

OPTIGA™ Trust M Express & CIRRENT™ Cloud ID The easy way to securely deploy IoT devices to the cloud – at scale

April 2024

public

Connecting IoT devices to the cloud securely and at scale – challenges and how to overcome them

List of definitions

Public key infrastructure

A PKI governs the issuance of digital certificates to protect sensitive data, provide unique digital identities for users, devices and applications and secured end-to-end communications.

Certification Authority

An entity responsible for creating digital certificates and own the policies, practices, and procedures for vetting recipients and issuing the certificates.

X.509

An ITU Telecommunications Standardization Sector (ITU-T) standard used in cryptography to implement PKI. X.509 relates to the use of certificates for digital and web security.

Unique identity

A cryptographically unique device identifier.

Trust anchor

The root certificate issues by the CA. All the other (intermediary) certificates directly or indirectly derive their trust from the trust anchor.

Chain of trust

A set of certificates related to the CA (or root) certificate.

Secure Element

A highly secured, tamper-resistant companion device of an MCU used to store and protect confidential and cryptographic data.

Secure Element provisioning

The process of configuring a Secure Element (usually for the 1st time).

Secured cloud provisioning

The act of configuring the cloud instance of the device.

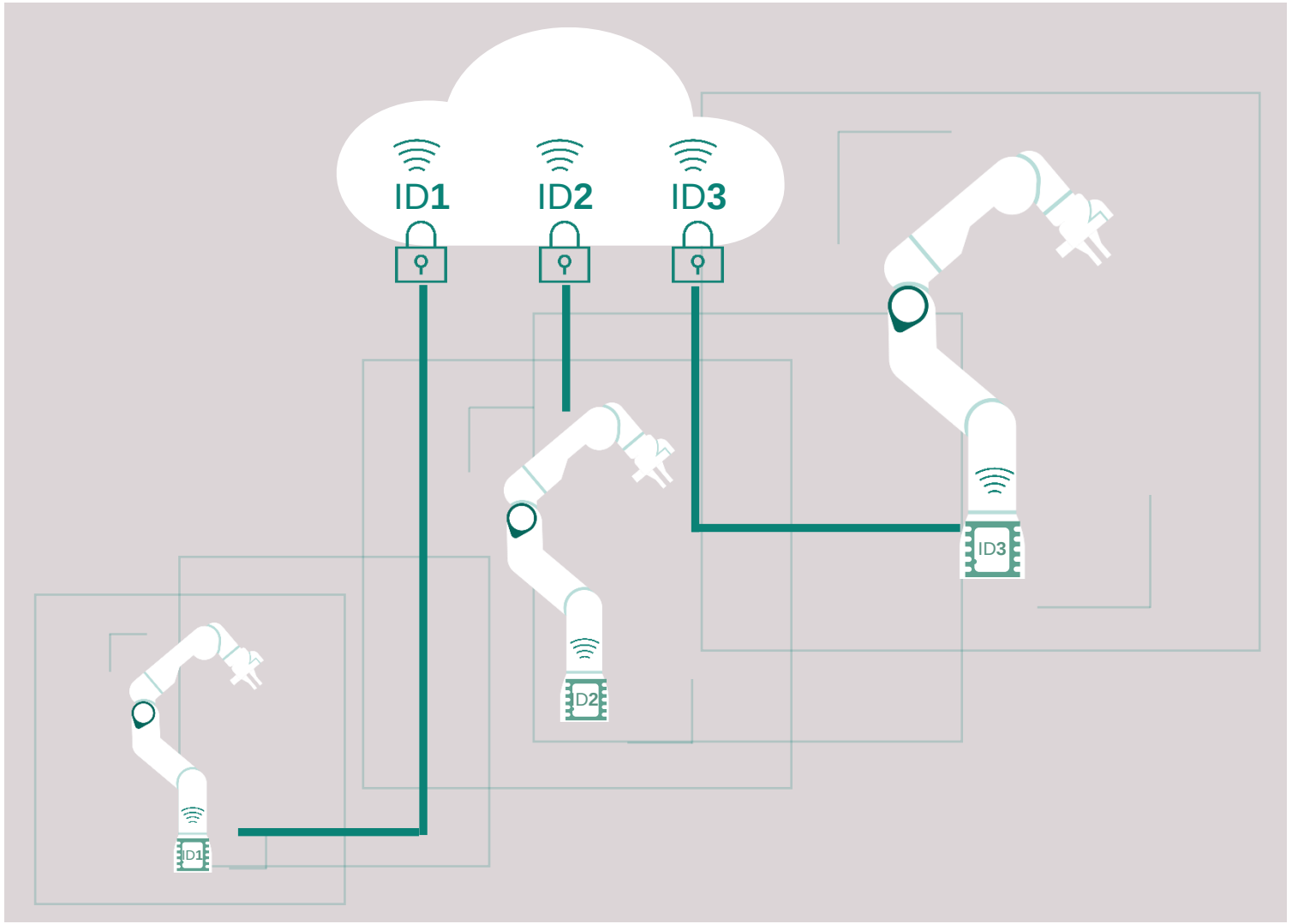
Common criteria

The Common Criteria for Information Technology Security Evaluation (abbreviated as Common Criteria or CC) is an international standard for security certification.

Copyright © Infineon Technologies AG 2024. All rights reserved.

The challenge

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**.



Copyright © Infineon Technologies AG 2024. All rights reserved.

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

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.**



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

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

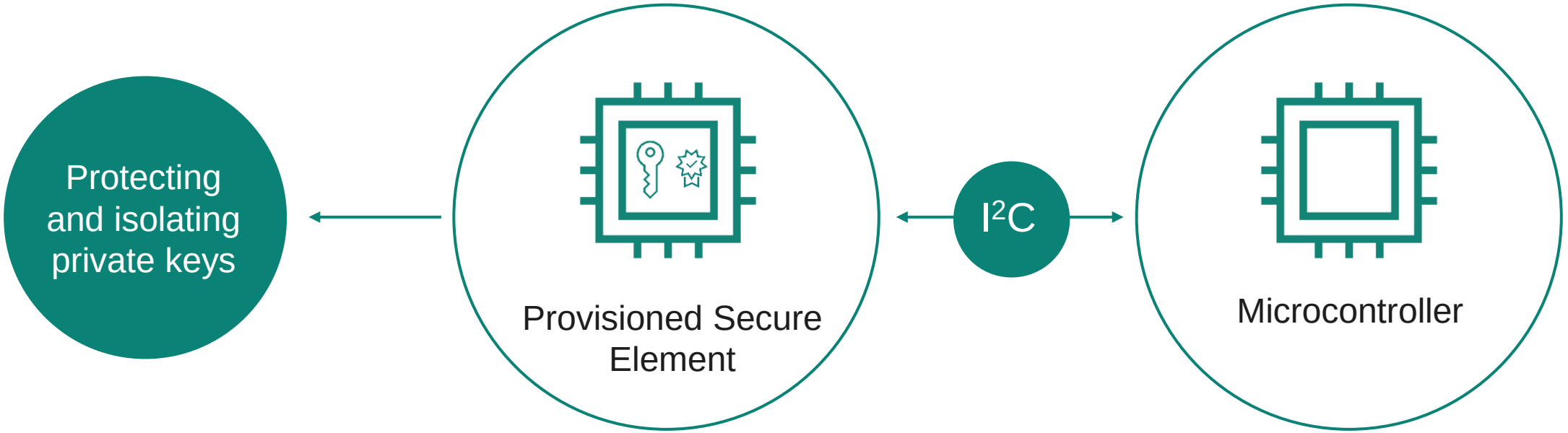
Copyright © Infineon Technologies AG 2024. All rights reserved.

Hardware security is essential for protecting the unique identity of an IoT device

Typical for IoT operations	Software IoT security	Hardware IoT security
Resource-constrained systems	Software code must be run on the same processor that is being protected → may lead to reduced performance	The cryptographic operations are run on a separate device
Often remote locations	Difficult to update the operating system in the field	Designed to resist attacks over long periods of time without intervention
A need for strong protection against complex threats	Software code is easily analyzed and understood using standard tools; relatively easy to alter or damage	Physically isolated data in silicon is highly stable and resistant to change

Copyright © Infineon Technologies AG 2024. All rights reserved.

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



Provisioning alternative 1

On the OEM/CM manufacturing line

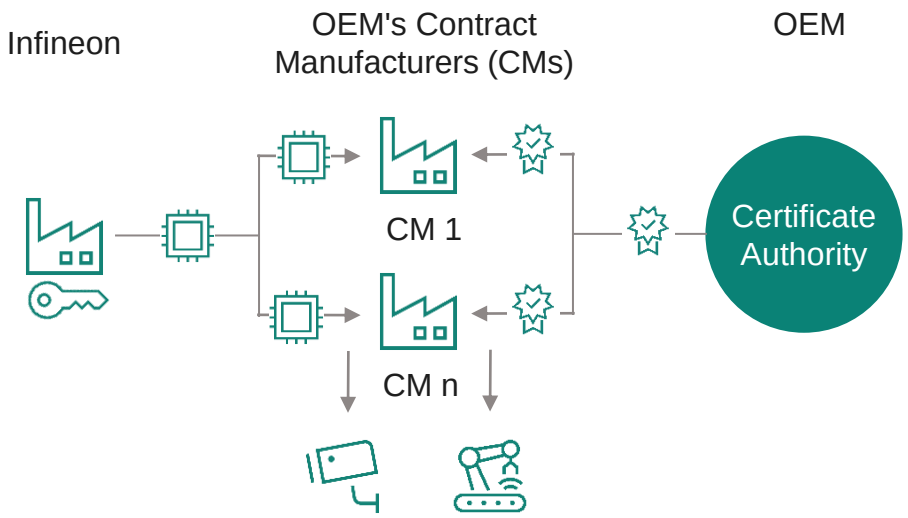
Provisioning alternative 2

At the semiconductor facility (pre-provisioning)

Copyright © Infineon Technologies AG 2024. All rights reserved.

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

Provisioning at Original Equipment Manufacturer (OEM)



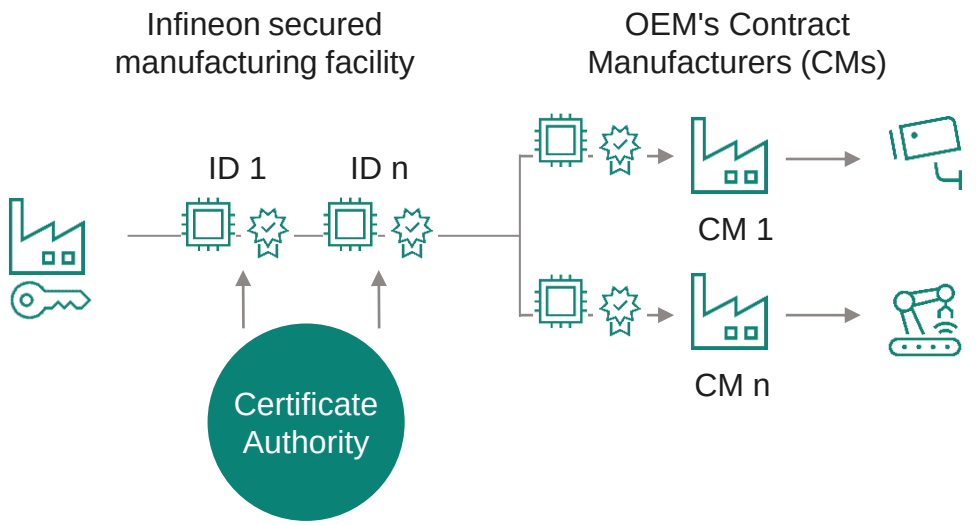
Higher cost for OEM

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

Higher risk for OEM

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

Provisioning at semiconductor facilities



Cost optimization for OEM

- No need for secured manufacturing capabilities at CMs
- Semiconductor provider acts as CA

Higher security for OEM

- IDs are injected in a certified facility, establishing a Chain of Trust from silicon to IoT device
- No data transfers between manufacturing locations → no exposure of IDs

Copyright © Infineon Technologies AG 2024. All rights reserved.

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

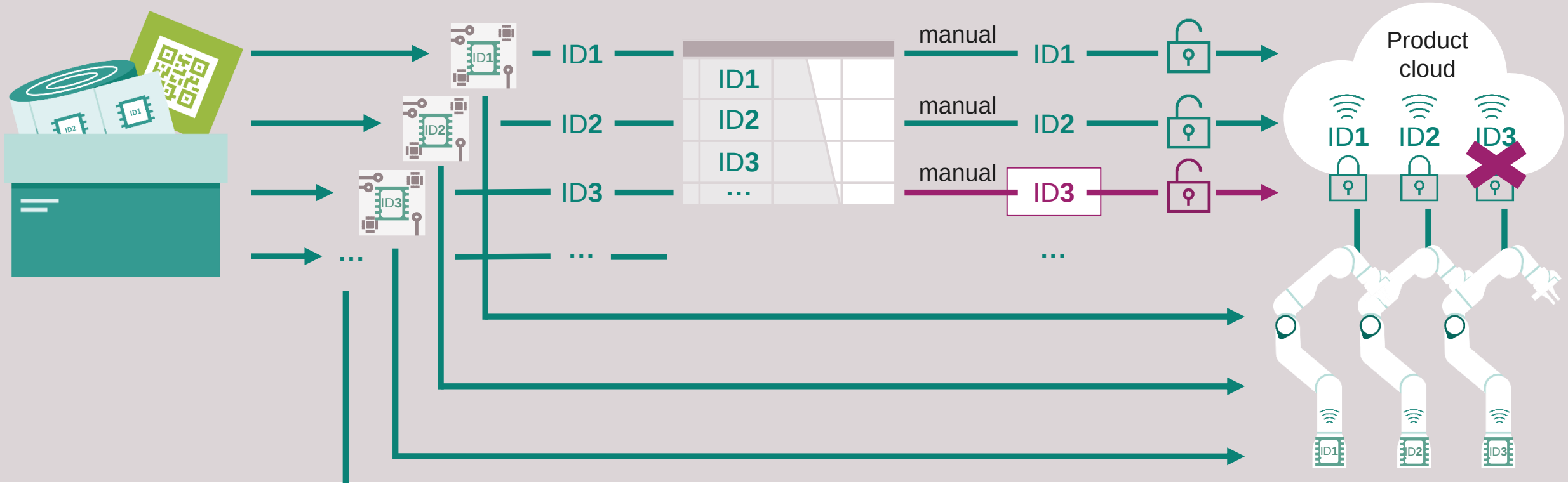
1 Order
Your batch of security chips with pre-provisioned certificates

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

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

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

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



Copyright © Infineon Technologies AG 2024. All rights reserved.

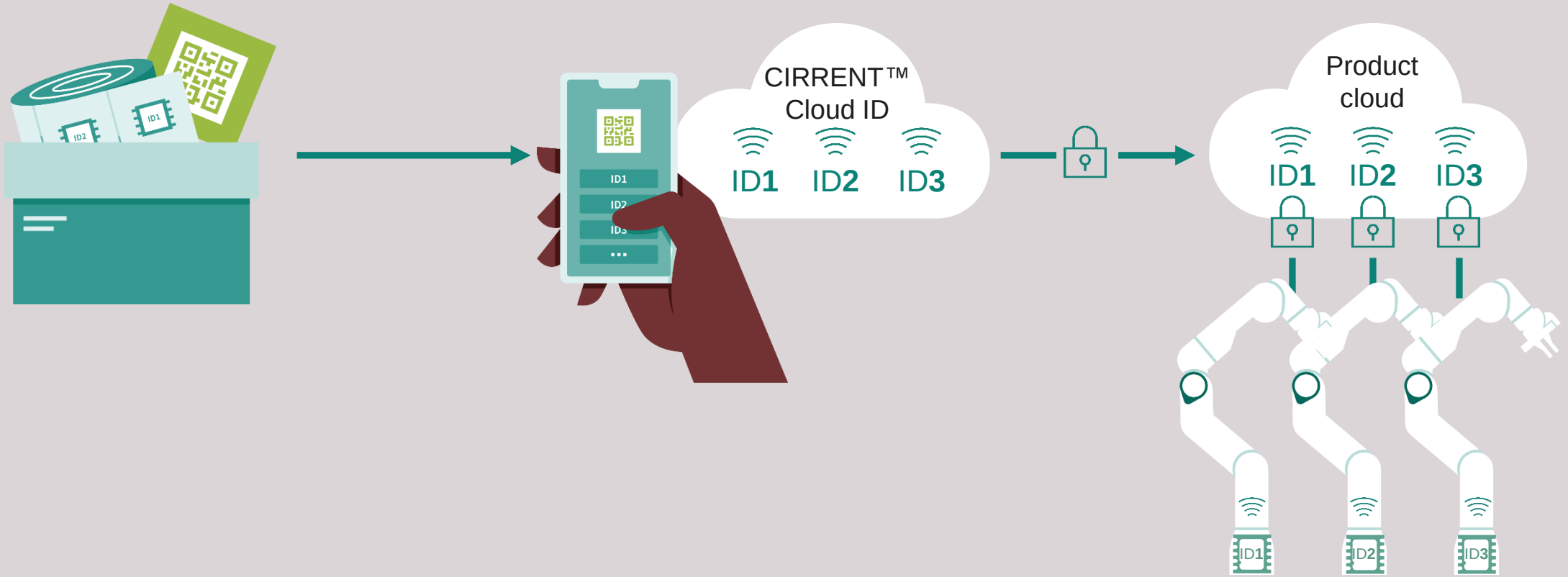
Start personalizing devices at scale with Infineon's secured, automated cloud capabilities

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

1 Order
No exposure of IDs during the manufacturing process

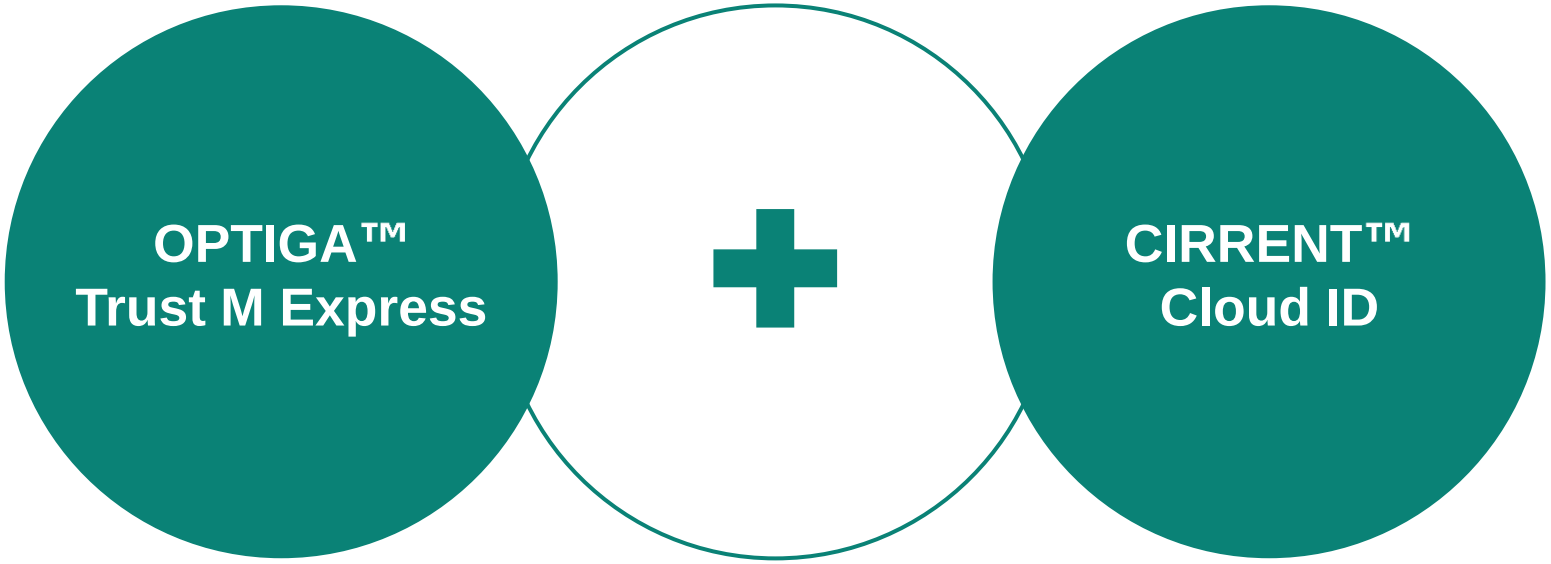
2 Claim
Automated cloud provisioning

3 Connect
The entire process is now automated



Copyright © Infineon Technologies AG 2024. All rights reserved.

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



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

An Infineon cloud service launched in Oct 2021 that automates IoT device certificate registration and the provisioning of the device in the product cloud.

Copyright © Infineon Technologies AG 2024. All rights reserved.

How it works

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

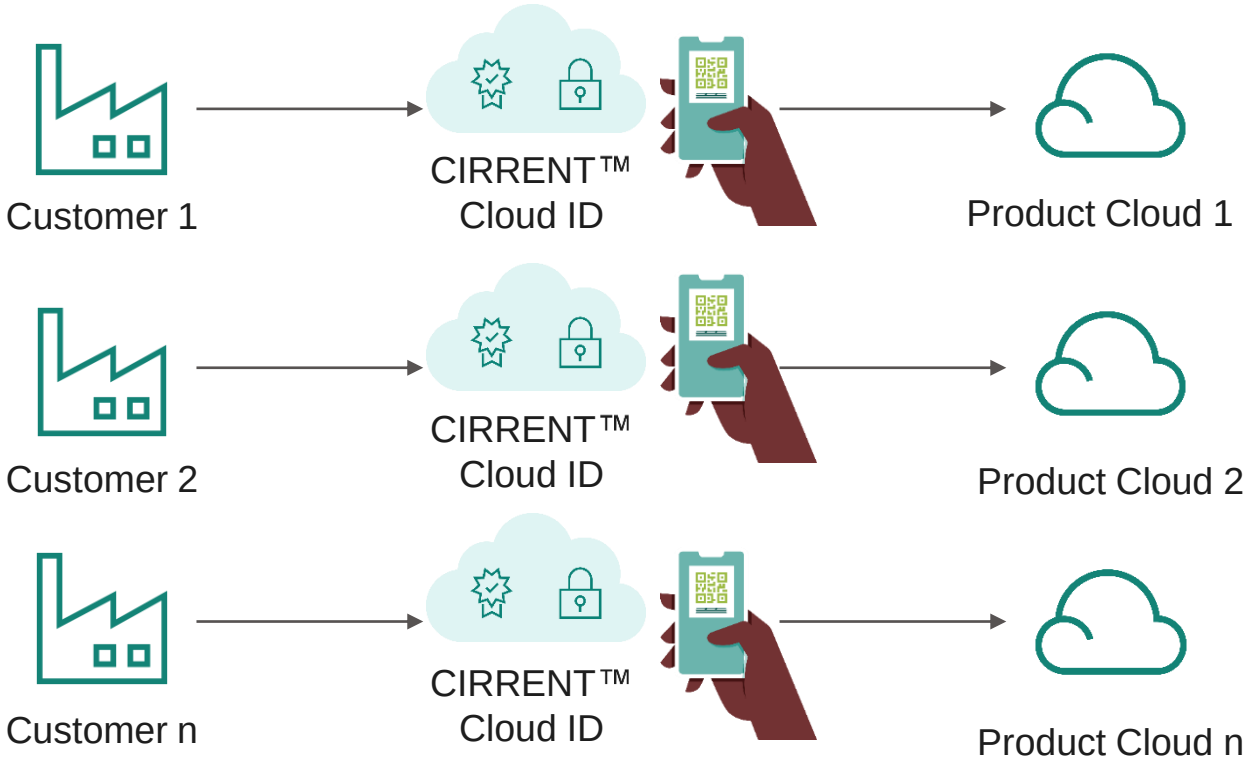
Infineon's Public Key Infrastructure (PKI)

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









Copyright © Infineon Technologies AG 2024. All rights reserved.

The device claiming process in three quick steps



1 Each reel comes with an envelope containing a QR code, Reel ID (a unique alphanumeric reel identifier) and instructions.

Log onto Cloud ID from any browser to insert the product cloud coordinates and configure the automation.
Note: you do not need to include your product cloud credentials for this step.

2 An Operator scans the QR code using any smartphone, and binds the reel to the product cloud.

Alternatively, you can log onto Cloud ID and type in the Reel ID to bind the reel to the product cloud.

3 The certificates are automatically registered on your product cloud and the product is provisioned on the cloud.

Copyright © Infineon Technologies AG 2024. All rights reserved.

OPTIGA™ Trust M Express + CIRRENT™ Cloud ID: Features and applications deep dive

You can count on us



- 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

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

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

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

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

Copyright © Infineon Technologies AG 2024. All rights reserved.

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

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 your cloud
- **Simplified Device Customization**
  No need for personalization in a highly secured manufacturing environment
- **Only Authenticated Devices attach to Product Cloud**
  Firewall can prevent unauthorized or spoofed devices from sending data to your product cloud

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

Copyright © Infineon Technologies AG 2024. All rights reserved.

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+ (high) certified hardware
- Support for all latest symmetric and asymmetric cryptographic algorithms
- Unique and protected identity pre-provisioned in a CC certified facility
- Protection against data breeches and human errors as IDs are handled in a closed system

Copyright © Infineon Technologies AG 2024. All rights reserved.

Application examples



Smart City

Street lights



Smart Mobility

EV charging authentication, E-scooters



Smart building

Commercial smart HVAC



Smart home

Residential aircon, large home appliances



Industrial IoT

Cyber security



Healthcare

Connected dental equipment, connected toothbrush

Typical use cases

Secured cloud authentication, secured cloud communication, crypto offloading, secured software updates, IP protection, trust anchor

Copyright © Infineon Technologies AG 2024. All rights reserved.

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

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

Copyright © Infineon Technologies AG 2024. All rights reserved.

How to get started

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



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

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

Copyright © Infineon Technologies AG 2024. All rights reserved.

Why the OPTIGA™ family and why Infineon

Infineon's OPTIGA™ family: flexibility, robust security, ease of use and a commitment to quality, supply and support

- Scaling from basic authentication chips to sophisticated implementations
- Designed for easy integration into embedded systems
- Robust protection of the confidentiality, integrity and authenticity of information and devices
- A trusted advisor with 30+ years of expertise in hardware security, helping you to reduce complexity and implementation costs



Copyright © Infineon Technologies AG 2024. All rights reserved.

Our solutions come with service and support



We support you by…

- Providing Design-In Application Notes for our products
- Host side integration support
- Evaluation kits

- Providing a secured Public Key Infrastructure
- Custom certificate loading in secured production environment

- Answering questions immediately
- Two-level customer service

- Providing trainings for our security products
- Showing Demo Applications as a starting point for custom designs

Copyright © Infineon Technologies AG 2024. All rights reserved.

You can count on us

Extensive track record and reliable logistics

> 2,5 billion

Securiy ICs shipped every year

Best partner network

50+ partners

for security

Most trustworthy and innovative network of partners in the security space

Shaping tomorrow's standards

> 100

standardization bodies

Driving standardization bodies like GSMA, ETSI, Global Platform, 3GPP, and NFC Forum

Strong innovation power

> 25,000

patents

7,161 R&D employees; 11% of Infineon's revenue goes into R&D

Copyright © Infineon Technologies AG 2024. All rights reserved.

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



Key Takeaways

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

Copyright © Infineon Technologies AG 2024. All rights reserved.

For more information, visit the OPTIGA™ Trust M Express page

Order online the OPTIGA™ Trust M IoT Security Development Kit

Visit GitHub for the Open Source, NDA-free OPTIGA™ Trust M host software and all product documentation




Infineon