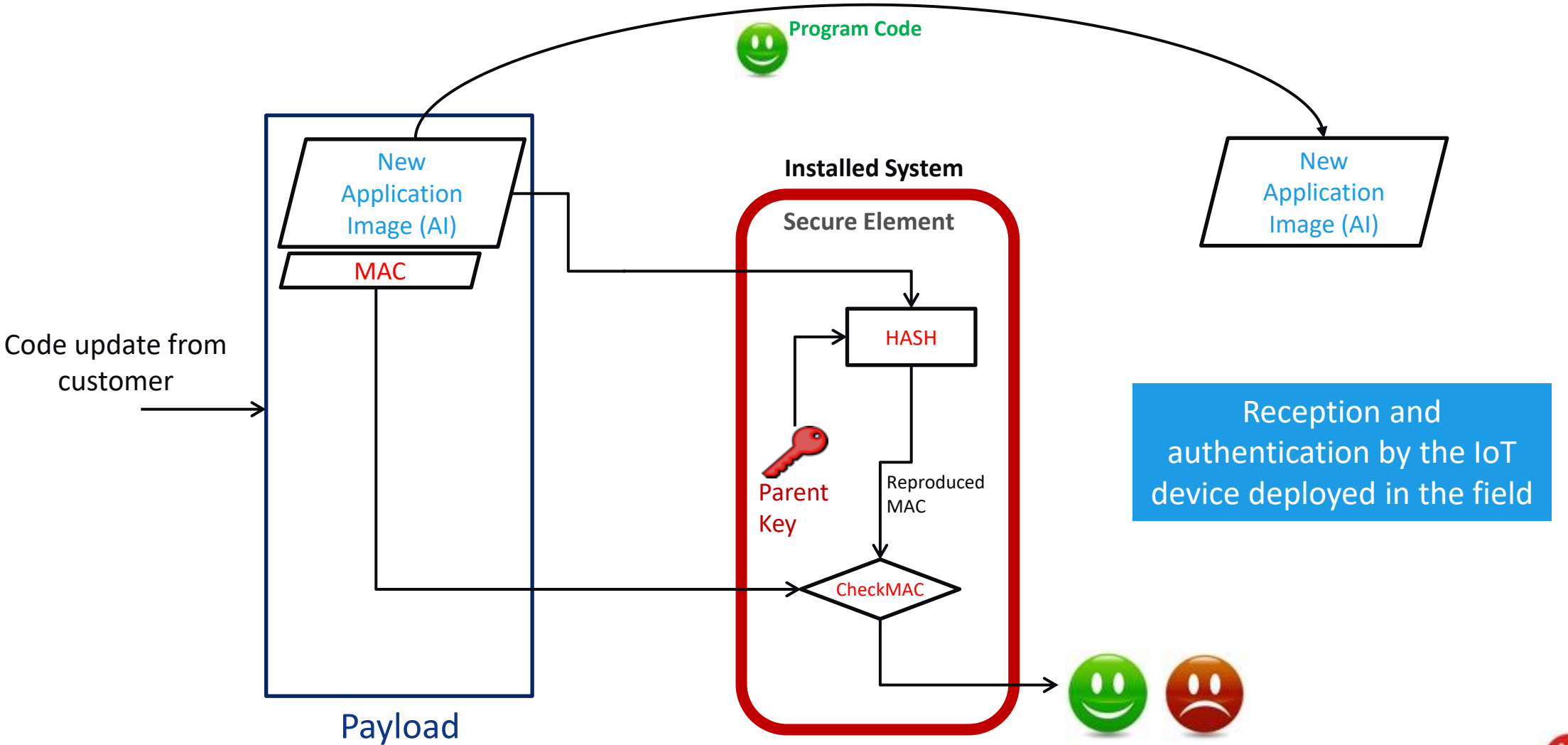
At the Customer Site



- No encryption
- Firmware sent in the clear
  Ideally, the code is encrypted too, but let's keep things simple

Symmetric Secure DFU

Inside the Deployed IoT Device



Reception and authentication by the IoT device deployed in the field

MICROCHIP

Hardware Development Tools

DM320118

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

Mikroe.com Socket

- 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

MICROCHIP

Simpler Onboarding

Trust Platform Design Suite Software

1 Define

Map use case to configuration

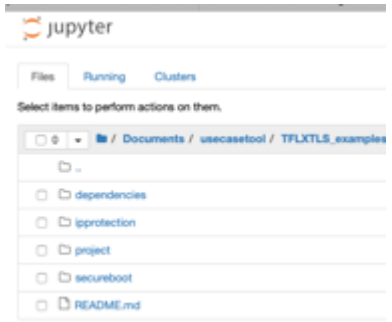
Use Case Tool

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

Download from : https://microchipdeveloper.com/authentication:trust-platform

MICROCHIP

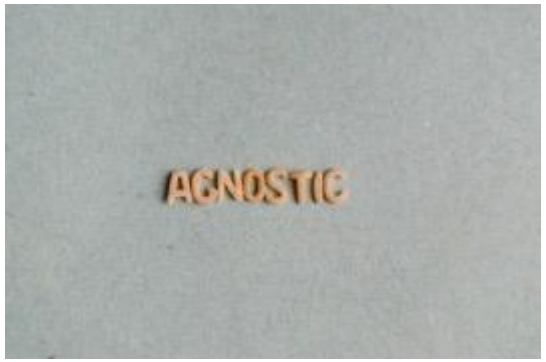
Takeaways

Easier onboarding with **predefined use cases**

Quick development with **simple toolsets**

Simpler flows leveraging **e-commerce stores**

Fitted for mass market with **low MoQ** including **provisioning** and **Microchip certificates**



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

*PKI : public key infrastructure

Microchip Trust Platform

microchip.com/TrustFLEX

MICROCHIP

Thank You