Pre-provisioned Secure Elements: Onboarding with Trust&GO for AWS IoT

Presenter: Brett Kim – Senior Embedded Solutions Engineer

MICROCHIP

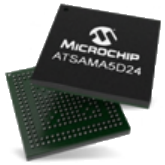
Embedded Security Snapshot

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

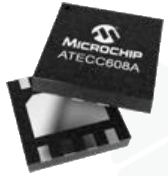
Application layer security	Leverage cryptographic capabilities of the system to further harden the implementation (access rights - privileges)
Secure Connectivity	Authenticate and encrypts the device communication
Secure update	Leverage secure communication and secure boot mechanisms to ensure safe delivery 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

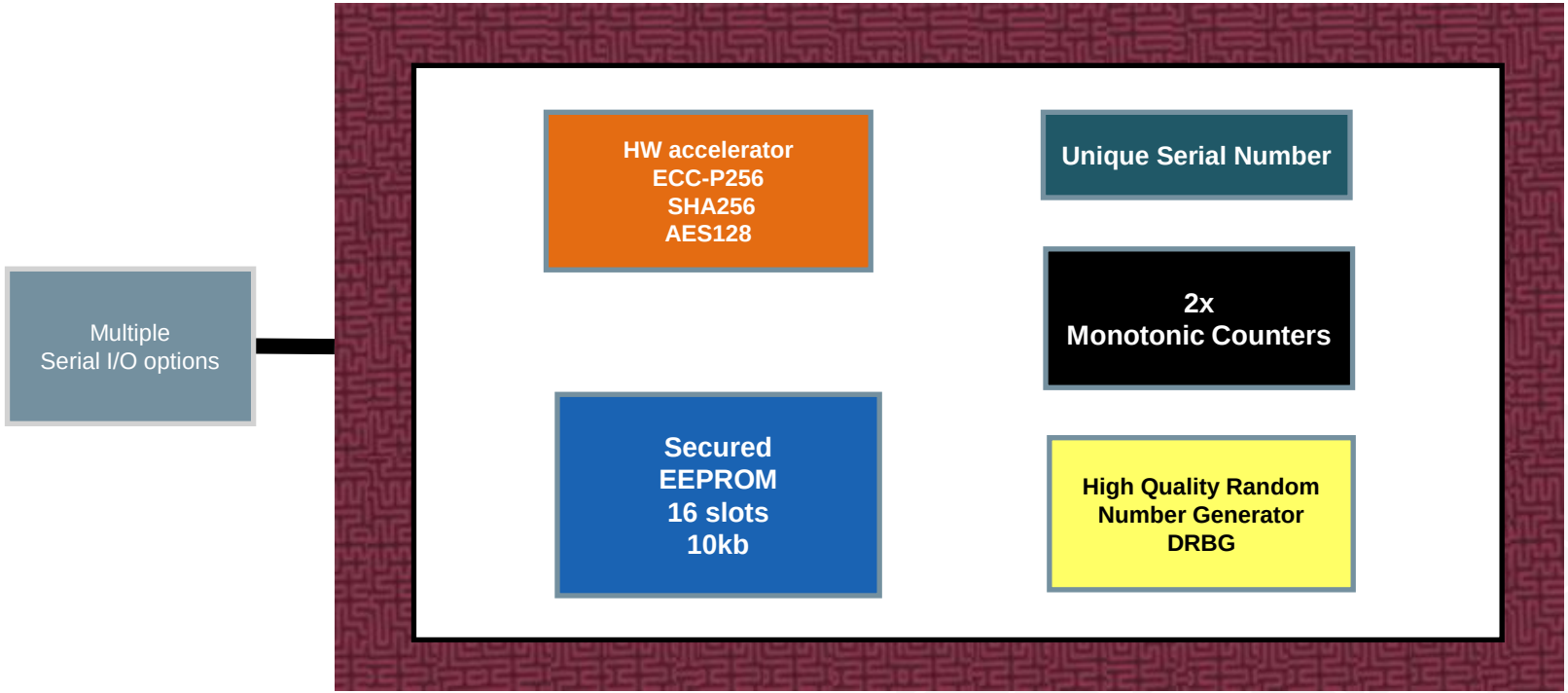
What a private key really looks like
JVFDvdfvJvfdnjvjk543524cds9ics9cCDSCcs0dcw8eidpciswsn8934XSCDS

The Enemy Knows the System

Claude Shannon

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

ATECC608 Isolates keys in Hardware



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

MICROCHIP

Onboarding with Trust&GO for AWS IoT

+

MICROCHIP

The Value

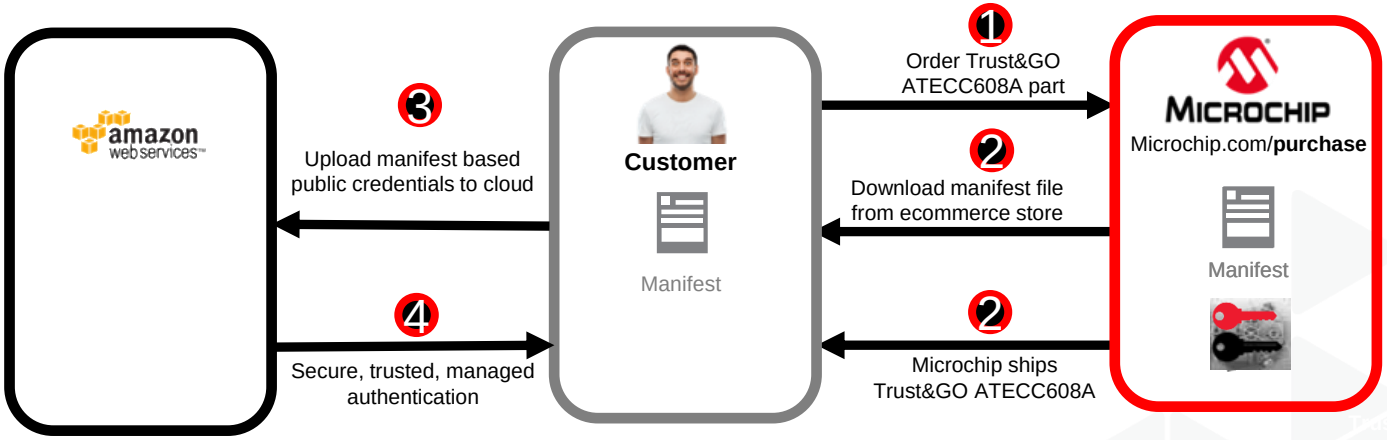
Trust&GO

- No need to purchase a Certificate Authority
- No need for device customization
- Black box secure element + certificate and keys pre-provisioned
- Very short lead time for a provisioned device (less than 4 weeks)

AWS multi-account registration

- Device transfer from Staging to Production AWS account during manufacturing
- Company to company change of ownership
- Connection routed based on SNI (Server Name Indication)
- Register the device certificate in multiple accounts (even across regions) and when device connects
- Load balance as device volume grows by moving some of the devices to another account owned by same company

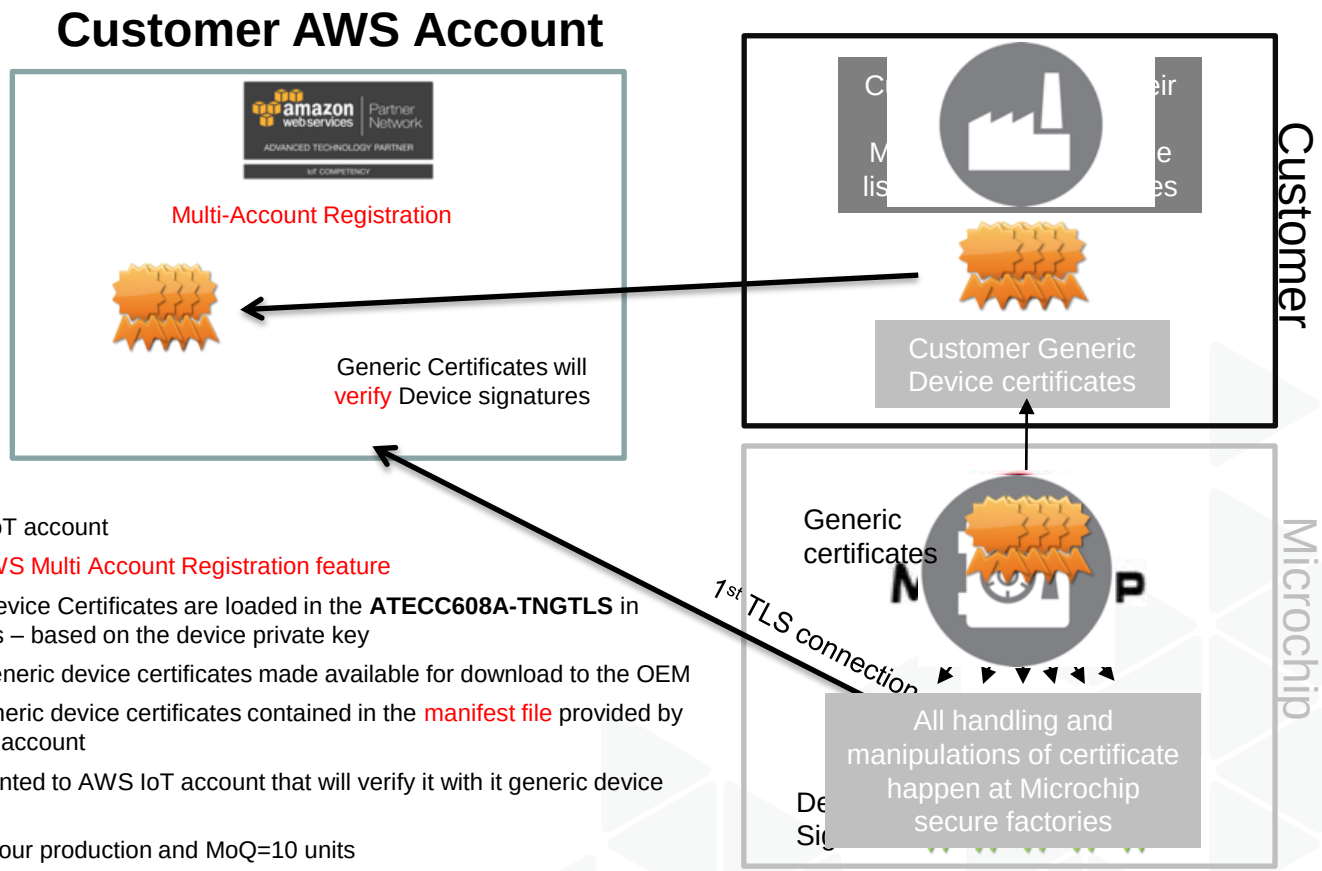
Trust&GO:
Simple Ordering Process



TRUST &GO

MICROCHIP

AWS IoT Use Case



1. Customer creates AWS IoT account
2. Customer has natively AWS Multi Account Registration feature
3. Customer place order - Device Certificates are loaded in the **ATECC608A-TNGTLS** in Microchip secure factories – based on the device private key
4. Manifest file containing generic device certificates made available for download to the OEM
5. Customer bulk upload generic device certificates contained in the manifest file provided by Microchip into their AWS account
6. Device Signature is presented to AWS IoT account that will verify it with it generic device certificate
7. No CPN needed to start your production and MoQ=10 units

Hands-on

For prototyping :

- Install Trust Platform Design Suite (microchip.com/TrustPlatform)
- Generate manifest and upload it to AWS IoT from the Trust Platform Design Suite
- Update the WINC1500 firmware
- Flash the provided code example in the SAMD21 microcontroller
- Connect to AWS IoT

Hands-on

For prototyping :

- Install Trust Platform Design Suite (microchip.com/TrustPlatform)
- Generate manifest and upload it to AWS IoT from the Trust Platform Design Suite
- Update the WINC1500 firmware
- Flash the provided code example in the SAMD21 microcontroller
- Connect to AWS IoT

For production :

- Order the ATECC608A-TNGTLS from your e-commerce store
- Get the manifest file from your e-commerce account
- Go to production

Step 1

Install the Trust Platform Design Suite Software

&

Go to the start menu and click on “Start_Here”

Step 2

Buy the following hardware

- DM320118 containing the SAMD21 microcontroller and all the Trust Platform secure elements: Trust&GO, TrustFLEX, TrustCUSTOM

- The WINC1500 click board from mikroe.com as indicated on our website.

Step 3

Build a manifest file from the Trust Platform Design Suite for prototyping only

Step 4

Update the WINC1500 firmware

Step 5

Setup your AWS account

&

Load the manifest file

Step 5

Setup your AWS account

&

Load the manifest file

Step 6

Flash the AWS IoT Trust&GO project in the SAMD21

&

Make sure to setup the hotspot credentials

Production step

How to order Trust&GO ATECC608 for production ?

Recap

Turning months of development into minutes

- **Microchip Trust&GO ATECC608**
  - **Pre-provisioned** secure element with no secret exchange needed
  - Simple ordering process
  - Cost effective certificate solution
- **AWS Multi-Account Registration feature**
  - Easy device onboarding to AWS IoT avoiding certificate authority verification
  - Scalable load balancing and smooth transfer of ownership
- **Turnkey hardware :**
  - SAMD21 ARM® Cortex®-M0+
  - WINC1500 Wi-Fi
  - ATECC608 secure element to protect the private key
- **Turnkey secure mutual authentication**
  - bare metal code example for AWS IoT Core

MICROCHIP

Thank you

microchip.com/**TrustPlatform**