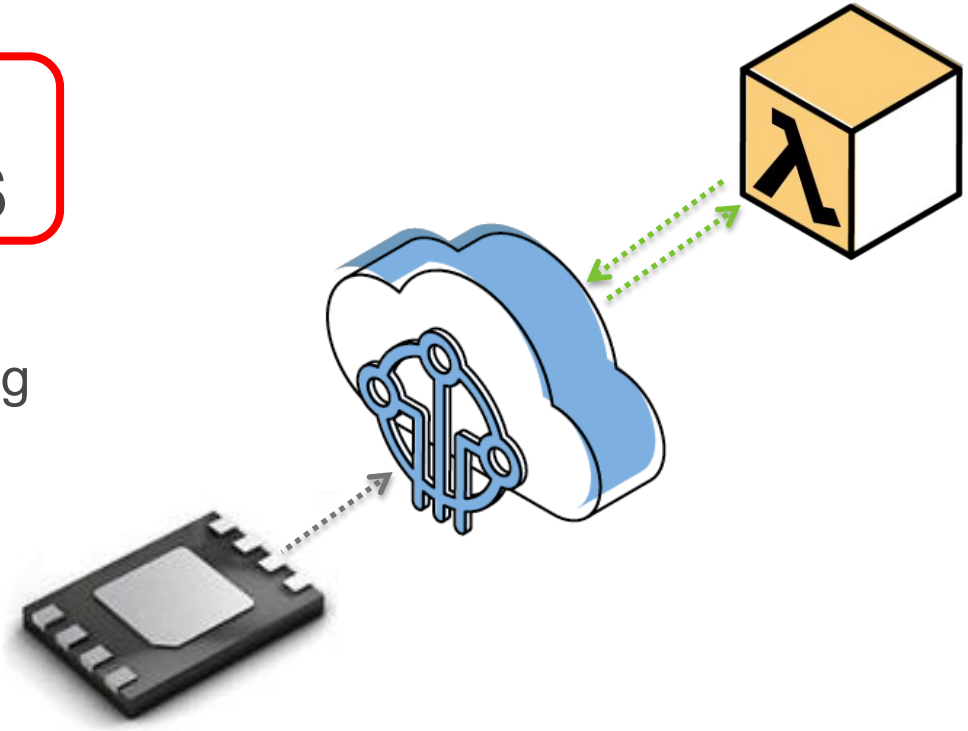
Strong turnkey security

Microchip/Atmel ATECC508A-AWS

Encapsulate the entire provisioning process into a turnkey IC

Focus design effort on customer experience



IoT device identity requirements

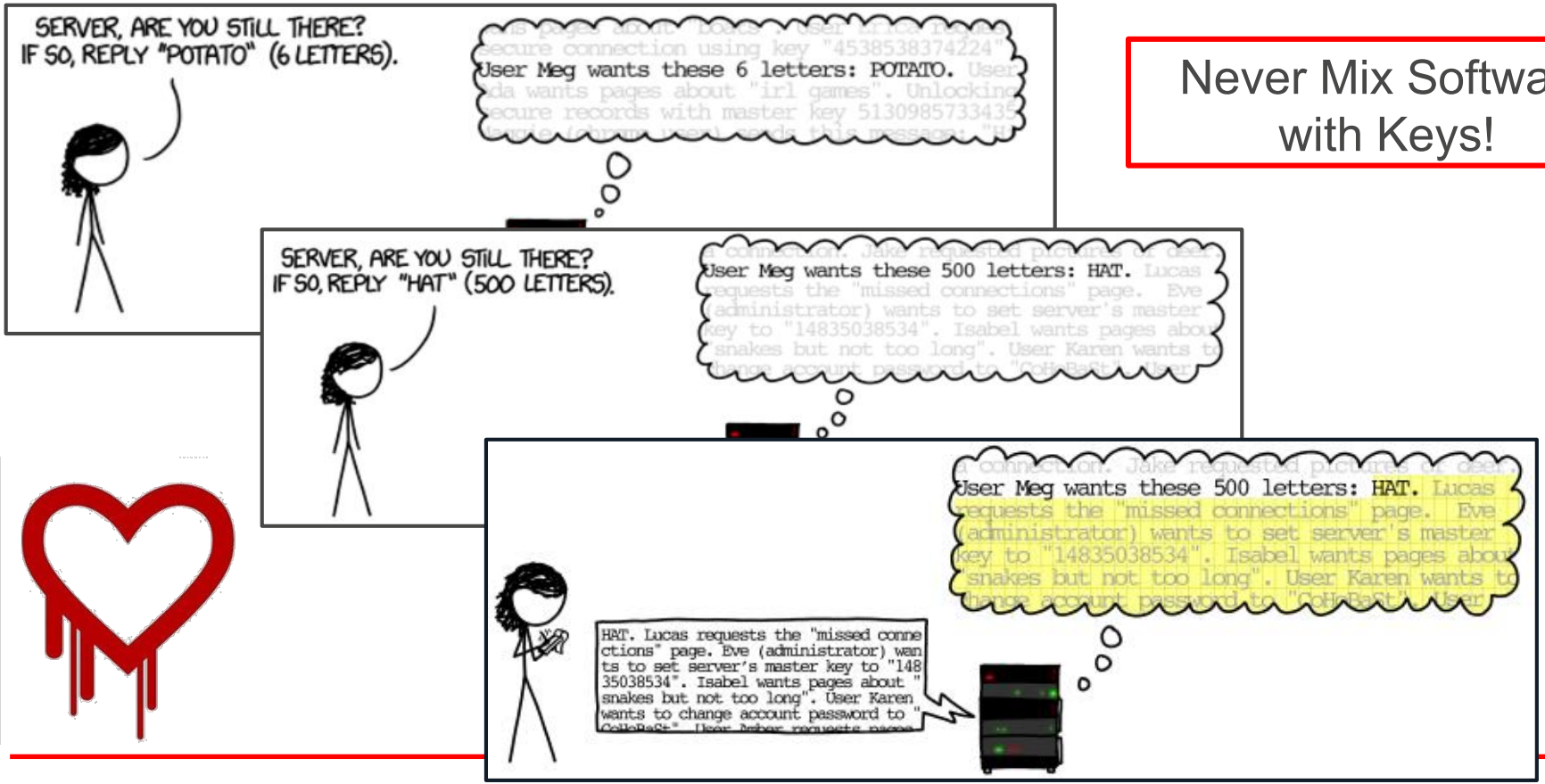
Every device must have a Trustable Identity

Private key can never be revealed!!!

Authenticate every entity with which you communicate

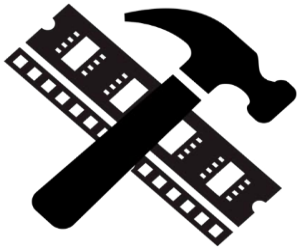
Authentication Process must be trusted

Perfect software exists in theory only



Never Mix Software with Keys!

Attackers don’t need physical access!



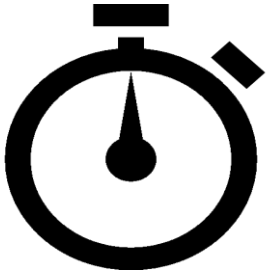
Rowhammer

Modify DRAM state to gain kernel privileges

Acoustic Cryptanalysis

Listen to component vibration across room, extract keys

http://www.tau.ac.il/~tromer/acoustic/



Timing Attack (First published in 1996)

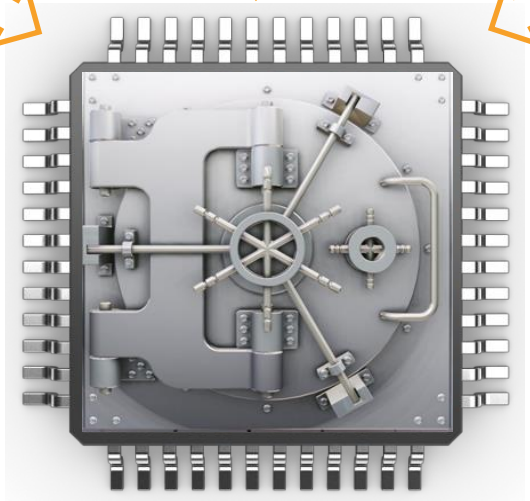
Extract confidential data based on response delay

Get critical stuff out of the micro!

Keys

Passwords

Elliptic Curve FW



High security key storage

Root of trust for secure code

10x-100x faster than MCU

Less code = Lower cost

ATECC508A-AWS

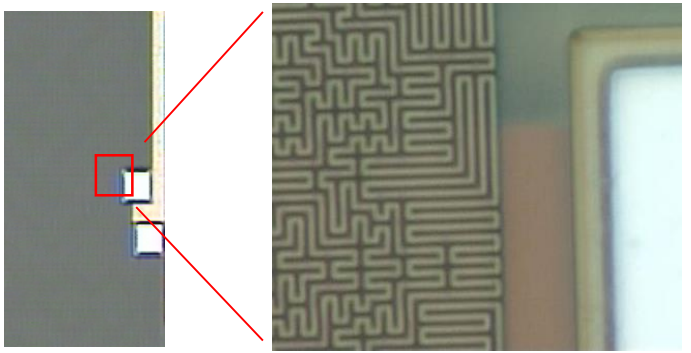
What makes ATECC508A a vault?

Advanced Security Circuitry

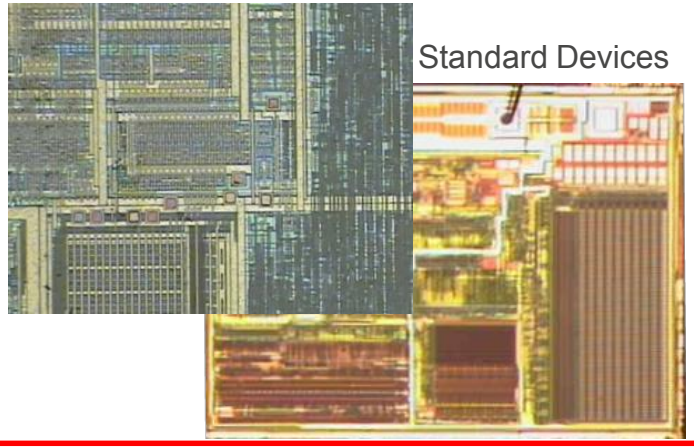
Active shield, internal encryption, randomization, tampers, no JTAG, …

Strong attack defenses

Microprobe, Timing, Emissions, Faults, Glitches, Temperature



Microchip Security Devices



Standard Devices

Comprehensive thing security

Keys never leave chip - No back doors!

Software asks for keys to be used - chip accelerates math using the key

Elliptic curve algorithm in hardware – can’t exploit software bugs!

Secure in the factory

Private key generated entirely inside the ATECC508A

- Completely random
- NEVER readable
- NEVER known by anybody

Certificates generated by world-class HSMs at Microchip

- Protected in State-of-the-art Secure Facilities

No special equipment or procedures required in the OEM factory

Microchip's factory provisioning

Secure Facilities

- 24/7 camera monitored, locked cages, network isolation, physical access control

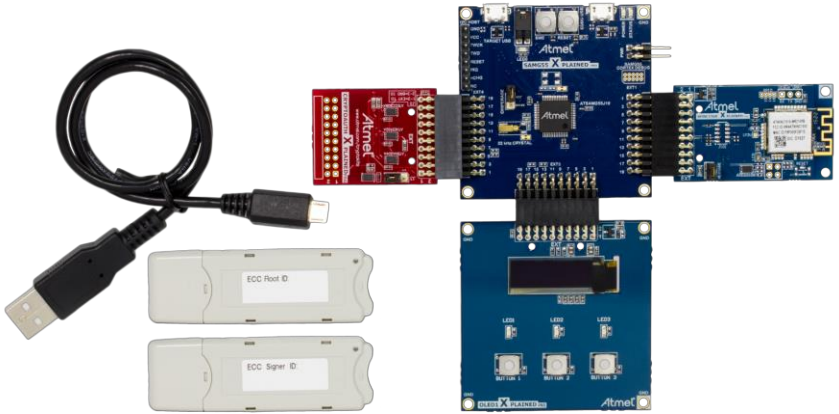
Hardware Secure Modules (HSM)

- Highly secure computers, World class certifications : FIPS 140-2, CC EAL 4+, …

Easy to get started

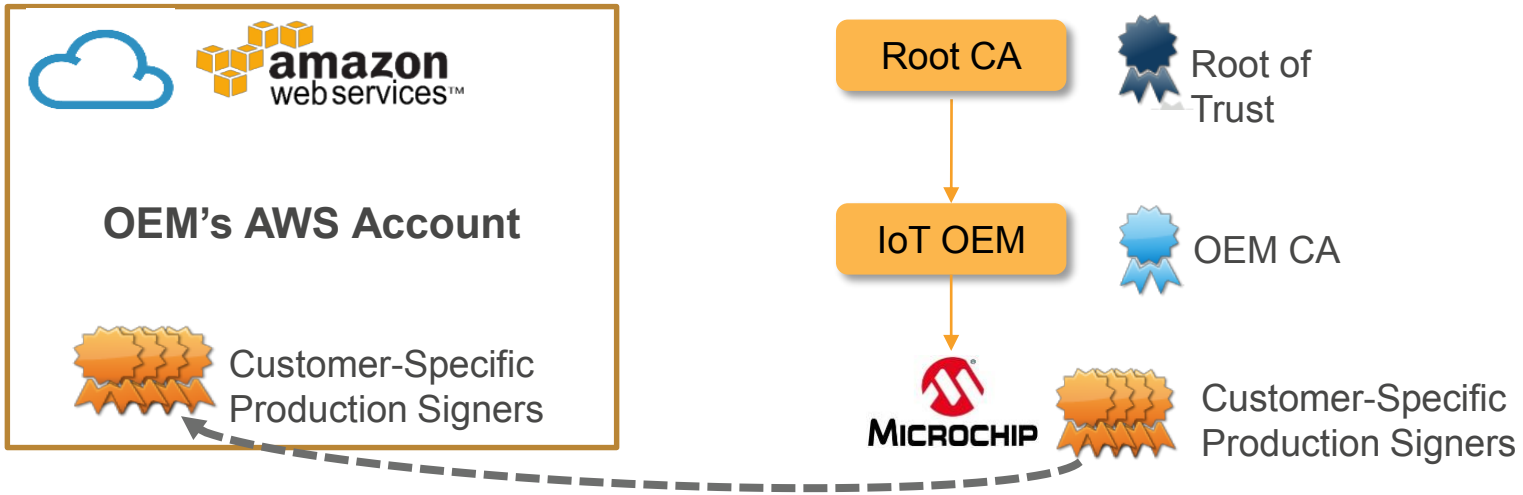
Reference design

- ARM® Cortex®-M4 microcontroller
- Wi-Fi® connectivity
- ATECC508A pre-configured for AWS IoT
- I/O module
- Root CA & Intermediate CA demo dongles
- FreeRTOS
- WolfSSL TLS 1.2
- MQTT client
- JSON library
- Example Application with 6 I/Os



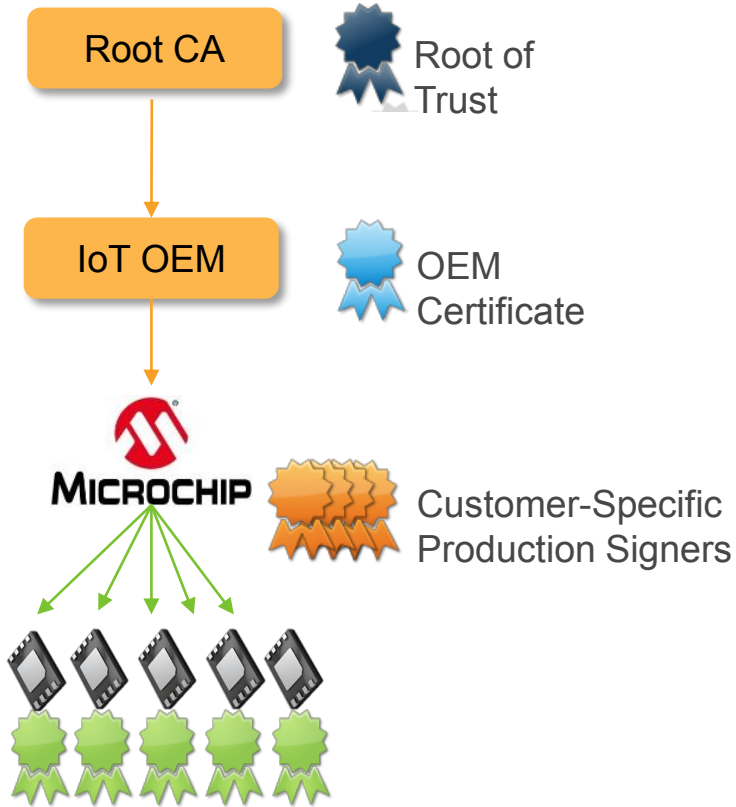
Source code & Documentation on GitHub:
https://github.com/MicrochipTech/AWS-Secure-Insight

Easy OEM setup



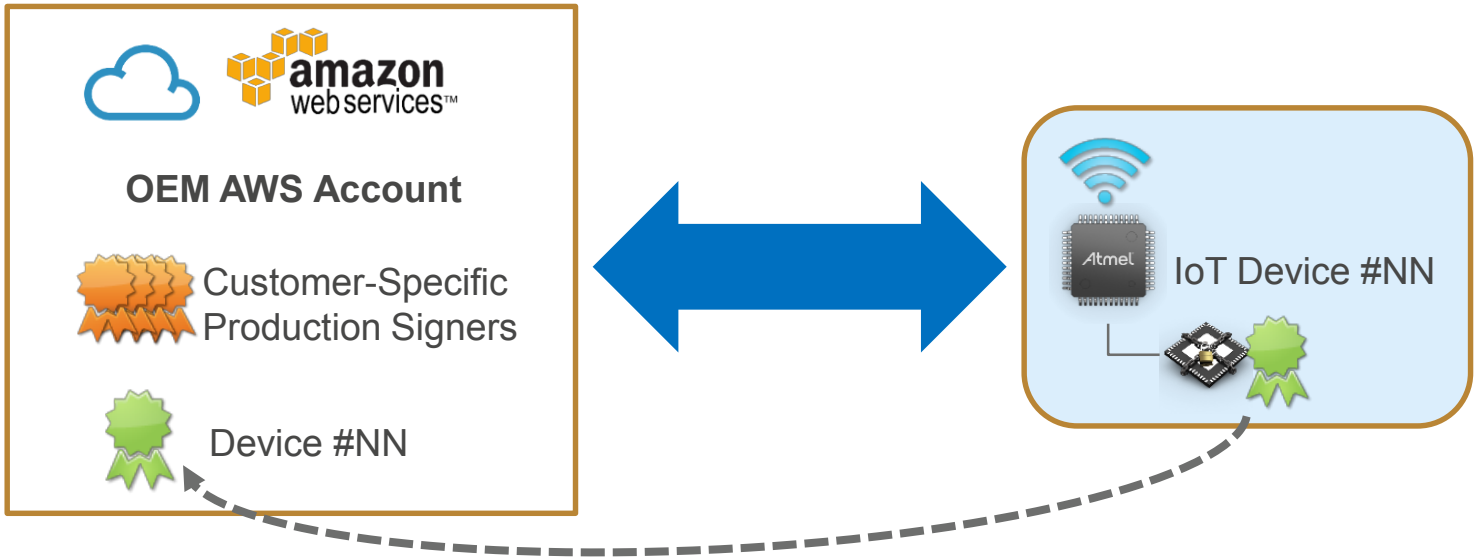
1. OEM creates AWS IoT account, sets up OEM CA
   Existing OEM capability, 3rd party Trusted CA, Microchip CA kit
2. OEM creates certificates for Microchip production signers
3. OEM registers production signer certificates into their AWS account

Zero touch provisioning - Manufacture



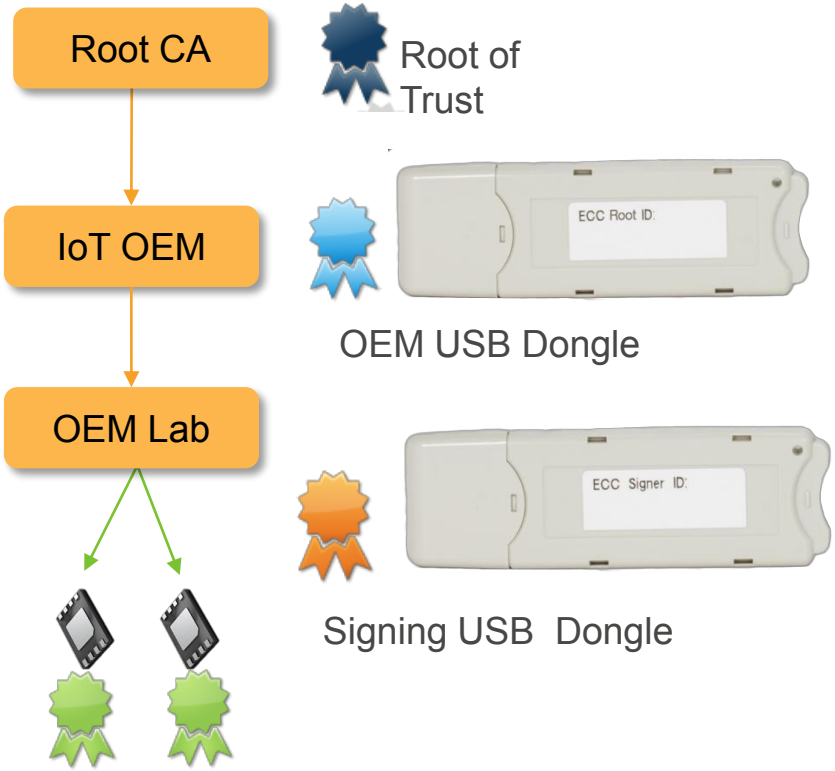
1. **Microchip ships ATECC508A including certificates to board shop**
2. **IoT provisioning easy : assemble ATECC508A into IoT product**
3. **Final product ships with little or no cloud enrollment instructions or actions needed**

Zero touch provisioning - Field



Device certificate automatically transferred to AWS and registered on first connection

Easy prototyping



1. **Development kits readily available from distributors**
2. **Includes turnkey USB dongles set up to model the OEM CA and the Microchip production signers**
3. **Use to create demonstration systems and alpha units for testing and qualification**

Easily secure your AWS IoT device

Secure Keys - Ultimate protection for keys to prevent any software attack, accelerate ECC up to 100x faster

Fast Design - Prototyping kits available now, complete reference design on the web, tiny package fits any system

Easy Manufacturing - Secure and seamless manufacturing logistics. JITR means Ready-to-Go with AWS out of the box

ATECC508A-AWS