Pre-configured Secure Elements: Onboarding with TrustFLEX for Microsoft Azure IoT Hub

Presenter: Peter Kwak – Principal Embedded Solutions Engineer

MICROCHIP

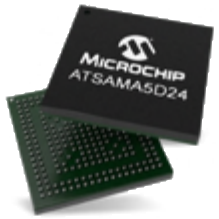
Embedded Security Snapshot

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

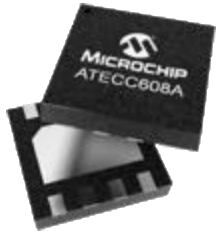
Application Layer Security	Leverage cryptographic capabilities of the system to further harden the implementation (access rights - privileges)
Secure Connectivity	Authenticate and encrypts the device communication
Secure Update	Leverage secure communication and secure boot mechanisms to ensure safe delivery 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
Secure Key Storage



Network controllers
Wired & Wireless
Integrated communication stacks

FPGA
Solutions

MICROCHIP

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

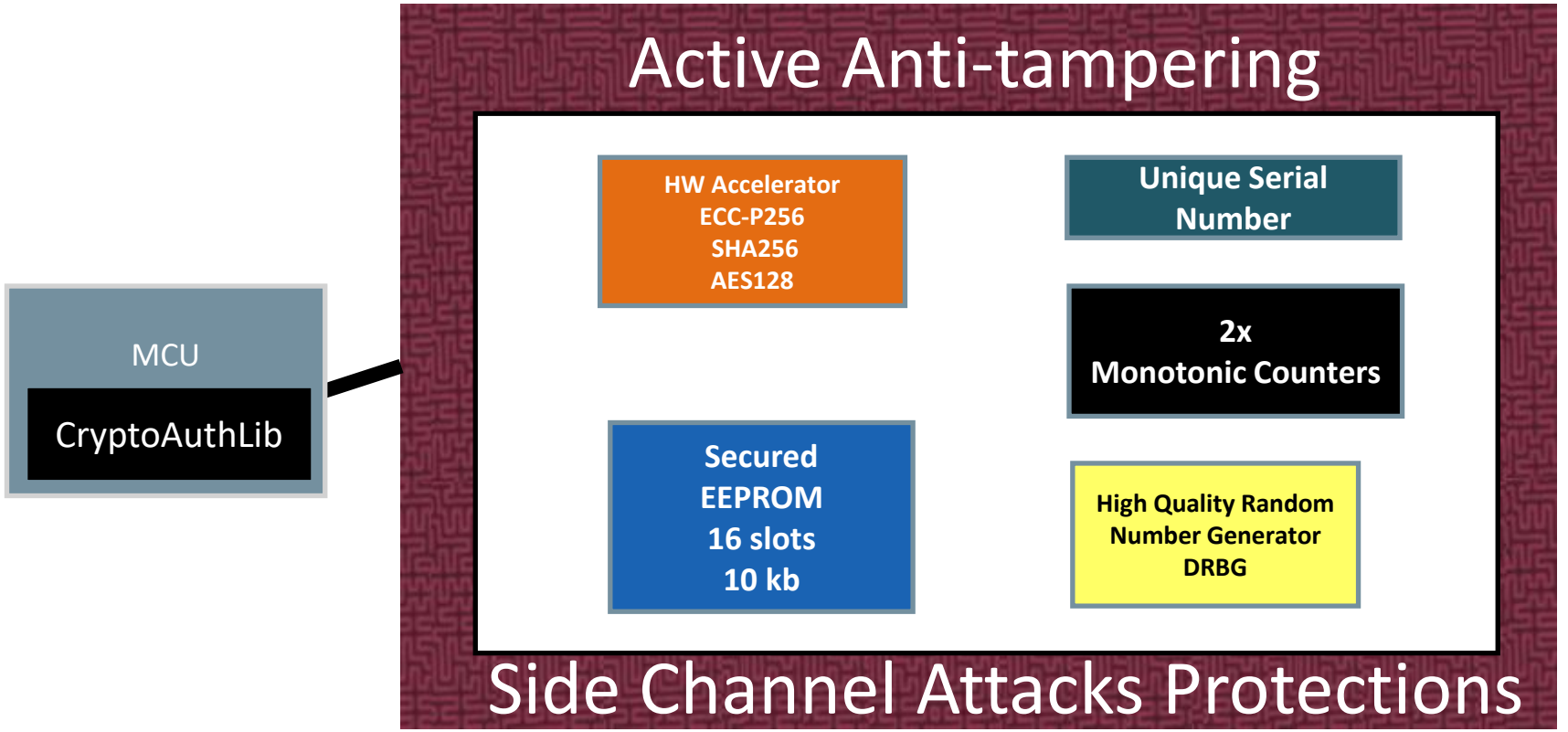
The Enemy Knows the System

Claude Shannon

Why are the keys important? With the possession of the key,

critical transactions can be impersonated

Protects and Isolates Keys in Hardware ATECC608



Challenges

1. **Time to configure the secure authentication use cases in the device**
2. **Logistic complexity of securely provisioning keys and credentials:**
   - Shipping keys globally for any project size
   - Keep keys isolated from everything
   - In a fragmented marketplace

Solution: Microchip Trust Platform
A Scalable and Adapted Provisioning Service

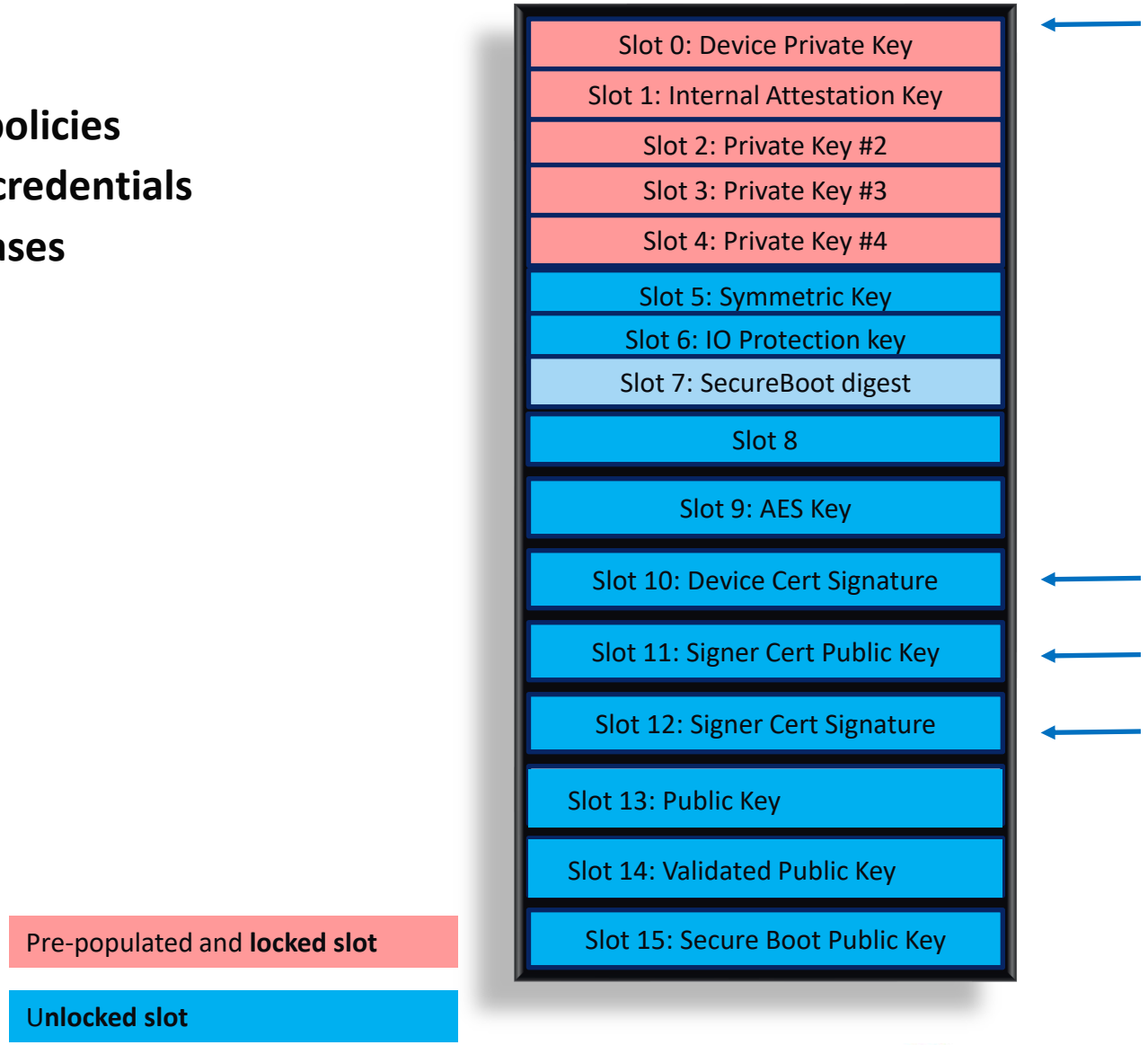
	TRUST&GO	TRUST FLEX	TRUST CUSTOM
Pre-configured	YES	YES	NO
Pre-provisioned	YES	YES (flexible)	NO
MOQ*	10 units	2000 units	4000 units
Development time	Lowest	Lower	Custom
Complexity	Lowest	Lower	Custom
Secure key Storage	JIL High	JIL High	JIL High

Onboarding with TrustFLEX for Microsoft Azure IoT Hub

+

A Flexible Trust Model

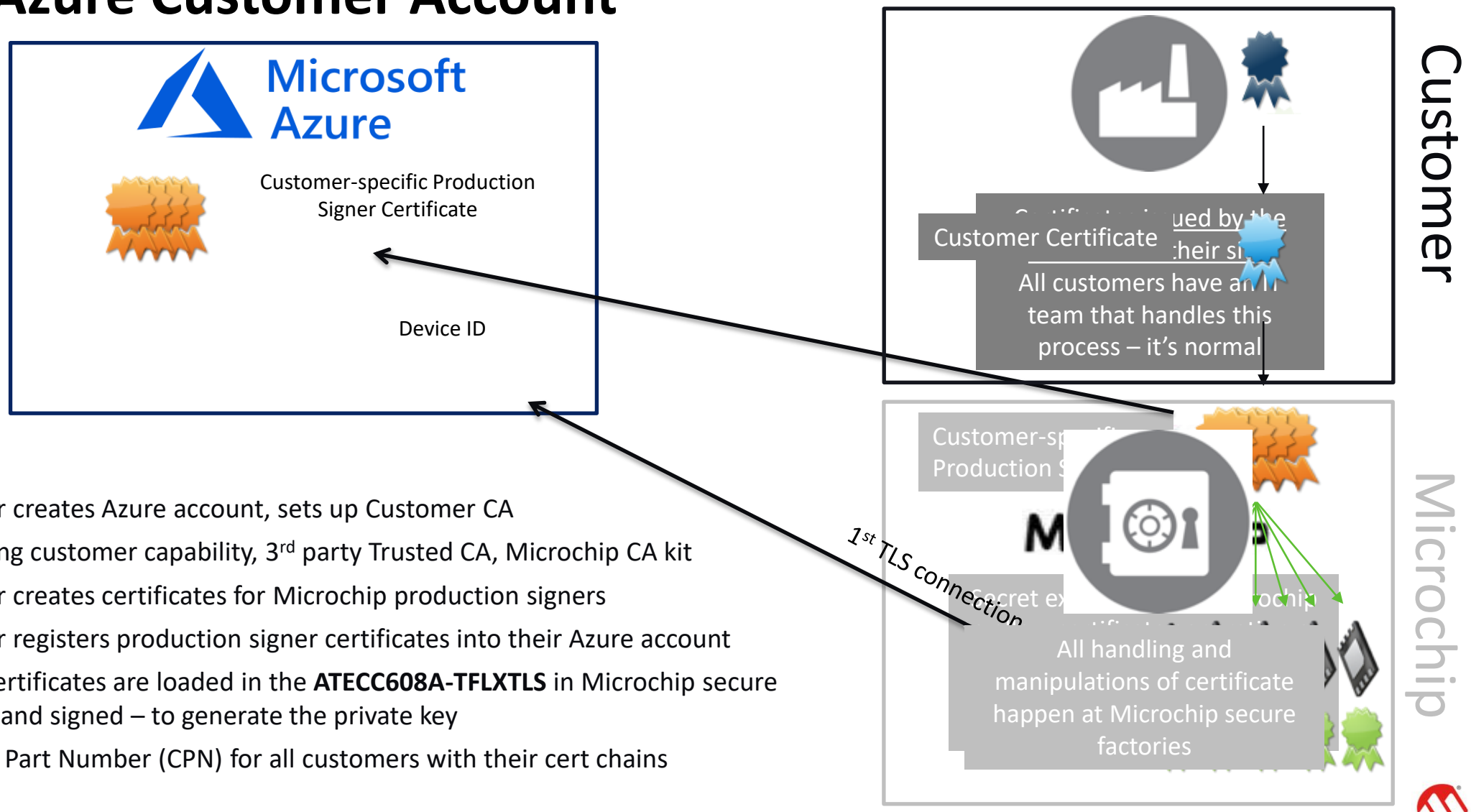
- ✓ **Start with pre-configured device policies**
- ✓ **To be provisioned with customer credentials**
- ✓ **Cover all the most common use cases**
  - ✓ Certificate authentication
  - ✓ JWT authentication
  - ✓ Secure Boot assistance
  - ✓ OTA verification
  - ✓ IP protection
  - ✓ Message encryption
  - ✓ Key rotation
  - ✓ I/O protection key
- ✓ **Low MOQ (2ku)**
- ✓ **Shortened development time**
- ✓ **Low complexity**
- ✓ **JIL-rated high key storage**



MICROCHIP

TrustFLEX with 3rd Party PKI Authentication on Azure

Azure Customer Account



1. Customer creates Azure account, sets up Customer CA
   - Existing customer capability, 3rd party Trusted CA, Microchip CA kit
2. Customer creates certificates for Microchip production signers
3. Customer registers production signer certificates into their Azure account
4. Device Certificates are loaded in the **ATECC608A-TFLXTLS** in Microchip secure factories and signed – to generate the private key
5. Standard Part Number (CPN) for all customers with their cert chains

MICROCHIP

Turning Months of Development to Minutes

Trust Platform Design Suite

1 Define

Map use case to configuration

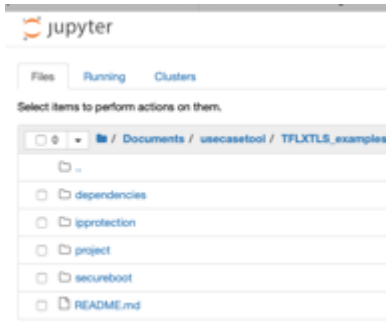
Use Case Tool

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

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

MICROCHIP

Hands-on

For prototyping only:

- **Install Trust Platform Design Suite (microchip.com/TrustPlatform)**
- **Generate manifest and upload it to Microsoft Azure IoT Hub using leveraging the Trust Platform Design Suite software**
- **Update the WINC1500 firmware**
- **Flash the provided code example in the SAMD21 microcontroller**
- **Connect to Microsoft Azure IoT Hub**

For production:

- **Start with the ATECC608A-TFLXTLS-proto from your e-commerce store**
- **Trigger the secret exchange process**
- **Get the manifest file from your e-commerce account**
- **Go to production with your custom ATECC608A-xxxxx**

Trust Platform Development Kit

+

DM320118

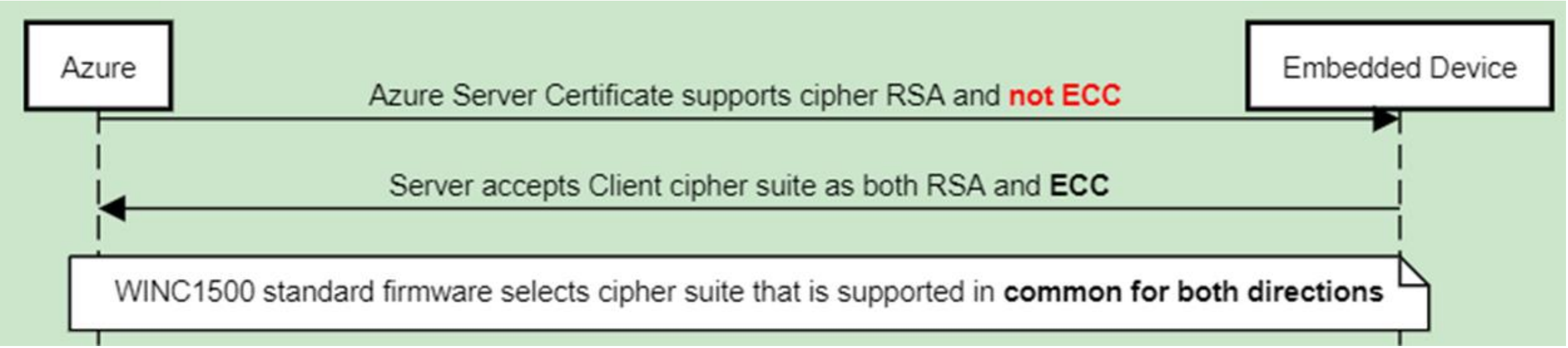
- Arm® Cortex® M0+ SAMD21
- ATECC608A Trust&GO, TrustFLEX, TrustCUSTOM
- Debugger

WINC1500

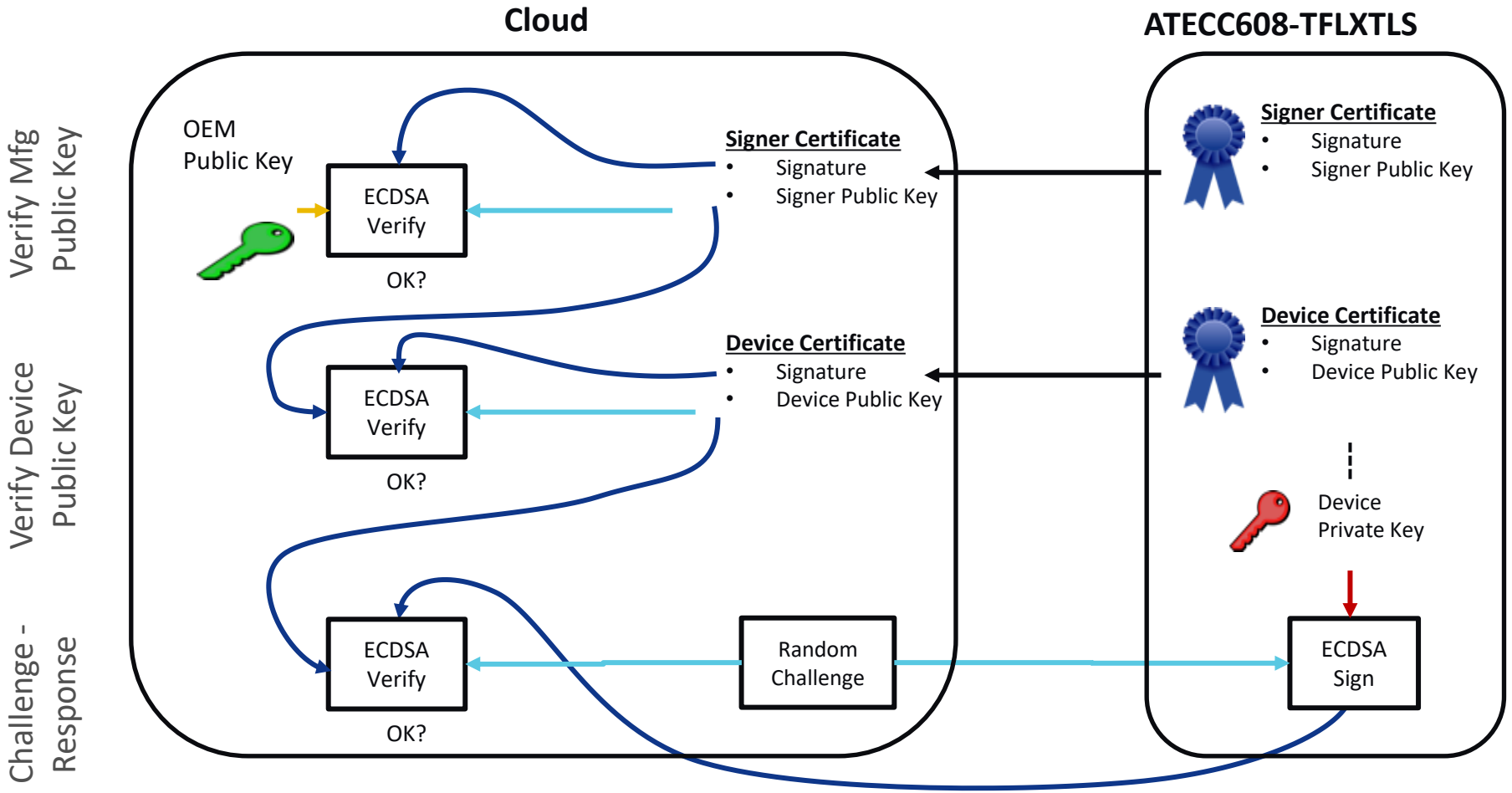
- Wi-Fi b/g/n
- Integrated TLS and TCP/IP stacks
- MikroBUS™ pinout
- Mikroe.com

MICROCHIP

Cipher Suites and Azure

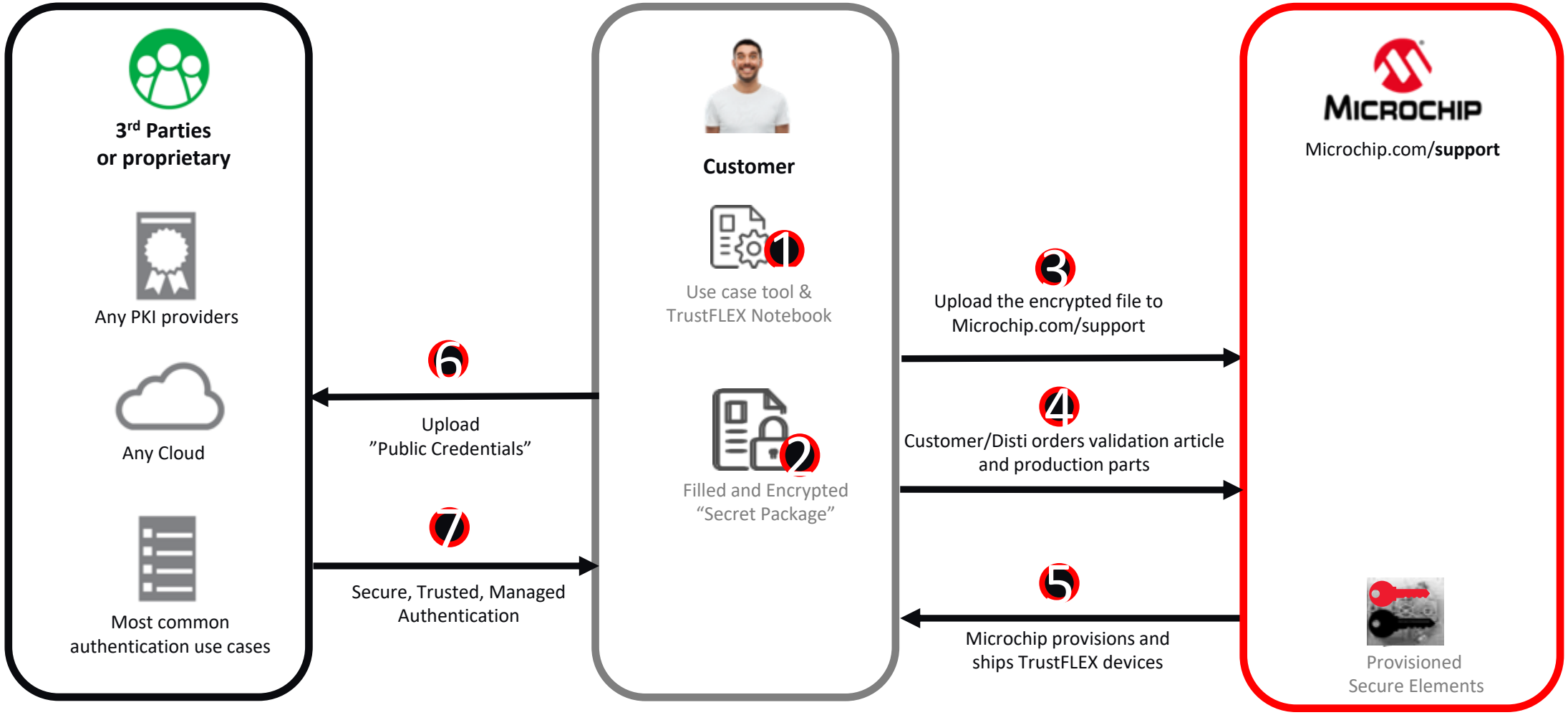


Azure IoT Authentication with Custom PKI



MICROCHIP

Production Ordering Flow



Microsoft Azure Device Provisioning Service (DPS)

1. Help bulk uploading public keys in the Azure environment
2. Register the device public key to DPS first
3. DPS will authenticate with the targeted Azure IoT Hub
4. Azure IoT will provision the register statuses of the embedded device with the desired state
5. Watch Microchip Livestream with Microsoft expert
   youtube.com/watch?v=g1Ndy7mOUp0

MICROCHIP

Challenges

1. **Time to configure the secure authentication use cases in the device**
2. **Logistic complexity of securely provisioning keys and credentials:**
   - Shipping keys globally for any project size
   - Keep keys isolated from everything
   - In a fragmented marketplace

Solutions

1. **Trust Platform Design Suite software turn months of development into minutes**
   - Trust&GO: pre-provisioned
   - TrustFLEX: pre-configured
   - TrustCUSTOM: fully customizable
2. **Logistic simplicity with the Microchip Trust Platform**
   - Ships globally under EAR99 export rules
   - No more high volume MoQ limitations
   - Ideal service for today fragmented market
   - Gives everyone access to secure authentication

Thank You