Trust Platform for the CryptoAuthentication™ Family

Presenter: MH Eum - Senior Embedded Solutions Engineer

Cryptography Basic

Security Basic (CIA)

Confidentiality e.g. AES : Encryption

- The message should not be exposed?
- Encryption/Decryption required.

Integrity e.g. HASH Algorithm, Message Authentication Code (MAC)

- Are you sure the message or data is not modified?
- Need to know if it is the original.

Authenticity e.g. ECDSA Algorithm

- Are you sure if the message comes from the right sender?
- Need to authenticate the sender or requester.

Symmetric or Asymmetric?

Symmetric

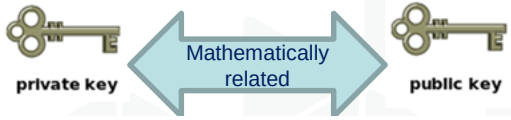
- Same secret key in both host and client, must be protected
- SHA is the most common hash algorithm
- AES is the most common encryption algorithm
- Fast and small in software
- 128 - 256 bits of key storage required
- **ATSHA204, ATAES132**

same security key used in all devices

Asymmetric

- Public key in host is not secret, but must not be changed
- Private key in client needs to be protected
- Typically RSA or ECC; RSA is slower & needs more memory than ECC
  - 768 – 8192 bits of key storage required for RSA
  - 160 – 384 bits of key storage required for ECC
- **ATECCx08**

unique security key pair (private/public key) used in each device



PRIVATE KEY

```
44 C6 33 B6 26 8A 92 A3 44 38 EA 1C 36 7F 52 E8
A3 ED 3F 23 49 81 2E FA 1B FA 83 3B 31 4B F2 59
```

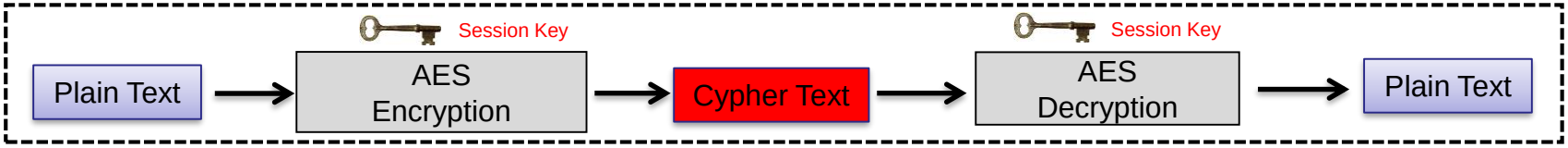
PUBLIC KEY

```
DD 46 4D B5 3D 38 31 EC 58 52 E2 F7 4F 97 4A 7A
B7 31 E2 95 47 03 E5 DA 01 82 CE 1B 84 A9 FE B9
BC D5 4A F3 5F CC C9 82 90 30 E2 51 53 25 76 17
47 FC 5B 35 F9 50 46 13 60 4F 87 FE A7 AC 5C 3F
```

MICROCHIP

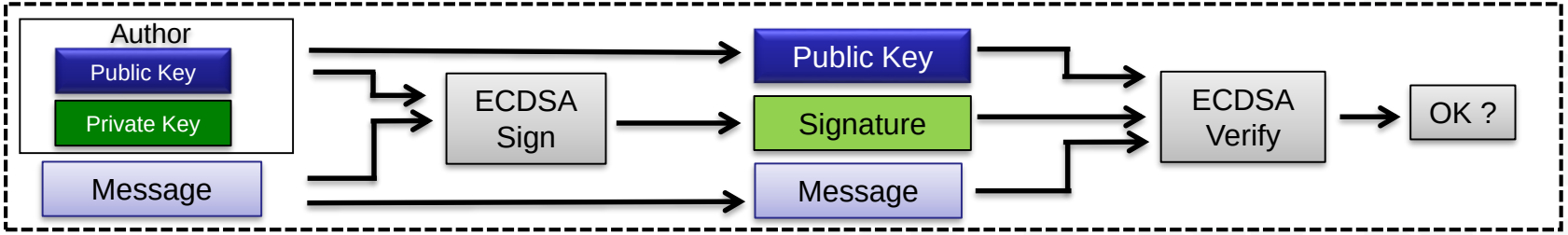
Security Algorithms on ATECC608

AES128 Algorithm - Symmetric - Confidentiality



HASH256 Algorithm – Symmetric – Integrity / Authenticity

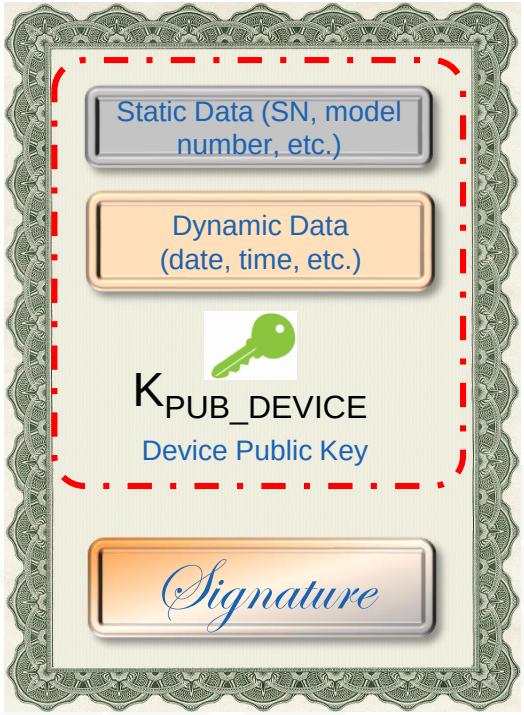
ECC Algorithm – Asymmetric – Integrity / Authenticity



What is Digital Certificate?

The x.509 Digital Certificate

- The Digital Certificate is a unique verifiable form of identity for the node.
- It comprises three main components:
  - The device public key
  - A signature to enable verification of the authenticity
  - Data capturing any attributes the owner intends as part of the identity
- Certificates are standards driven form of identity for the internet.



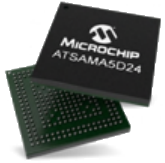
Embedded Security Snapshot

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

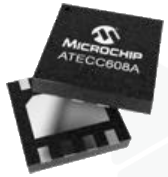
Application layer security	Leverage cryptographic capabilities of the system to further harden the implementation (access rights - privileges)
Secure Connectivity	Authenticate and encrypts the device communication
Secure update	Leverage secure communication and secure boot mechanisms to ensure safe delivery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



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

Today's Weaknesses

Security by design: embedded security is now being considered but hard to implement

Lack of education: The chain of trust principle is not well understood, complex, hard to implement and consequently incorrectly implemented

Keys/Certificates mishandling: Private keys are being handled by software at best and **left accessible in the clear** of the system memory

Backdoors are consequently left open to hackers – they attack the weakest point, in IoT, the **unsecure software** and **exploit the user habits**

Manufacturing is not trustable, not secure and create scalability issues

MICROCHIP

Customization Challenges…

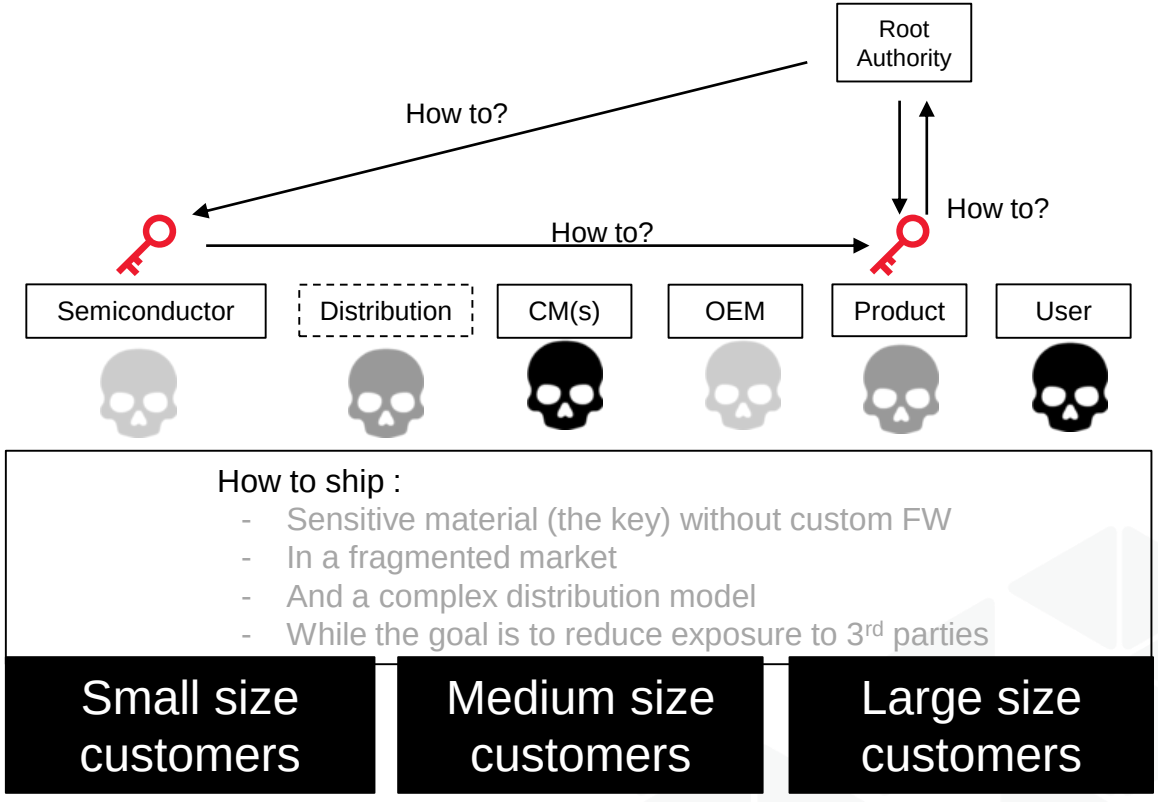
Challenge: Notion of Personalization

The secure device needs to be personalized

- Find and learn complex tools and access expert knowledge to start prototyping
- Configuration mapping of the use case(s)
- Key ceremony to “exchange secrets” and trigger provisioning process
- Manufacture the device in a secured supply chain equipped with Hardware Secure Modules (HSM)
- Results in custom part number (Today market threshold for direct support and provisioning services >100ku)

Distributing Keys in Hardware

A logistic problem for global scale



MICROCHIP

The Needed Improvements are...

Improve user onboarding

Reduce friction due to personalization

Make secure key storage is available to the mass

Microchip Trust Platform for the CryptoAuthentication™ Family

What Are We Launching?

Microchip launches the

Trust Platform for the CryptoAuthentication™ Family

… a secure provisioning service
… a secured device family
… a supply chain channels
… packaged code examples
… a suite of tools

It's all of it!

For any project size…

Microchip Trust Platform for the CryptoAuthentication™ Family: Provisioning Service

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 Trust Platform for the CryptoAuthentication™ Family: the Device

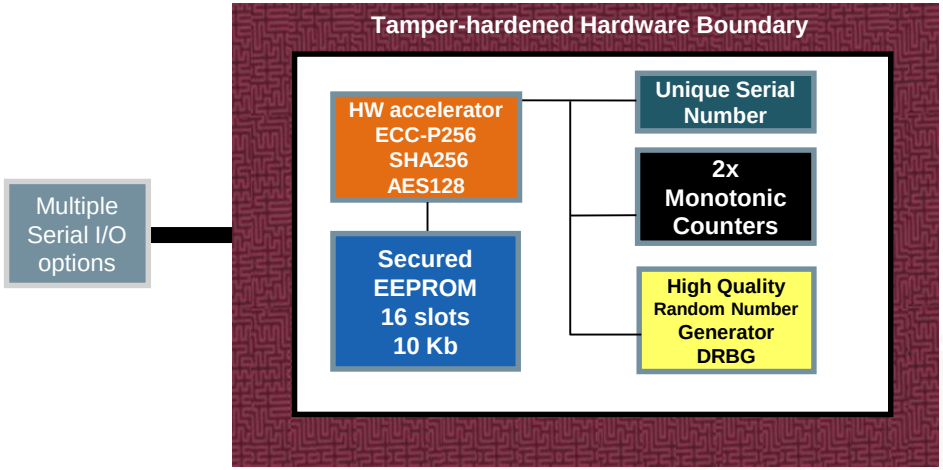
ATECC608A Isolate Keys in Hardware

The ATECC608a securely store key material for the *lifetime* of the device.

Keys are safely **generated inside the device by the device** using a “best in class” Random Number Generator (RNG) meeting NIST specifications

All critical crypto-primitives are executed inside the device where the keys are

- **This keeps the keys, secrets and primitives *strictly segregated* from any vulnerable resources**



- Cryptographic acceleration performs primitives faster and with less power than MCU/MPU
- Information inside is uniquely scrambled and encrypted in EEPROM
- Each device has a unique serial number
- Monotonic counters for usage controls
- Multiple serial I/O options

MICROCHIP

How to Make Sure it's Robust?

Security is Measurable: Common Criteria JIL Rating

Remember the star rating sale model for appliances, energy, water and car safety?

Microchip submitted the ATECC608A to a 3rd party lab to extract the keys. In 3 man-months of expert time, they have not managed to extract the keys using various types of attacks.

The ease, or difficulty, in extracting the keys in usage or at rest results in a Joint Interpretation Library (JIL) rating defined by Common Criteria. They range from 1 to 31. ANY NUMBER is bad, as it means some information was gained during testing.

The ATECC608A has received a JIL "HIGH" rating. It's the highest JIL rating available. There is no number because no secrets were revealed. Could be assimilated to EAL6/7.

MICROCHIP

CryptoAuthLib library

CryptoAuthLib source code

- https://github.com/MicrochipTech/cryptoauthlib

CryptoAuthLib Documentation

- https://microchiptech.github.io/cryptoauthlib/html/index.html

Microchip Trust Platform for the CryptoAuthentication™ Family: the Tools and Examples

Trust Platform Design Suite
A Simpler Onboarding

1 Define

Map use case to configuration

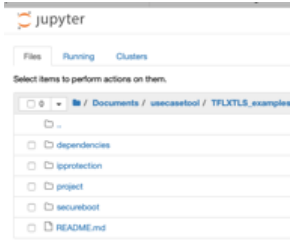
Use Case Tool

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

MICROCHIP

Hardware Development Tools

DM320118

Trust Platform USB Kit

- Direct prototyping
- PC Host via USB (with Python Jupyter Notebook tutorials)
- Or onboard SAMD21 with debugger

DT100104

ATECC608A Trust Platform Board

- Onboard:
  - Trust&GO,
  - TrustFLEX,
  - TrustCUSTOM
- MikroBUS male

AT88CKSCKTUDFN

CryptoAuthentication™ Socket Kit

- uDFN8 socket
- SOIC8 socket
- Xplain PRO form factor

Mikroe.com Socket

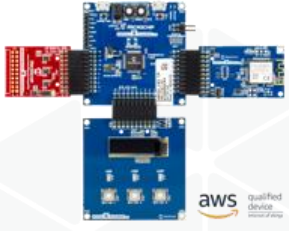
- UDFN and SOIC
- Same Functionality as XPRO Socket Boards
- MikroBUS™ male pinout
- Sold through Mikroe.com

Complete Stack Solutions

All the code packages include

Wiki user manual

Turnkey code examples



Complete HW solutions

Microchip Trust Platform for the CryptoAuthentication™ Family: Supply Chain Value

A Ready to GO Trust Model

- Pre-provisioned with generic certificates and keys for thumbprint authentication
- Fixed configuration with related cloud authentication use cases

- **IP based cloud with TLS** that accepts “same device certificate across multiple accounts”
  - AWS “Multi Accounts Registration”
  - Google Cloud Platform™: Token authentication
  - Microsoft “Certificate Thumbprint”
  - Private cloud

- **LoRaWAN®**: Pre-provisioned with
  - Application keys
  - Network keys
  - Re-keying feature available to transfer out of Joint Server
  - Compatible for
    - The Things Industries
    - Actility

Value of Trust&GO Authentication

Ease of Use

- **Less complexity**: No expert involvement
- **More affordable**: a full managed PKI involve 10s or 100s of thousands of dollars – not with Trust&GO
- **No certificate authority** involvement due to AWS Multi-Account Registration or Google JWT or Azure Certificate Thumbprint

Connectivity Agnostic

- **Any TLS** based networks
- **LoRa®** support (different P/N)

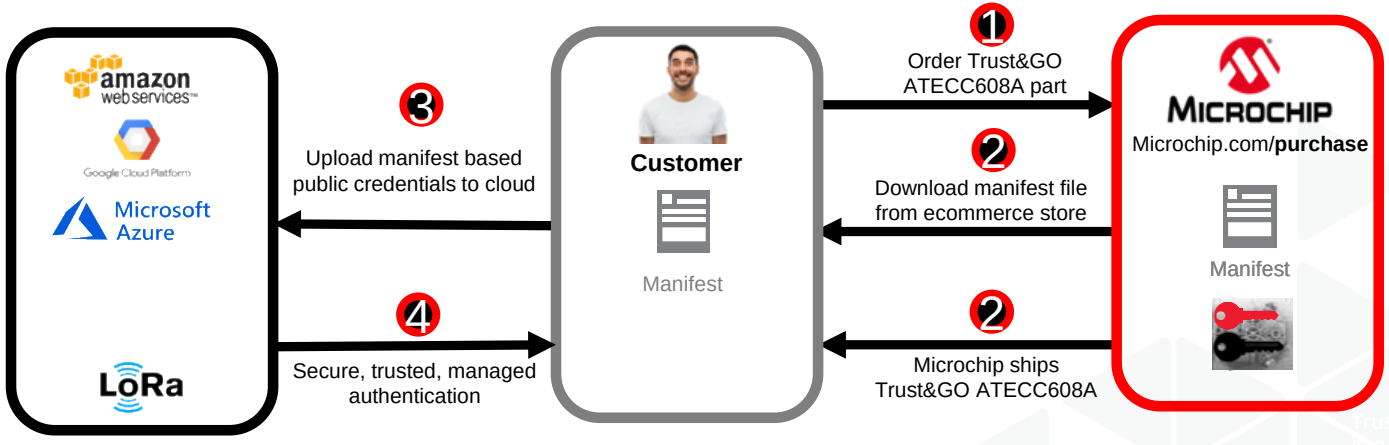
Very Low MOQ including Provisioning (10 units)

- **Lowest market MOQ** – compare to 100ku-150ku from other providers to get direct support
- **Simplify the logistics** – shipping private keys is now automated
- Make secure key storage **available** for the mass market

Shorter Time-to-Market

- **More autonomy**: No paperwork (NDA, letter of agreement, …)
- **Less complexity**: all development happening in the controller with CryptoAuthLib
- **Simplest onboarding** leveraging Microchip and distribution partner ecommerce stores

Trust&GO: Simple Ordering Process



TrustFLEX Overview

What if the customer likes Trust&GO, but their use case requires more?
TrustFlex allows an overlay of Trust&GO functionality with any combination of the following use cases:

- ✓ Start with pre-configured only device policies
- ✓ Cover all the most commonly used use cases
  - ✓ Custom certificate authentication
  - ✓ JWT authentication
  - ✓ Secure boot (with key attestation)
  - ✓ OTA verification
  - ✓ FW IP protection
  - ✓ Message encryption
  - ✓ Key rotation
  - ✓ I/O protection key
  - ✓ Host accessory authentication

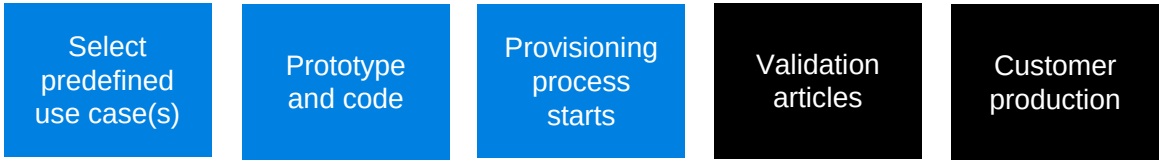
Needs to be provisioned with customer credentials
All these use cases require some customer information:

- ✓ Secure boot public key
- ✓ Secure boot master public key
- ✓ Accessory / IP protection master secret
- ✓ PKI chain

microchip.com/TrustFLEX

MICROCHIP

What's in it?



Low MOQ (2k units) including provisioning

- Unique low MOQ market offer
- Address all types of project and company volume sizes
- Uncompromised security solution for the masses

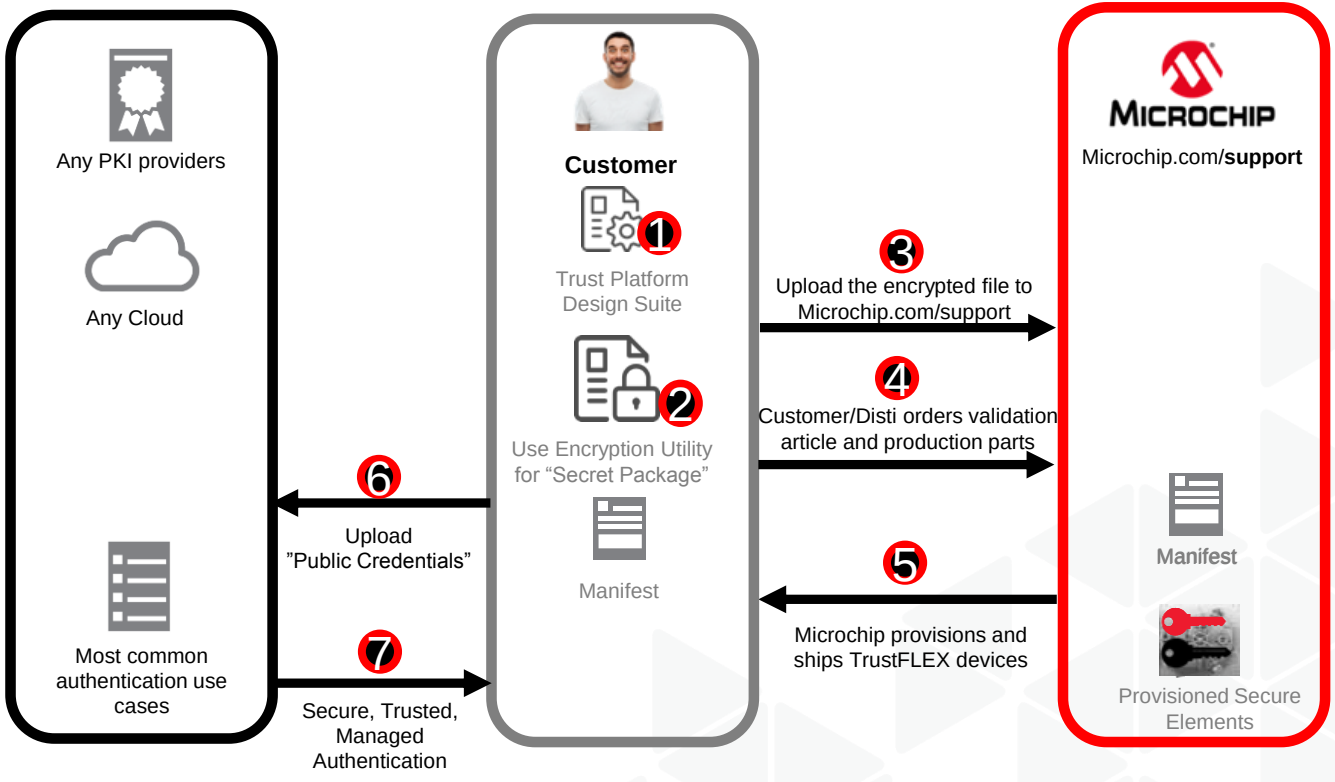
Pre-defined most common use cases

- Support any cloud
- Compatible to support any certificate authority providers
- Accommodate customer's own secrets

Simplified engagement model for provisioning process

- The Trust Platform Design Suite removes friction for both development and secret exchange

TrustFLEX flow



Fully Customizable Secure Key Storage

Features

- ✓ Device can become anything
- ✓ Start with blank device
- ✓ Fully customizable
- ✓ Low MOQ = 4 ku
- ✓ Secret exchange using the new configurator
- ✓ Tradeoff: Customer fully responsible for the MCU FW

Customer Benefits

- ✓ Customization accessible to low volume products
- ✓ Simplified onboarding with new tools
- ✓ Keys protected in JIL High secure key storage

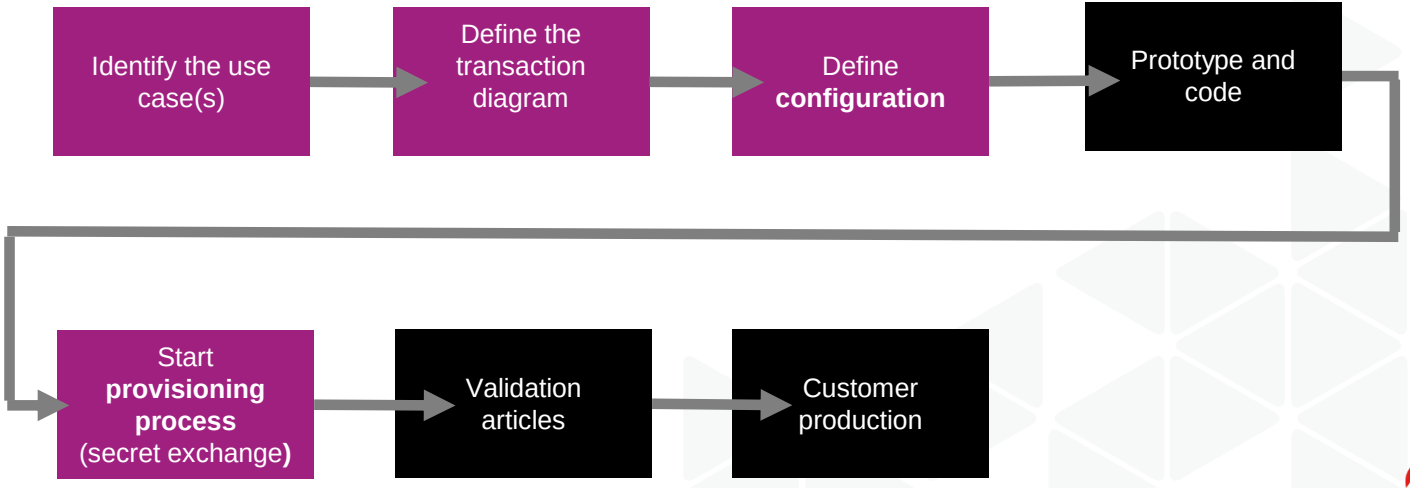
microchip.com/**TrustCUSTOM**

MICROCHIP

TrustCUSTOM Provisioning Flow

Onboarding Highlights

- ✓ Easier development starts with the use case tool
- ✓ Easier configuration with the configuration tool
- ✓ Easier onboarding for secret exchange with the XML Generator



Microchip Trust Platform for the CryptoAuthentication™ Family: Customer Journey

Customer Journey 1/2

Yes

1. Lab evaluation
- USB dongle
- Code from GitHub

2.Prototyping
- Order on Microchip store or distribution

3. Low volume production
- Order on Microchip store or distribution

4. High volume production
- Assigns a custom part number*

No

OK with using generic certificates for thumbprint authentication?
Cloud infrastructure support generic certificate only authentication (no intermediate certificate)?
OK with only cloud authentication use case?

Yes

1. Detailed use case definition
- Use case tool

2. Lab evaluation
- Notebooks examples
- Code from GitHub
- USB dongle

3. Generate light secret exchange
- Use case tool

4.Prototyping
- Submit ticket to send encrypted XML file to MCHP

5. Low volume production
- Order through Microchip store

6. High volume production
- Assigns a custom part number
- Orders direct

OK with pre-defined use cases?

No

MICROCHIP

Customer Journey 2/2

Yes

1. Detailed use case definition
- Use case tool
- Expert support

2. Lab evaluation
- Notebooks examples
- GitHub example code
- USB dongle

3. Generate secret exchange
- Secret exchange tool

4. Prototyping
- Upload secret exchange to support ticket

5. Low volume production
- Order through Microchip store

6. High volume production
- Assigns a custom part number

Trust Platform Device Family

Trust & Go	Description
ATECC608A-TNGTLSS-B	Trust & Go TLS, Proto Typing, 8-SOIC, I2C, (10 bulk)
ATECC608A-TNGTLSU-B	Trust & Go TLS, Proto Typing, 8-UDFN, I2C, (10 bulk)
ATECC608A-TNGTLSS-C	Trust & Go TLS, Provisioned, 8-SOIC, I2C, (100 unit reel)
ATECC608A-TNGTLSU-C	Trust & Go TLS, Provisioned, 8-UDFN, I2C, (100 unit reel)
ATECC608A-TNGTLSS-G	Trust & Go TLS, Provisioned, 8-SOIC, I2C, 2K reel
ATECC608A-TNGTLSU-G	Trust & Go TLS, Provisioned, 8-UDFN, I2C, 2K reel
Trust Flex	**Description**
ATECC608A-TFLXTLSS-Proto	Trust Flex TLS, Proto Typing, 8-SOIC (10 bulk)
ATECC608A-TFLXTLSU-Proto	Trust Flex TLS, Proto Typing, 8-UDFN, I2C, (10 bulk)
ATECC608A-TFLXTLSS	Trust Flex TLS, Provisioned, 8-SOIC 2K MOQ
ATECC608A-TFLXTLSU	Trust Flex TLS, Provisioned, 8-UDFN 2K MOQ
Trust Custom	**Description**
ATECC608A-TCSMS	Trust Custom, Provisioned, 8-SOIC, 4K MOQ
ATECC608A-TCSMU	Trust Custom, Provisioned, 8-UDFN 4K MOQ
Trust & Go LoraWan	**Description**
ATECC608A-TNGLORAS-B	Trust & Go LORAWAN, Proto Typing, 8-SOIC, I2C, (10 bulk)
ATECC608A-TNGLORAU-B	Trust & Go LORAWAN, Proto Typing, 8-UDFN, I2C, (10 bulk)
ATECC608A-TNGLORAS-C	Trust & Go LORAWAN, Provisioned, 8-SOIC, I2C, (100 unit reel)
ATECC608A-TNGLORAU-C	Trust & Go LORAWAN, Provisioned, 8-UDFN, I2C, (100 unit reel)
ATECC608A-TNGLORAS-G	Trust & Go LORAWAN, Provisioned, 8-SOIC, I2C, 2K reel
ATECC608A-TNGLORAU-G	Trust & Go LORAWAN, Provisioned, 8-UDFN, I2C, 2K reel

Trust Flex LorWan	Description
ATECC608A-TFLXLORAS-Proto	Trust Flex LORAWAN, Proto Typing, 8-SOIC (10 bulk)
ATECC608A-TFLXLORAU-Proto	Trust Flex LORAWAN, Proto Typing, 8-UDFN, I2C, (10 bulk)
ATECC608A-TFLXLORAS	Trust Flex LORAWAN, Provisioned, 8-SOIC 2K MOQ
ATECC608A-TFLXLORAU	Trust Flex LORAWAN, Provisioned, 8-UDFN 2K MOQ
Trust & Go Actility	**Description**
ATECC608A-TNGACTS-B	Trust & Go Actility LORAWAN, Proto Typing, 8-SOIC, I2C, (10 bulk)
ATECC608A-TNGACTU-B	Trust & Go Actility LORAWAN, Proto Typing, 8-UDFN, I2C, (10 bulk)
ATECC608A-TNGACTS-C	Trust & Go Actility LORAWAN, Provisioned, 8-SOIC, I2C, (100 unit reel)
ATECC608A-TNGACTU-C	Trust & Go Actility LORAWAN, Provisioned, 8-UDFN, I2C, (100 unit reel)
ATECC608A-TNGACTS-G	Trust & Go Actility LORAWAN, Provisioned, 8-SOIC, I2C, 2K reel
ATECC608A-TNGACTU-G	Trust & Go Actility LORAWAN, Provisioned, 8-UDFN, I2C, 2K reel
Trust Flex Actility	**Description**
ATECC608A-TFLXACTS-Proto	Trust Flex Actility LoraWan, Proto Typing, 8-SOIC (10 bulk)
ATECC608A-TFLXACTU-Proto	Trust Flex Actility LORAWAN, Proto Typing, 8-UDFN, I2C, (10 bulk)
ATECC608A-TFLXACTS	Trust Flex Actility LORAWAN, Provisioned, 8-SOIC 2K MOQ
ATECC608A-TFLXACTU	Trust Flex Actility LORAWAN, Provisioned, 8-UDFN 2K MOQ

MICROCHIP

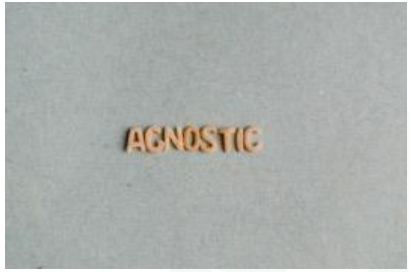
Takeaways

Easier onboarding with **predefined use cases**

Quick development with **simple toolsets**

Simpler flows leveraging **e-commerce stores**

Fitted for Mass Market with **low MoQ** including **provisioning** and **Microchip certificates**



Architecture Agnostic with any cloud, any PKI*, any controller, any connectivity

*PKI : public key infrastructure

Thank you!

microchip.com/**TrustPlatform**