Trust Platform Design Suite v2 Overview and Update

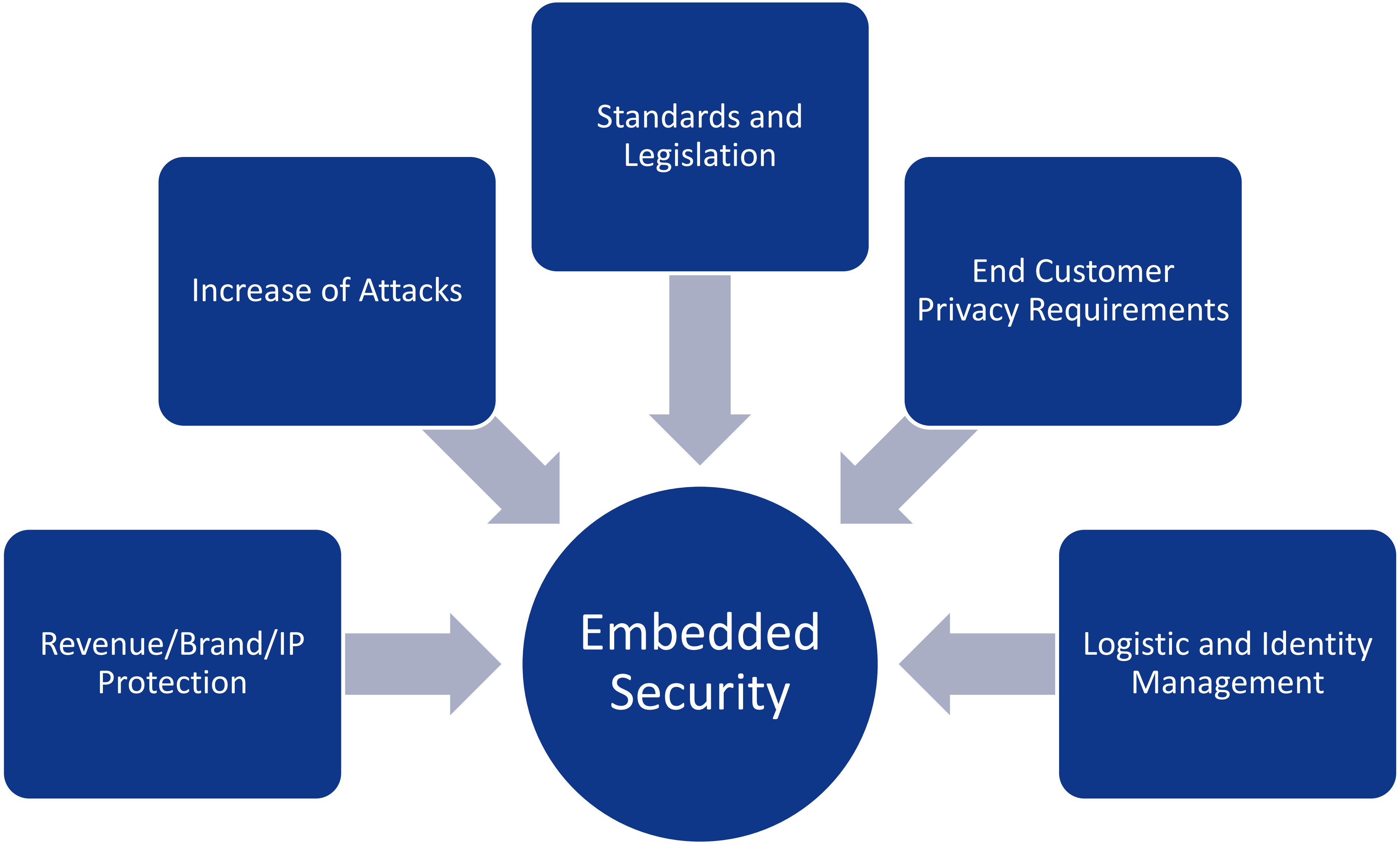
A Leading Provider of Smart, Connected and Secure Embedded Control Solutions

엄명흠(MH Eum) 책임, Sr. Embedded Engineer

July 12, 2022

SMART | CONNECTED | SECURE

Why Embedded Security?



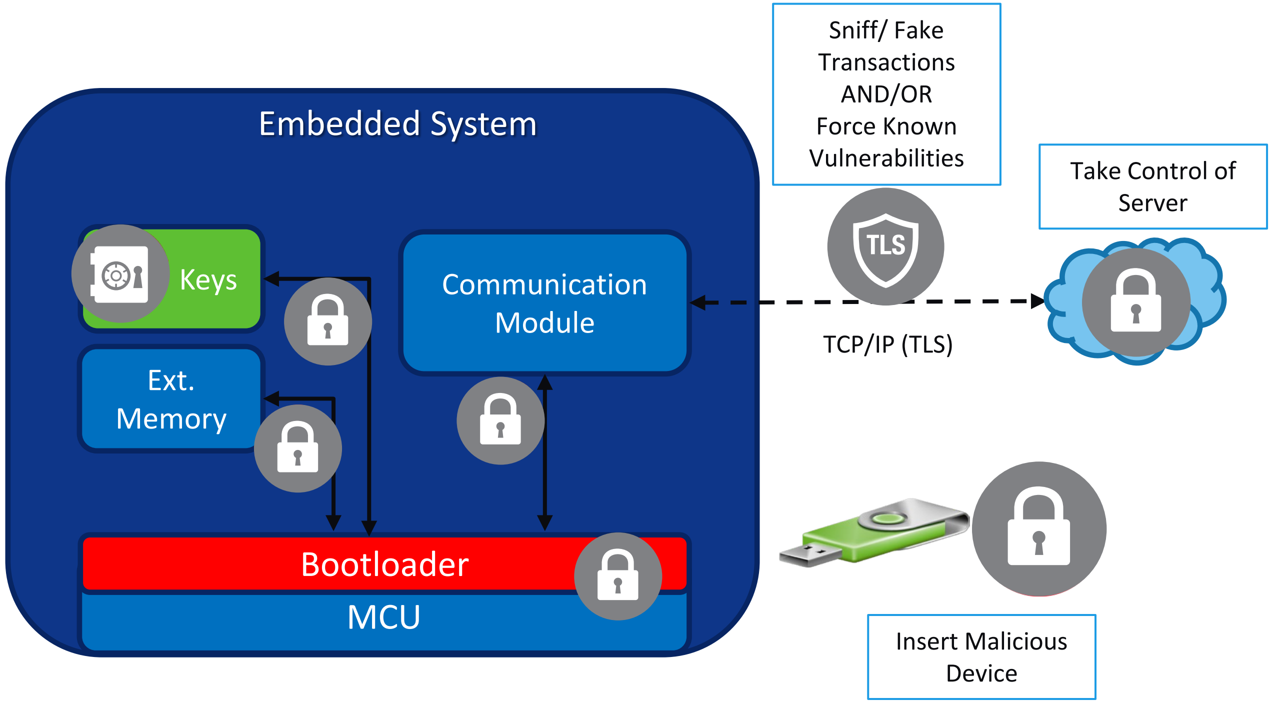
Anatomy of a Secure Embedded System

Threat Modelling

Developing Hack-Resilient Systems

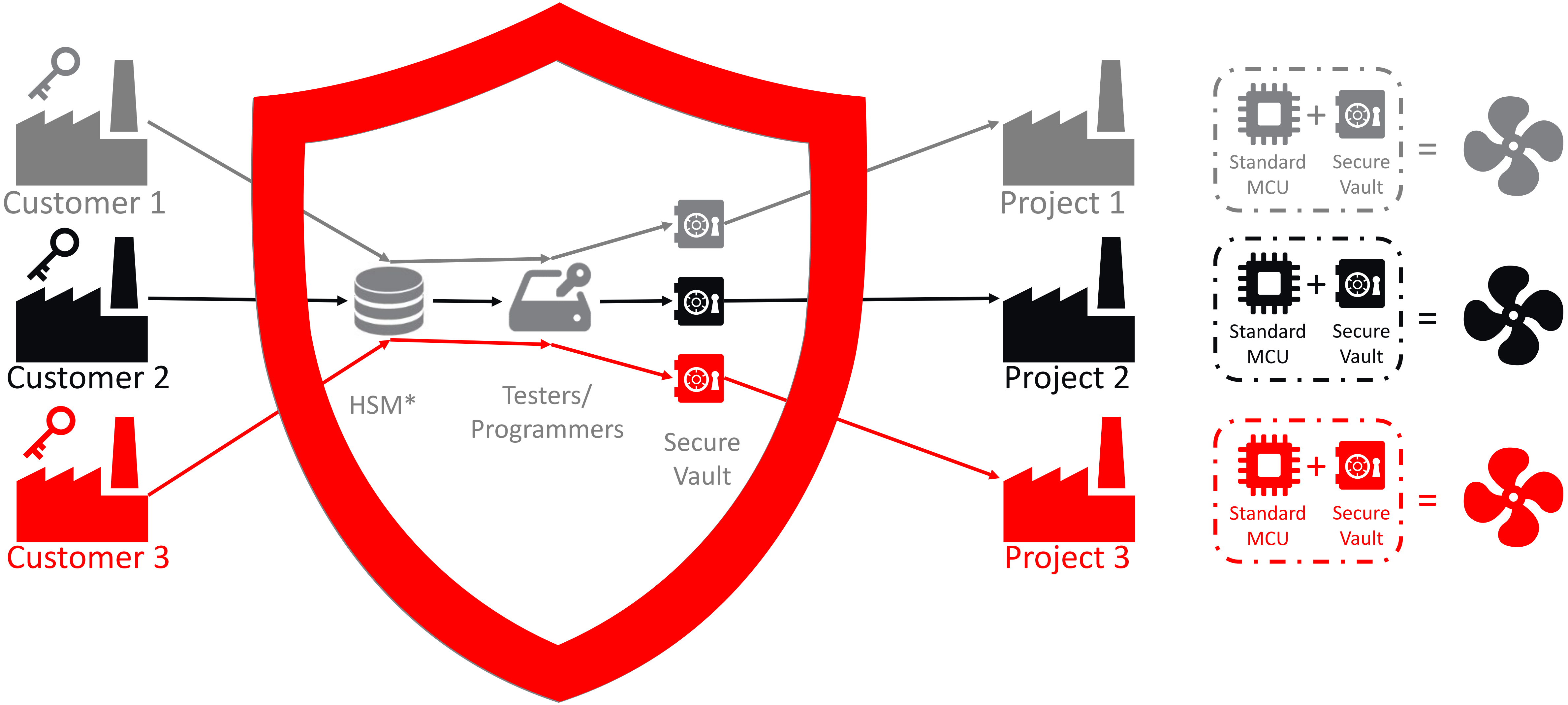
- Define system requirements
- Risk analysis

→ Security implementation



Next step: How to secure manufacturing?

Secure Provisioning (Customization)



*HSM: Hardware Security Module in isolated network and dedicated secure rooms

MICROCHIP

How Can Microchip Help?

Concept Prototyping
- Cybersecurity requirements
- Cost and time constraints (Iron triangle)
- Threat analysis

Development
- Hardware integration
- Software integration
- Cloud integration

Production
- Key and certificate provisioning
- Distribution and logistics

Utilization
- End user activation
- Operation
- Sensitive data handling

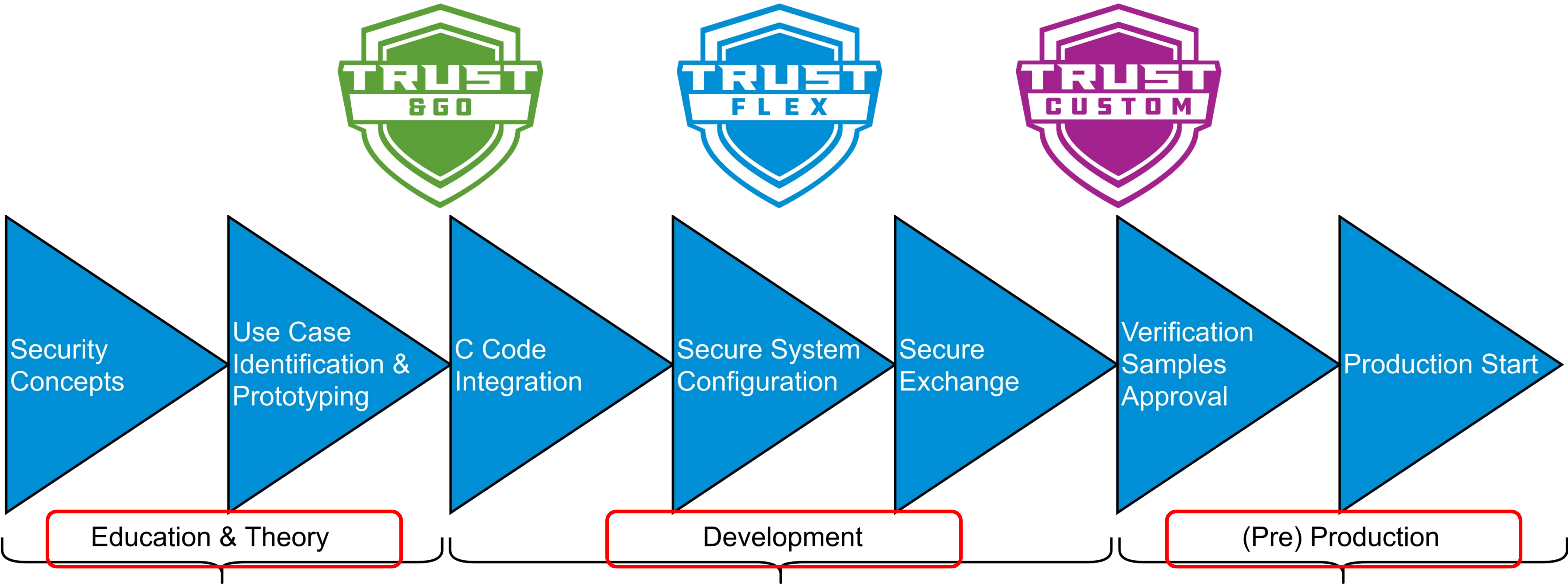
Support
- Software updates
- Vulnerability management

Retirement
- Sensitive data management
- Device recovery and repurpose

Trust Platform

Trust Platform Design Suite v2

The Journey to Success



MICROCHIP

Trust Platform Design Suite v2

Learning Center

Welcome to the Trust Platform Design Suite Learning Center on Security

In the below videos, you will find all necessary information to onboard with embedded system security as well as dedicated training for specific Use Cases. Please reach out to Microchip if you want us to develop new content.

Cryptography Primer (part 1)	**Embedded Security Principles**
Cryptography Primer (part 2)	**Confidentiality, Integrity, Authentication**
Cryptography Primer (part 3)	**Hashing**
Cryptography Primer (part 4)	**Asymmetric Authentication**
Cryptography Primer (part 5)	**Chain of Trust**

MICROCHIP

Trust Platform Design Suite v2

Select Your Security Solution

Use Cases (Mandatory)

- AWS IoT Authentication
- Azure Authentication
- GCP Authentication
- Firmware Validation
- Firmware Upgrade Validation
- Custom PKI AWS
- Custom PKI Avnet IoTConnect

Application Category (Optional)

- Accessory Authentication
- Disposable Authentication
- IoT
- Automotive

Product Category (Optional)

- Secure Elements

Available solution by provisioning flow

Trust&GO

No products under Trust&Go are available based on the selection

TrustFLEX

ATECC608B-TFLXTLS

Usecase | Configurator

TrustCUSTOM

ATECC608B-TCSM

Configurator

TA100-VAO

Configurator

MICROCHIP

Trust Platform Design Suite v2

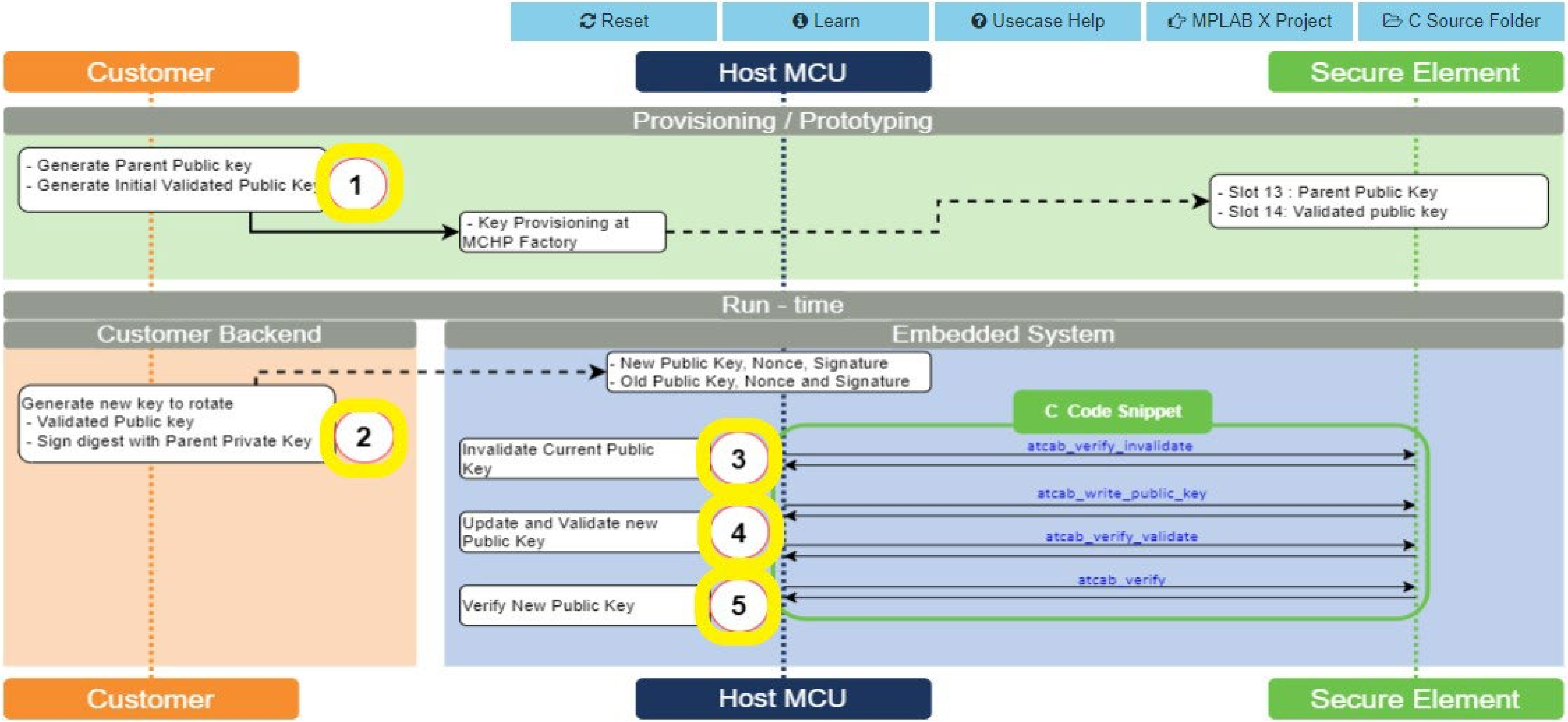
Cryptographic Asset List and Use Case Implementation

Slot #	Description
Slot 0	Primary private Key
Slot 1	Internal sign private key
Slot 2	Secondary private key 1
Slot 3	Secondary private key 2
Slot 4	Secondary private key 3
Slot 5	Secret key
Slot 6	IO protection key
Slot 7	Secure boot digest
Slot 8	General data
Slot 9	AES key
Slot 10	Device compressed certificate
Slot 11	Signer public key
Slot 12	Signer compressed certificate
Slot 13	Parent public key or general data
Slot 14	Validated public key
Slot 15	Secure boot public key

Step	Use Case basic Steps	Where / When
1	Generate a Validation Authority Key pair	At customer premises
2	Generating new rotating Public Key	At customer premises
3	Invalidate current key in the slot	Inside Secure Element
4	Update and Validate new Public key	Inside Secure Element
5	Verify the rotated Public key	Inside Secure Element

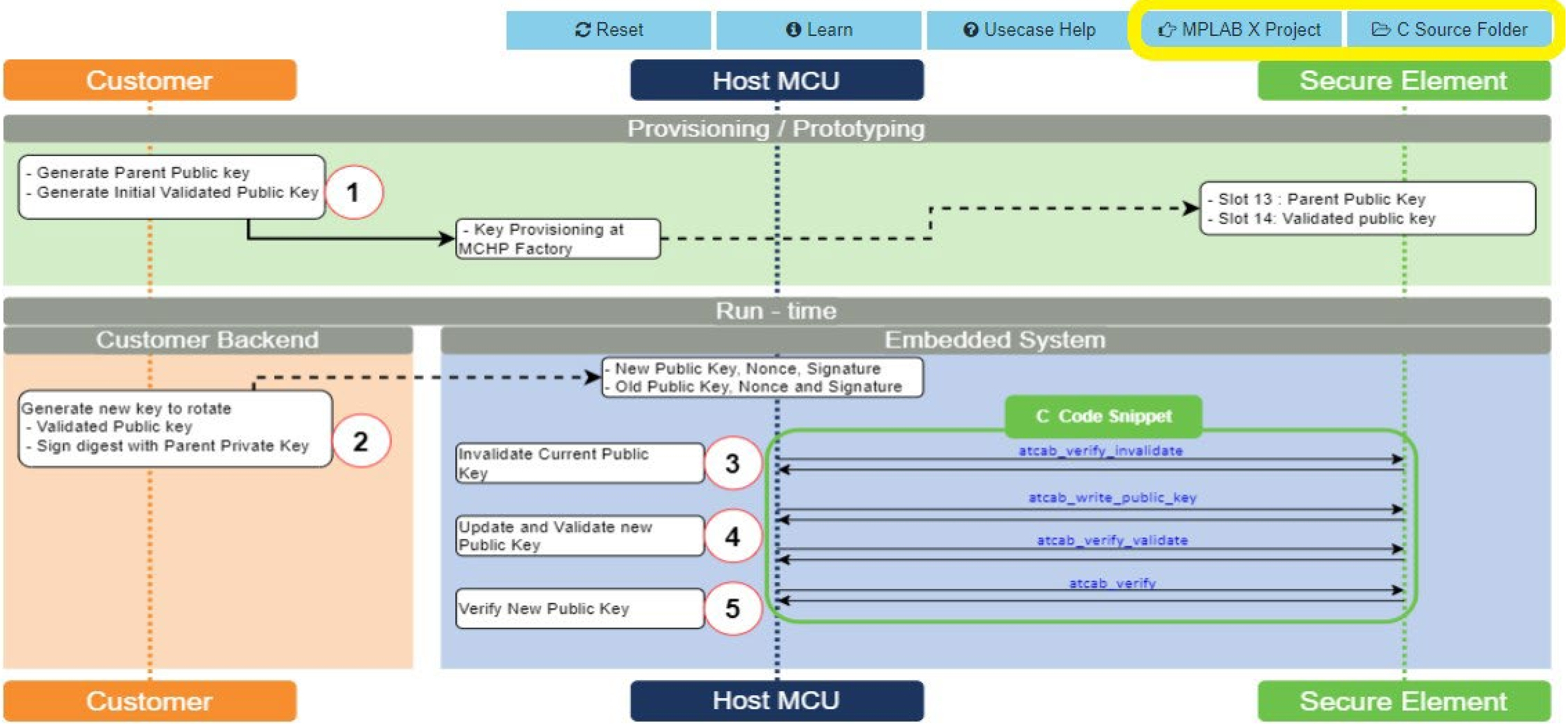
Trust Platform Design Suite v2

Interactive Application Notes



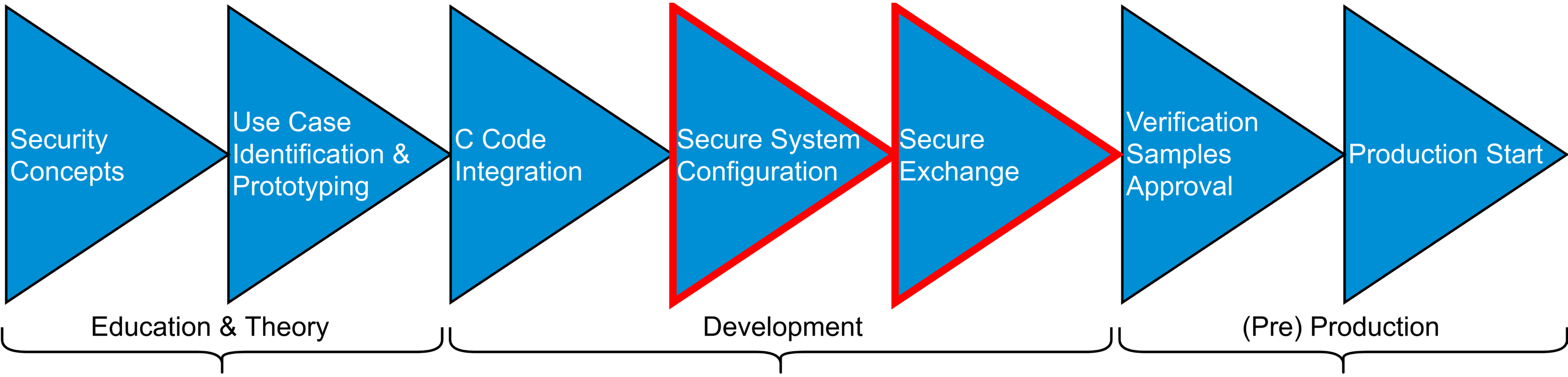
Trust Platform Design Suite v2

Use Case C Code



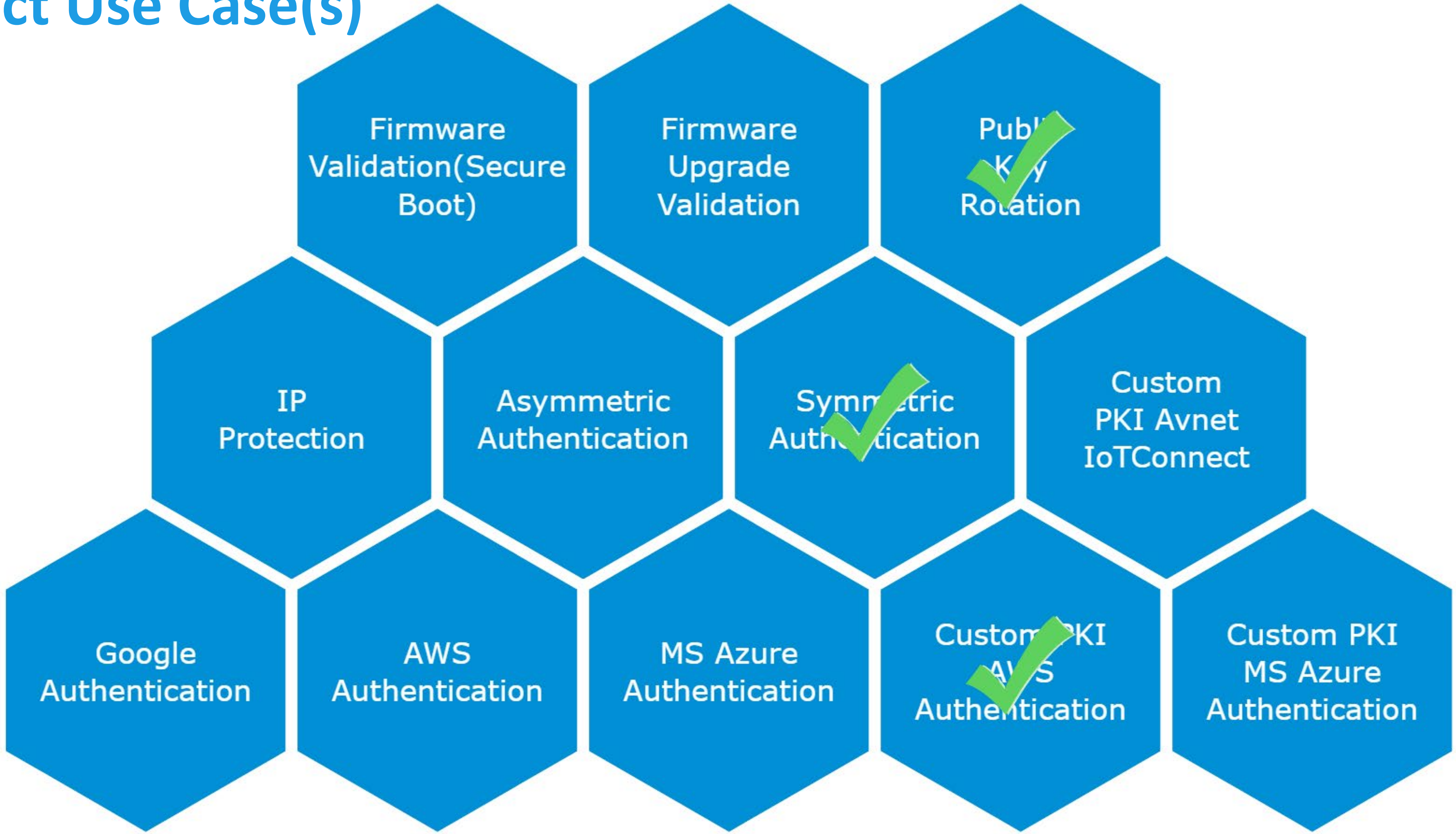
Trust Platform Design Suite v2

Secure Exchange Package Generation



Trust Platform Design Suite v2

Select Use Case(s)



MICROCHIP

Trust Platform Design Suite v2

Slot Number	Slot Use Case	Description	Slot Property
Slot 0	Primary private key	Primary authentication key.	Permanent, Ext Sign, ECDH
Slot 1	Internal sign private key	Private key that can only be used to attest internal keys and state of the device. Can't be used to sign arbitrary messages.	Permanent, Int Sign
Slot 2	Secondary private key 1	Secondary private key for other uses.	Updatable, Ext Sign, ECDH, Lockable
Slot 3	Secondary private key 2	Secondary private key for other uses.	Updatable, Ext Sign, ECDH, Lockable
Slot 4	Secondary private key 3	Secondary private key for other uses.	Updatable, Ext Sign, ECDH, Lockable
Slot 5	Secret key	Storage for a secret key	No read, Encrypted write(6), Lockable, AES key
Slot 6	IO protection key	Key used to protect the I2C bus communication (IO) of certain commands. Requires setup before use.	No read, Clear write, Lockable
Slot 7	Secure Boot digest	Storage location for secureboot digest. This is an internal function, so no reads or writes are enabled.	No read, No write
Slot 8	General data	General public data storage (416 bytes).	Clear read, Always write, Lockable
Slot 9	AES key	Intermediate key storage for ECDH and KDF output.	No read, Always write, AES key
Slot 10	Device compressed certificate	Certificate primary public key in the Crypto Authentication compressed format.	Clear read, No write
Slot 11	Signer public key	Public key for the CA (signer) that signed the device cert.	Clear read, No write
Slot 12	Signer compressed certificate	Certificate for the CA (signer) certificate for the device certificate in the CryptoAuthentication compressed format.	Clear read, No write
Slot 13	Parent public key or general data	Parent public key for validating/invalidating the validated public key. Can also be used just as a public key or general data storage (72 bytes).	Clear read, Always write, Lockable
Slot 14	Validated public key	Validated public key cannot be used (verify command) or changed without authorization via the parent public key.	Clear read, Always write, Validated (13)
Slot 15	Secure boot public key	Secure boot public key.	Clear read, Always write, Lockable

Trust Platform Design Suite v2

Slot details

Slot 5	Secret key	Storage for a secret key	No read, Encrypted write(6), Lockable, AES key

SLOT 5

Slot Description:

This slot provides a storage location for a symmetric key to use with the ATECC608B's symmetric key commands. The primary use case was to support secondary symmetric authentication. For example, many cloud providers perform symmetric authentication using HMACSHA256, which could be done with a key in this slot. Slot can only be updated with an encrypted write using the IO protection key as a write key. The IO protection key must be setup prior to writing this slot. This slot is also marked as an AES slot so it can be used with the AES command if required.

Provisioning:

The data entered in the below step will be stored in the device slot during provisioning.

Provisioning data input method:

- ( ) Slot Unused
- ( ) Enter HEX data
- (•) Upload data through .pem file

Choisir un fichier Aucun fichier choisi

Disable slot write:

If the following checkbox is checked, the contents of the slot cannot be modified under any circumstances.

Disable slot write ☐

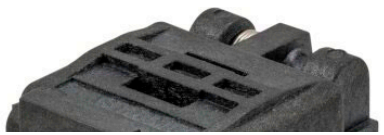
Trust Platform Design Suite v2

Secure Exchange Package Generation

Prototyping		Production
Generate Provisioning Package	Provision Prototype Samples	Generate Provisioning Package - Encrypted
PROTOTYPE package is meant only for understanding and prototyping. It should **NOT** be shared as secrets are available in plain text. Alternatively, you may use dummy secrets.	This button provisions the ATECC608B-TFLXTLSx-PROTO with the package generated from "Generate provisioning Package - Prototype". It only accepts zip files.	Production package must be used to generate the Secure Provisioning Package to be sent to Microchip Provisioning Service (through **Microchip Technical Support Portal**). You will be prompted to add the HSM encryption keys when starting the generation process.

Trust Platform Design Suite v2

Secure Exchange Package Generation



Prototyping

Generate Provisioning Package

PROTOTYPE package is meant only for understanding and prototyping. It should **NOT** be shared as secrets are available in plain text. Alternatively, you may use dummy secrets.

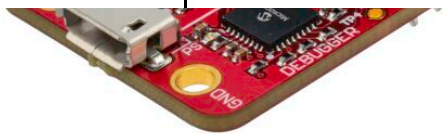
Provision Prototype Samples

This button provisions the ATECC608B-TFLXTLSx-PROTO with the package generated from "Generate provisioning Package - Prototype". It only accepts zip files.

Production

Generate Provisioning Package - Encrypted

Production package must be used to generate the Secure Provisioning Package to be sent to Microchip Provisioning Service (through **Microchip Technical Support Portal**). You will be prompted to add the HSM encryption keys when starting the generation process.



MICROCHIP

Trust Platform Design Suite v2

Secure Exchange Package Generation

Prototyping		Production
Generate Provisioning Package	Provision Prototype Samples	Generate Provisioning Package - Encrypted
PROTOTYPE package is meant only for understanding and prototyping. It should **NOT** be shared as secrets are available in plain text. Alternatively, you may use dummy secrets.	This button provisions the ATECC608B-TFLXTLSx-PROTO with the package generated from "Generate provisioning Package - Prototype". It only accepts zip files.	Production package must be used to generate the Secure Provisioning Package to be sent to Microchip Provisioning Service (through **Microchip Technical Support Portal**). You will be prompted to add the HSM encryption keys when starting the generation process.

Trust Platform: Provisioning Options

	TRUST &GO	TRUST FLEX	TRUST CUSTOM
Pre-configured	YES	YES	NO
Development Time	Lowest	Lower	Custom
Complexity	Lowest	Lower	Custom
Low MOQ Flow (<100ku EAU)	10 units MOQ	2000 units MOQ	4000 units MOQ
High Volume flow (>100ku EAU)	Starting 30 000 units MOQ	Starting 30 000 units MOQ	Starting 30 000 units MOQ
Secure Key Storage	JIL High	JIL High	JIL High
Use cases	TLS authentication LoRaWan authentication	TLS authentication LoRaWan authentication Token authentication Key rotation Firmware verification (OTA, Secure boot) IP protection Public key attestation (A-)symmetric Accessories authentication (A-)symmetric Disposable authentication	Fully customizable
Devices	ATECC608	ATECC608	ATECC608 ATSHA204A TA100

MICROCHIP

Thank you!