Avnet Silica – Security Services

Secure provisioning capabilities

AVNET SILICA

Main stake of IoT Security

IoT Security implies the use of good practices in term of **products, developments** but it implies also **to reduce opened doors, and provisioning** is one of them.

NEEDS

- Certification Authority
- Sub-CA per projects
- Unique ID
- Unique keys

CHIP MANUFACTURERS

- Provide generic CA
- Very High volumes for customization

EMS SERVICES

- Not equipped with HSM
- Lack of secure channel to communicate
- Difficulty to define TCO

SECURITY CONCERNS

- Security mechanism
- Authentication mechanism
- Integrity mechanism
- All manipulated by EMS

Secure provisioning by Avnet Silica

On top of MCU, Memory, MPU and Secure elements Avnet Silica is providing Secure provisioning services. It consists of

Keys generation

Secure Firmware programming

Device certificate creation

HSM

Root certificate

Fulfilling suppliers offering

Public key injection

TCO clearly identified

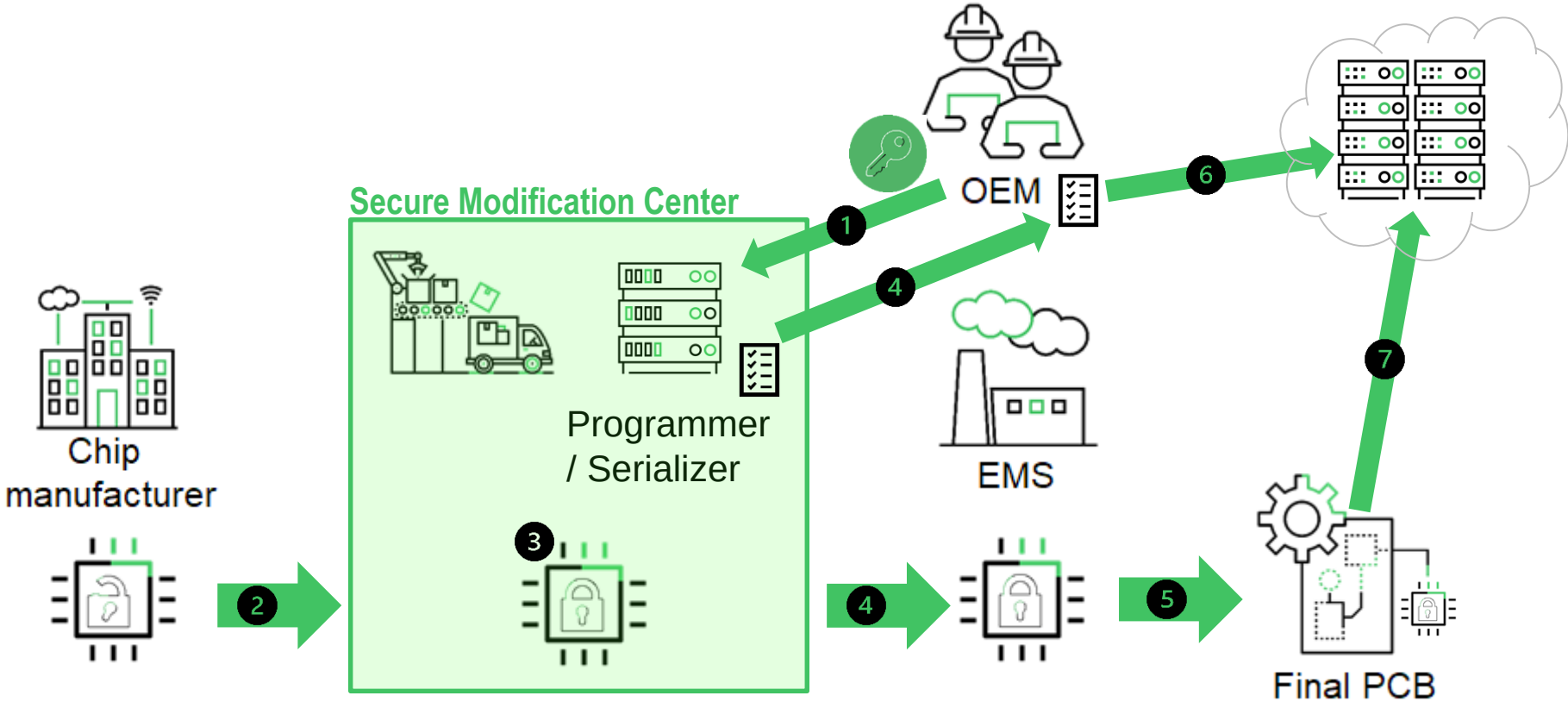
Secure programing machine

Secure programing area

AVNET SILICA

Use cases

Secure Provisioning General Principle



1 – Provisioning for IoT Cloud Platforms

They all required the same kind of process:

Device

- Certificate creations or loaded
- Keys generation
- Public key injection
- Private key

Cloud

- White List
- Credentials provisioning
- Identity provisioning
- Certification authority

Methods:

- X.509 certificates
  - Public/Private keys
  - Certificate in both sides
- Symmetric keys
  - Same keys on both sides

2 – Provisioning for specific Standard/Consortium

They required a specific PKI based authentication

- **OEM is using secure channel** to load its credentials into Secure programing machines
- **Avnet Silica** inject X.509 certificates into the device and associated keys
- **Certificate must be loaded on both side,** device and cloud and will be used in TLS connection for client authentication
- **Avnet Silica inject Public key of Trusted CA (Standard/Consortium),** so that devices can authenticate their peers

matter

CHARGING CONSORTIUM

AVNET SILICA

3 – Provisioning for IP Protection

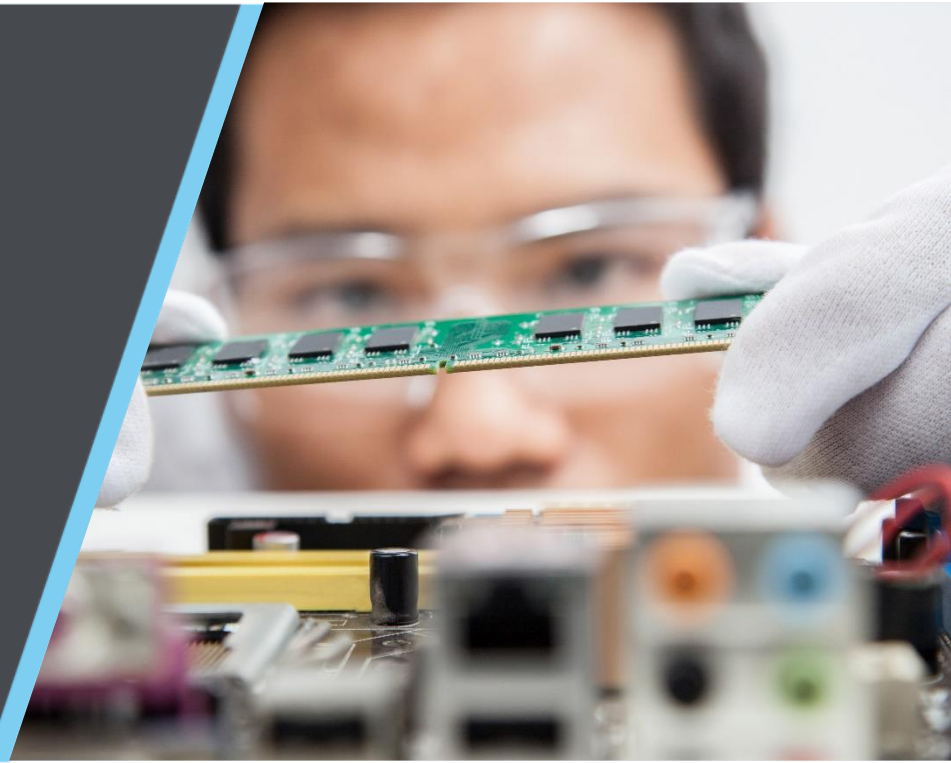
Some OEMs want to protect their IP from theft at manufacturing…

- **Avnet Silica provisioning capabilities can offer several options**
- **Program the components with the final Firmware and lock the components with readout protection. (Implies the FW is available when shipping components)**
- **Program the components with a Secure Boot Loader. Implies injecting a secret key for firmware encryption in the bootloader. Implies encrypting the firmware before sending it to the EMS. Implies injecting a secret key for firmware encryption in the bootloader**

4 – Provisioning for Secure Boot / Secure FOTA

FOTA is very convenient if not mandatory…And it MUST be done in a secure way

- **FOTA payload must be protected during transport**
- **FOTA payload must be authenticated, and integrity protected**
- **This can be achieved by asymmetric crypto**: Private key is kept by developer of the FW (RSA or ECDSA), FW signed with this key, matching public key must be loaded into each device to verify signature
- **Or by symmetric crypto** a secret key kept by developers. FW signed with this key (CMAC or HMAC). This secret key has to be programmed into each device.



Thank You