Welcome to the easy way to securely deploy IoT devices to the cloud at scale

Theodore Varelas,
Director Product Marketing & Management of IoT Security
8 June 2022

The Challenge for IoT device deployment

Cloud-connected IoT devices require a unique identity, but there is no easy, cost-effective way to personalize each device and connect them safely to the cloud – **at scale**.

Why a unique, secured identity is important

1. Trust is the foundation for all interactions between IoT devices and cloud services.

2. To establish this trust, IoT devices require a **unique identity**, typically in the form of a X.509 certificate with a **unique public and private key.**

3. **Devices with a unique and secured identity** are capable of establishing mutual trust and sending and receiving **accurate data** and commands to the right "things“ at the right time.
   This enables:

Privacy

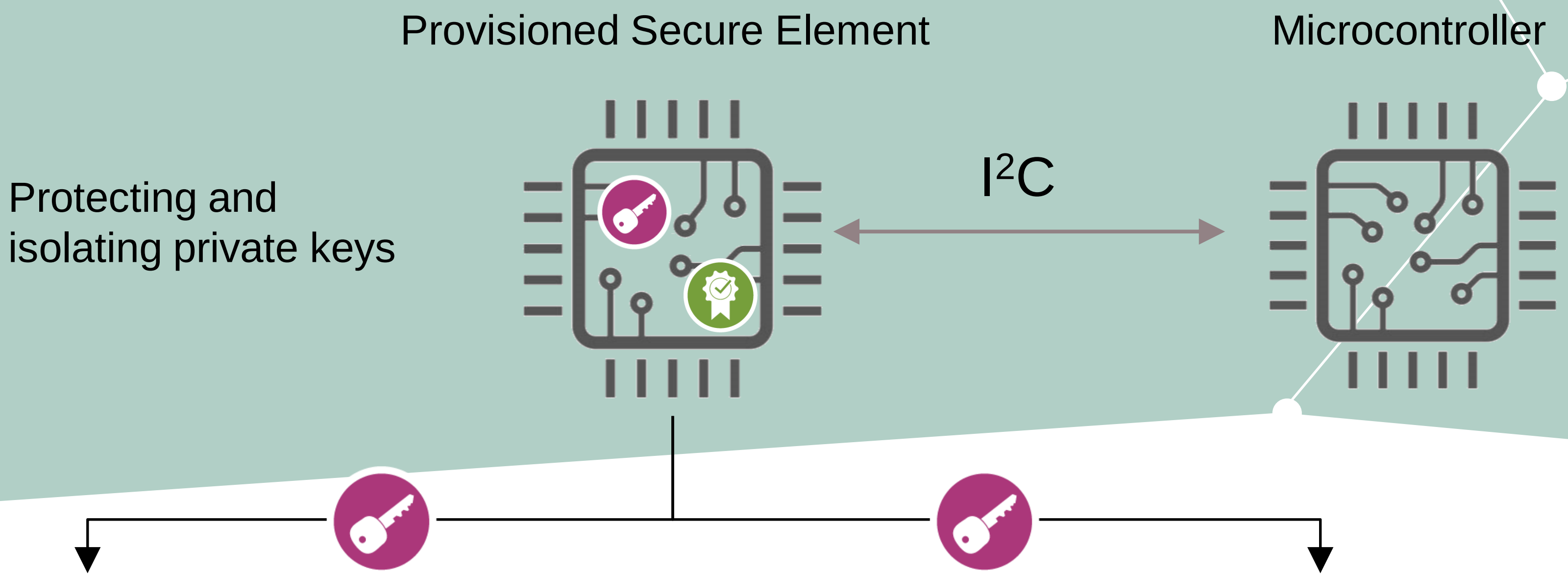
Protection of intellectual property

Software or security updates

Reactive & predictive maintenance

When "things" communicate, protecting their unique identity is crucial.

A Secure Element provides a hardware Root of Trust – the foundation of a Chain of Trust spanning from hardware to cloud



Provisioned Secure Element

Microcontroller

Protecting and
isolating private keys

I^2C

At the OEM/CM manufacturing line

At the semiconductor facility (pre-provisioning)

Using a pre-provisioned Secure Element reduces complexity and costs and increases security

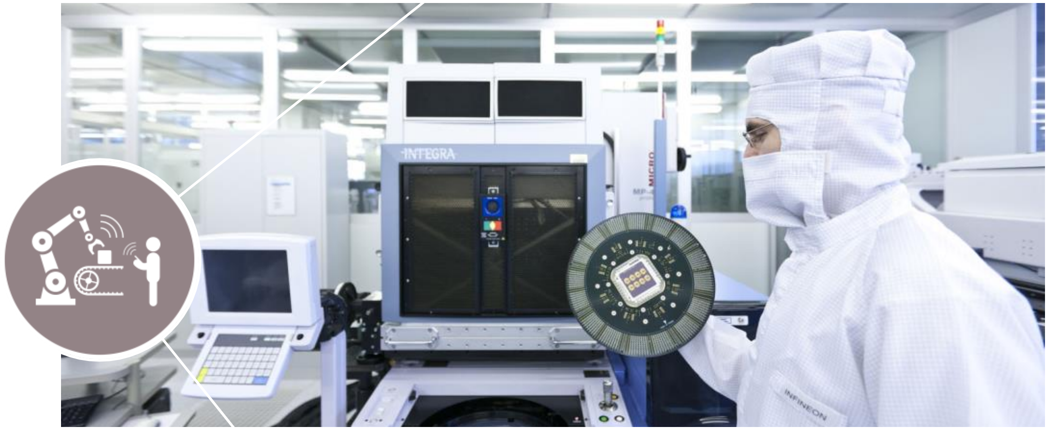
Provisioning at Original Equipment Manufacturer (OEM)

Higher cost for OEM

- OEM needs to enable secure provisioning at Contract Manufacturers (CMs)
- OEM needs to act as Certificate Authority (CA)

Higher risk for OEM

- OEM needs to share IDs with CMs – high risk of data breaches
- Increased complexity to keep track of device identity data over different locations



Provisioning at semiconductor facilities

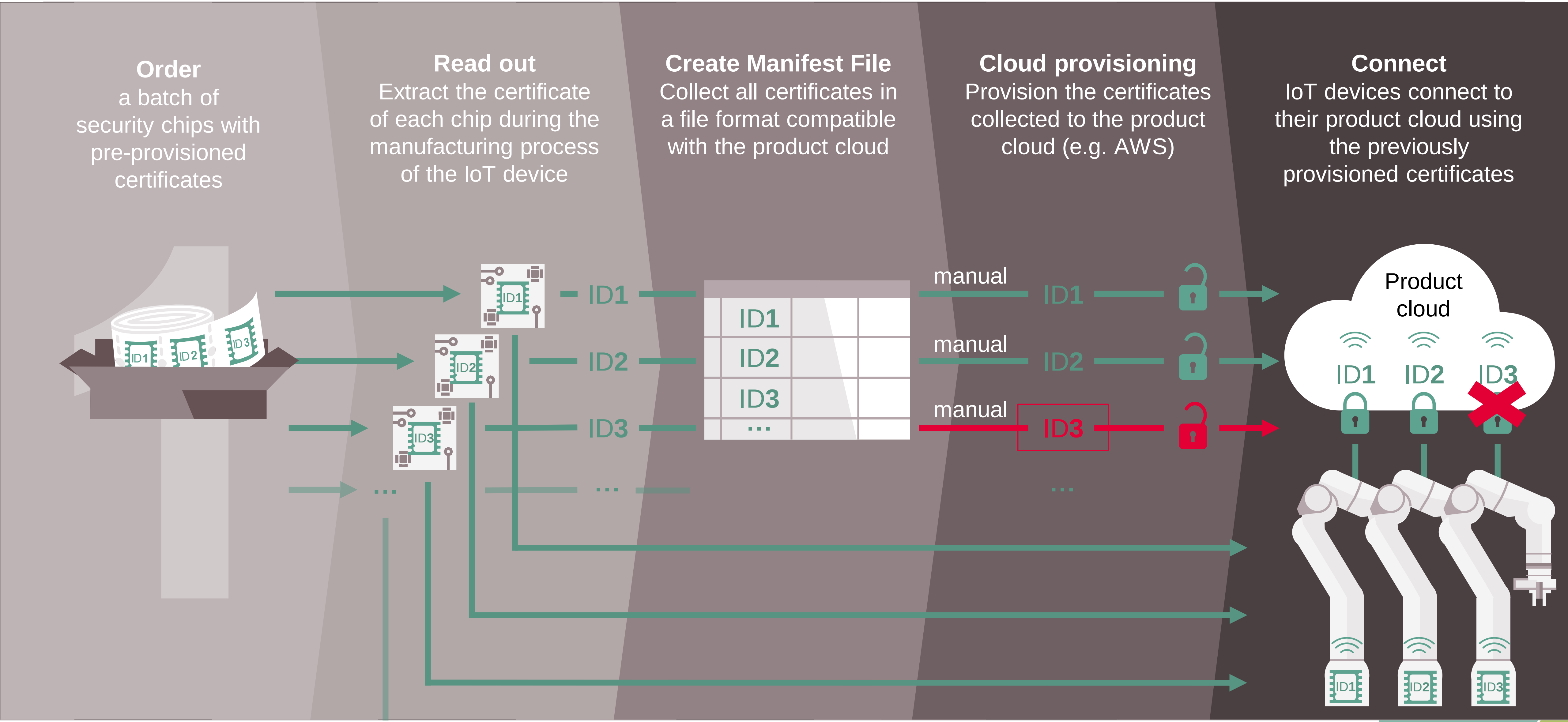
Cost optimization for OEM

- No need for secure manufacturing capabilities at CMs
- Semiconductor provider acts as CA issuing the device certificates

Higher security for OEM

- IDs are injected in a certified facility, establishing a "Chain of trust" from silicon manufacturing to final IoT device
- No data needs to be transferred between different manufacturing locations → no exposure of IDs

Typical IoT device-to-cloud onboarding is long and complex



Order
a batch of security chips with pre-provisioned certificates

Read out
Extract the certificate of each chip during the manufacturing process of the IoT device

Create Manifest File
Collect all certificates in a file format compatible with the product cloud

Cloud provisioning
Provision the certificates collected to the product cloud (e.g. AWS)

Connect
IoT devices connect to their product cloud using the previously provisioned certificates

OPTIGA™ Trust M Express + CIRRENT™ Cloud ID: simplified device-to-cloud authentication and robust protection for IoT devices

OPTIGA™ Trust M Express

An off-the-shelf security solution based on a certified Secure Element and pre-provisioned at Infineon's Common Criteria certified facility.

+

CIRRENT™ Cloud ID

An Infineon cloud service that automates IoT device certificate registration and the provisioning of the device in the product cloud.

CIRRENT^{TM} Cloud ID has been launched in Oct 2021

OPTIGA™ Trust M Express: An off-the-shelf, high-end Secure Element for IoT devices

Main Features

- Based on CC EAL 6+ certified HW
- Latest cryptography

Host compatibility

- Cortex M4: XMC4xxx, PSoC6x
- Cortex M0: XMC1xxx family
- SoC: NRF5x; ESP32
- OS: Linux, Zephyr OS, FreeRTOS

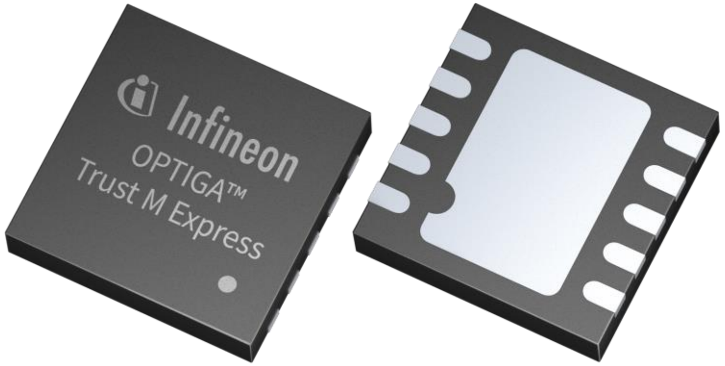
Typical Use Cases

- Secured cloud authentication
- Secured cloud communication
- Secured software updates
- Crypto offloads
- … and more!

Tools and support

- Open Source framework (MIT)
- NDA-free application notes and code examples
- Modus Toolbox™ support
- Development kits

- **Pre-provisioned in a certified facility and ready to securely connect to AWS, Azure and private clouds**
- **CIRRENT™ Cloud ID support for automated cloud provisioning**



CIRRENT™ Cloud ID service – Infineon's unique approach to automated device-to-cloud onboarding

Learn more

- Cloud ID Product Page
- Cloud ID Blog Post
- Cloud ID Documentation
- Cloud ID Virtual Developer Kit

How it works

The CIRRENT™ console carries the public-key certificates for Cloud-ID compatible products.

Companies can:

bind a batch of products using their CIRRENT™ account, establishing possession & ownership › **download the certificates from the cloud** › **set up automation within the CIRRENT™ console to provision the batch of products to their own product cloud**

Benefits

Automated cloud onboarding
QR-code scan triggers binding to an owner & registration & provisioning of compatible chips to only customer's cloud

Software based Device Customization
No need for personalization in a secured manufacturing environment – instead provided by Late Binding & Digital Twins

Only Authenticated Devices attach to Product Cloud
Firewall can prevent unauthorized or spoofed devices from pumping data into customer's product cloud

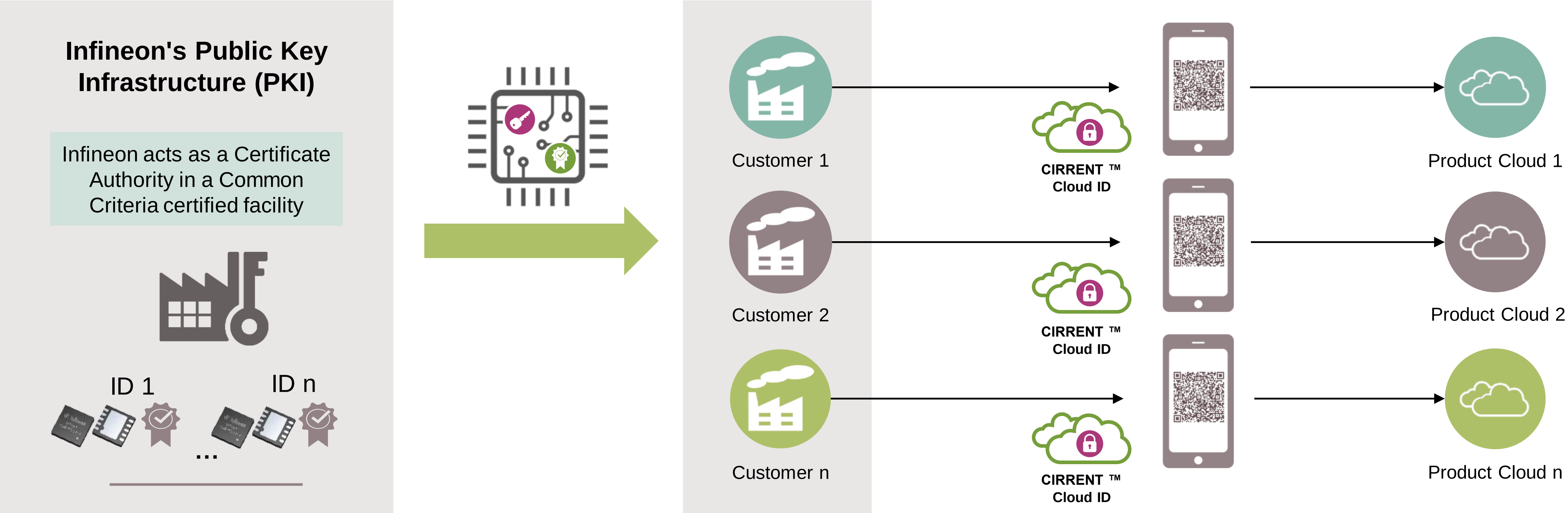
How it works: Production & On Boarding

Infineon manufactures OPTIGA™ Trust M Express chips with **pre-provisioned** certificates

Customers get batches of **standard, off-the-shelf** OPTIGA™ Trust M Express chips together with a QR code/alphanumeric string

Each customer claims their chips and automates the secure cloud provisioning

Devices with the chips inside connect automatically to the product cloud



Infineon's Public Key Infrastructure (PKI)

Infineon acts as a Certificate Authority in a Common Criteria certified facility

CIRRENT™ Cloud ID and OPTIGA™ Trust M Express: A unique approach to device-to-cloud authentication

Order

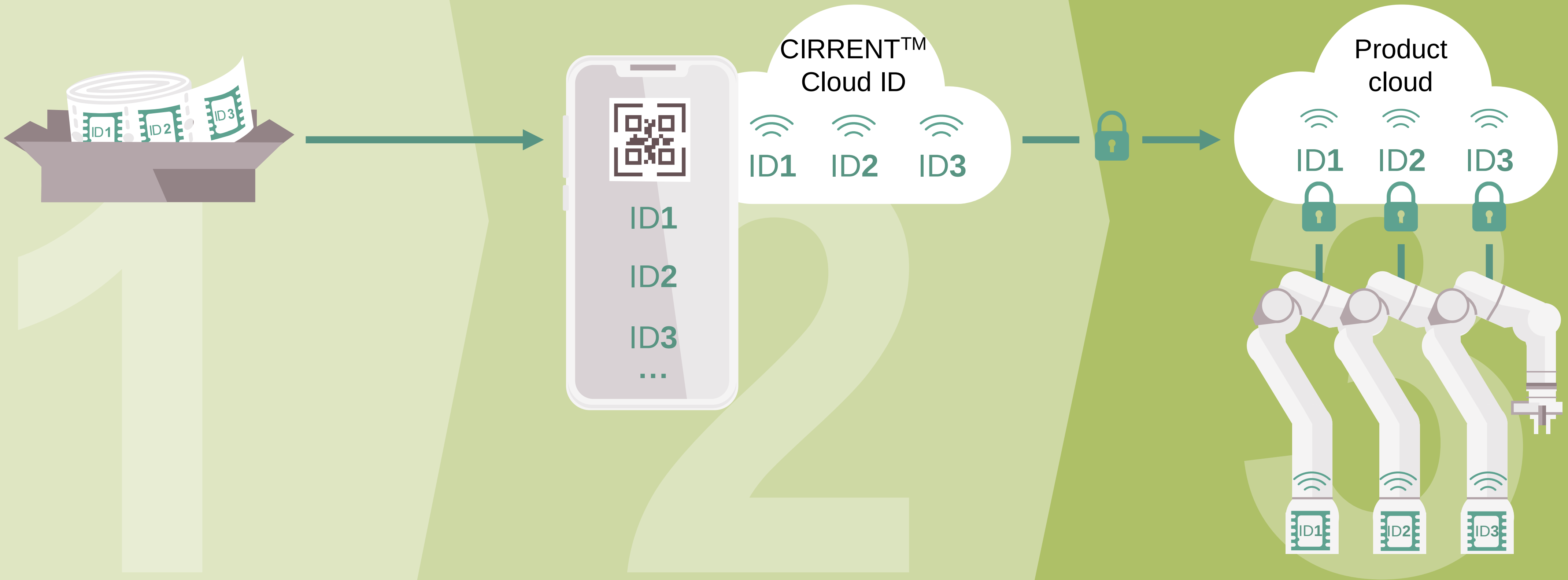
✓ No exposure of IDs during the manufacturing process

Claim

✓ Automated cloud provisioning

Connect

✓ The entire process is now automated



Develop and evaluate end-to-end security use cases for IoT devices with the OPTIGA™ Trust M Security Development Kit

See the OPTIGA™ Trust M IoT Security Development Kit unboxing video

Key features

- Featuring Adafruit Feather compatibility, OPTIGA™ Trust M, PSoC™ 62 MCU and AIROC™ Wi-Fi + Bluetooth® combo
- Pre-configured with two security use cases:
  - MQTT connectivity to AWS
  - Zero-touch cloud provisioning using CIRRENT™ Cloud ID
- ModusToolbox™ support
- Available to order online

The easy way to securely deploy IoT devices to the cloud at scale

1 **OPTIGA™ Trust M Express** – off-the-shelf security solution, pre-provisioned with X.509 certificates to enable a secured cloud authentication and secured communication with Azure, AWS and other private clouds.

2 **OPTIGA™ Trust M Express** is supported by **CIRRENT™ Cloud ID** – a brand-new Infineon cloud service that automates IoT device certificate registration and the provisioning of the device at the OEM product cloud.

3 Our customers can leverage the availability of a complete solution – Secure Element and Cloud Service – **reducing the complexity of managing the device identities and onboarding the devices to the cloud.**

4 **OPTIGA™ Trust M Express** will be available from September 2022.

Key Take aways

Please visit our webpage for more information:

www.infineon.com/OPTIGA-Trust-M-Express

infineon

Part of your life. Part of tomorrow.

OPTIGA™ Trust M Express + CIRRENT™ Cloud ID: the benefits

Save costs

- Removes the need for a highly secured manufacturing environment
- Removes the need to build & maintain a Public Key Infrastructure

Go to market fast

- Off-the-shelf Secure Elements for reduced design-in process
- Removes the need for personalization during manufacturing
- Easy-to-use developer kit for fast prototyping
- NDA-free product documentation on GitHub
- Ready to connect to Azure and AWS

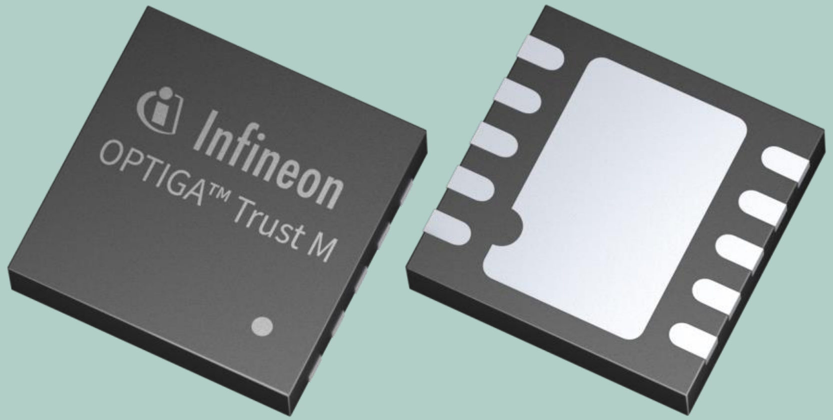
Scale fast

- Automated device onboarding to cloud
- Product-to-cloud provisioning with zero manual intervention
- Simplified claiming process

Robust security

- Based on CC EAL 6+ certified hardware
- Support for all latest symmetric and asymmetric cryptographic algorithms
- Unique and immutable identity pre-provisioned in a CC certified facility
- Protection against data breeches and human errors as IDs never leave the closed system

OPTIGA™ Trust M Express is just one of a line of solutions



OPTIGA™ Trust M Suite

OPTIGA™ Trust M Express

- An off-the-shelf solution pre-provisioned with unique device credentials (X.509 certificates) for secured cloud authentication
- Zero-touch secured cloud provisioning enabled by CIRRENT™ Cloud ID – the easiest way to securely deploy IoT devices to the cloud at scale
- Pre-provisioning done at security certified Infineon facility
- MOQ: 4000 pieces

OPTIGA™ Trust M Fit

- Highly customizable OPTIGA™ Trust M version that fits specific customer needs such as integration into customer's own PKI, injection of random numbers and more
- Customization done at security certified Infineon facility
- MOQ: 20.000 pieces