

# OPTIGA™ Trust M MTR

## The easy way to add Matter and security to your smart home devices

public

# Table of contents


1 A matter of simplicity - introduction to the Matter smart home standard 3

2 A matter of security - how Matter gives you a peace of mind 7

3 Challenges in enabling Matter-based smart home devices 10

4 Introducing OPTIGA™ Trust M MTR 13

5 Getting started 24

6 Key takeaways 26



Copyright © Infineon Technologies AG 2024. All rights reserved.

# Table of contents


1 **A matter of simplicity - introduction to the Matter smart home standard** **3**

2 A matter of security - how Matter gives you a peace of mind 7

3 Challenges in enabling Matter-based smart home devices 10

4 Introducing OPTIGA™ Trust M MTR 13

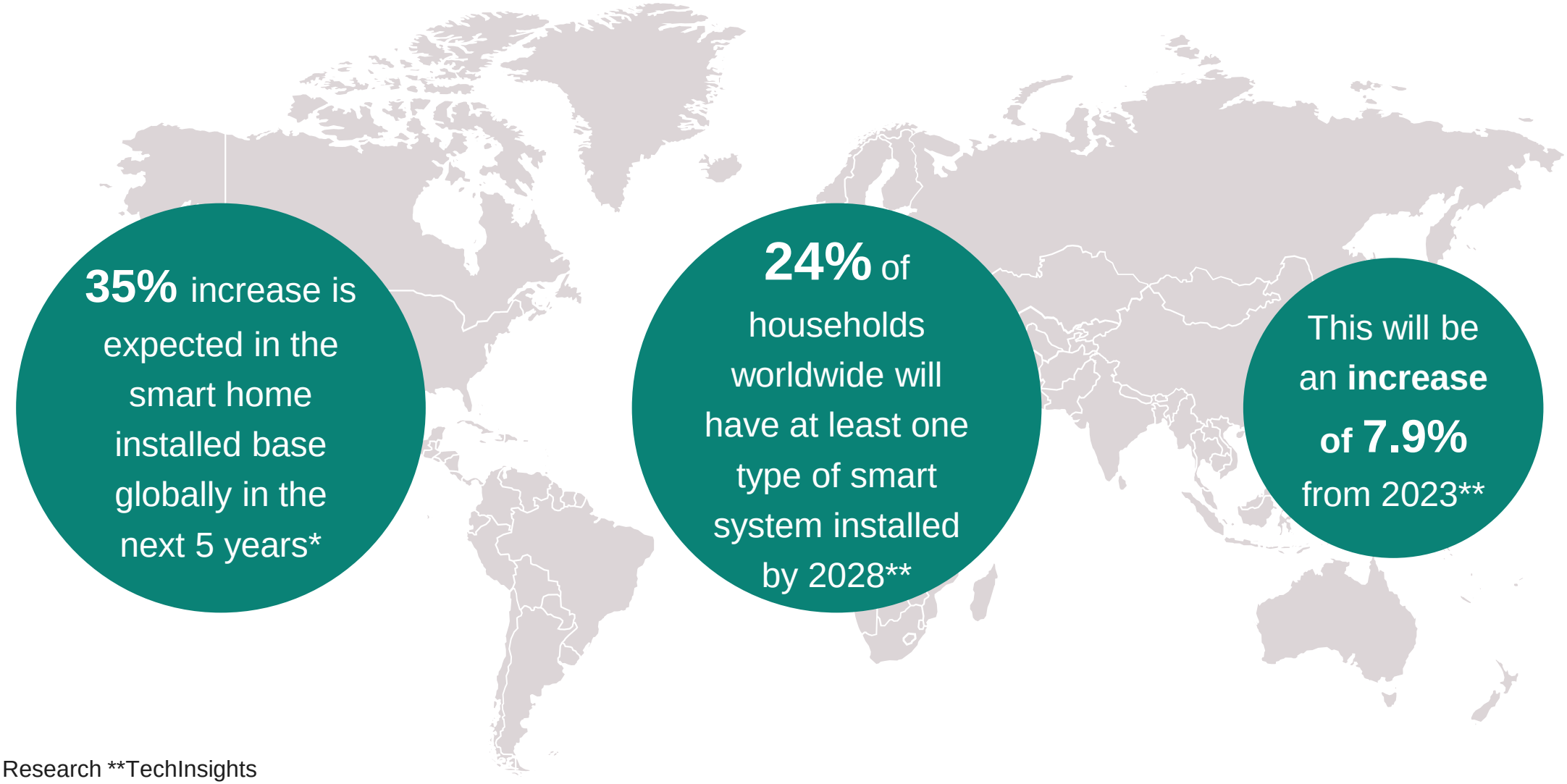
5 Getting started 24

6 Key takeaways 26



Copyright © Infineon Technologies AG 2024. All rights reserved.

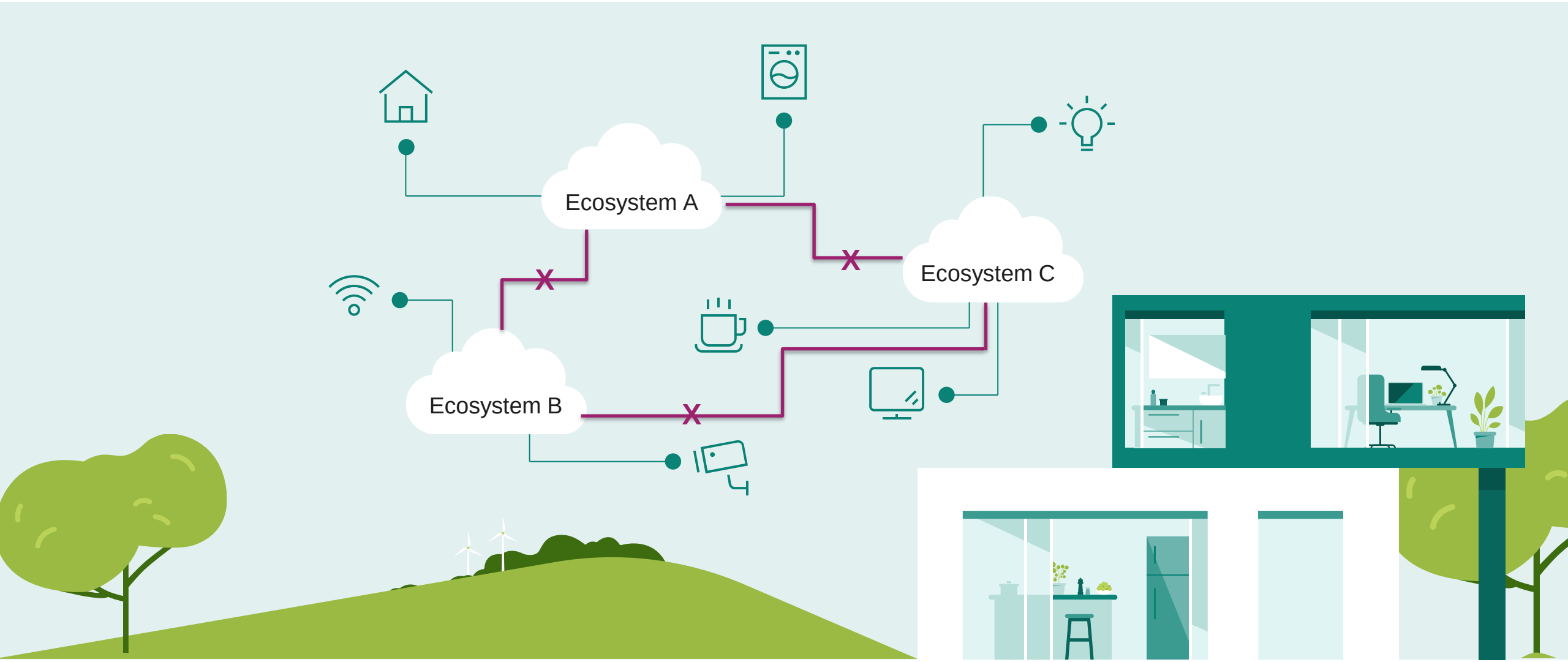
# The smart home market is growing




*ABI Research **TechInsights


Copyright © Infineon Technologies AG 2024. All rights reserved.

# Lack of interoperability is still an issue in smart homes





Copyright © Infineon Technologies AG 2024. All rights reserved.

# Matter

A new unifying protocol to connect smart home devices securely and reliably to each other and to the various popular smart home ecosystems.

Matter defines a set of principles in support of consistent security and privacy measures for the smart home.

CSA is developing, promoting and certifying the Matter connectivity standard

- On CSA Board of Directors
- A leader and contributor in Matter security groups

- **600+ companies** engaged in developing the specification
- **5.5B+** Smart Home Matter-compliant devices will ship by 2030[1]

## Some of CSA's key members and promoters of Matter[2]

[1]Source: ABI research, Matter and its smart home impact, Jan 21, 2022

[2] Source: https://csa-iot.org/members/

Copyright © Infineon Technologies AG 2024. All rights reserved.

# Table of contents


1 A matter of simplicity - introduction to the Matter smart home standard 3

2 **A matter of security - how Matter gives you a peace of mind** **7**

3 Challenges in enabling Matter-based smart home devices 10

4 Introducing OPTIGA™ Trust M MTR 13

5 Getting started 24

6 Key takeaways 26



Copyright © Infineon Technologies AG 2024. All rights reserved.

# The impact of security threats in a smart home

## Unauthorized access

Unauthorized monitoring, theft of personal information, physical harm

## Data privacy

Ranging from targeted advertising to identity theft

## Malware and cyberattacks

Infiltration of home networks; launch attacks on other systems



**Potential impacts on users**

- Personal safety
- Invaded privacy
- Disrupted services

**Potential impacts on brands**

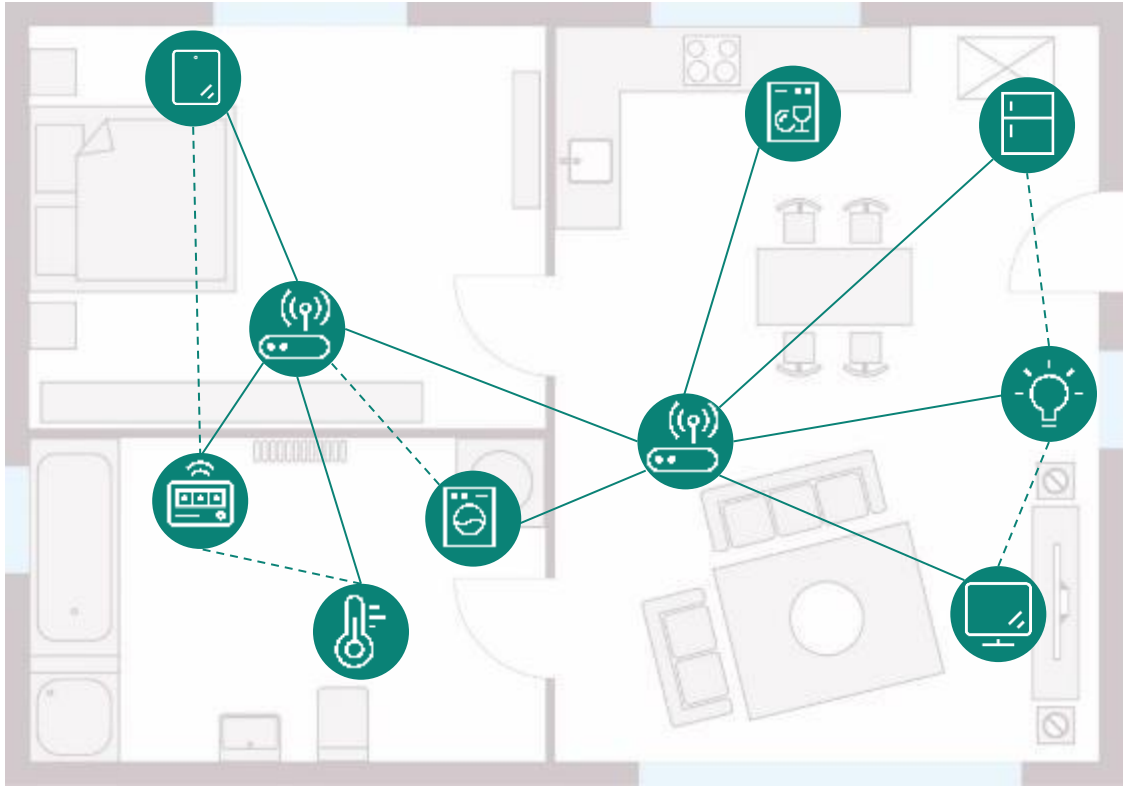
- Reputation damage
- Financial loss
- Liability


Copyright © Infineon Technologies AG 2024. All rights reserved.

# Security and Matter go hand-in-hand

## Matter raises the bar for IoT security and privacy*

1. Easy, secure, and flexible device commissioning
2. **Validation that each device is authentic and certified**
3. **Up-to-date info via Distributed Compliance Ledger**
4. **Strong device identity so only your devices can join your smart home**
5. Secured unicast communications
6. Secured group communications
7. Multiple administrators and controllers, maximizing choice
8. Verified access controls to prevent unauthorized actions
9. Secured, standard software updates
10. Verification of software integrity



*List source: Connectivity Standards Alliance (CSA)


Copyright © Infineon Technologies AG 2024. All rights reserved.

# Table of contents


1 A matter of simplicity - introduction to the Matter smart home standard 3

2 A matter of security - how Matter gives you a peace of mind 7

3 **Challenges in enabling Matter-based smart home devices** **10**

4 Introducing OPTIGA™ Trust M MTR 13

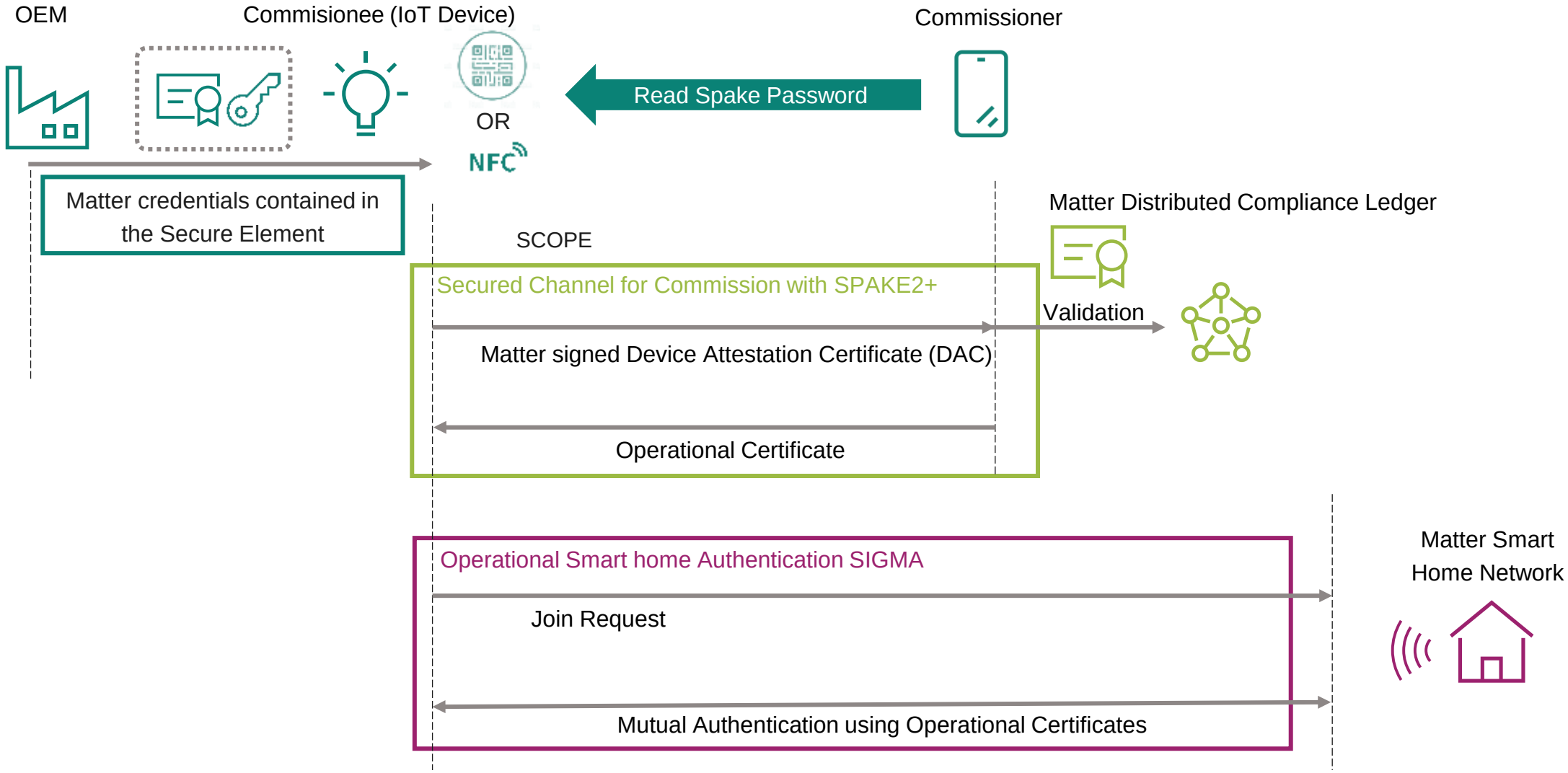
5 Getting started 24

6 Key takeaways 26



Copyright © Infineon Technologies AG 2024. All rights reserved.

# Matter onboarding flow





Copyright © Infineon Technologies AG 2024. All rights reserved.

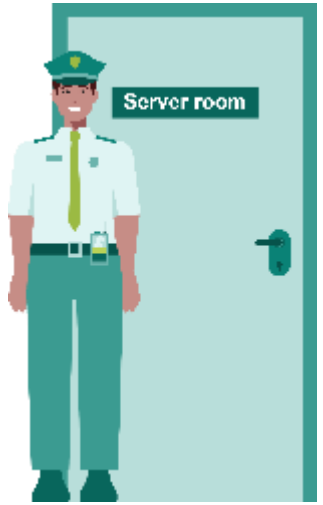
# Building Matter devices the old way



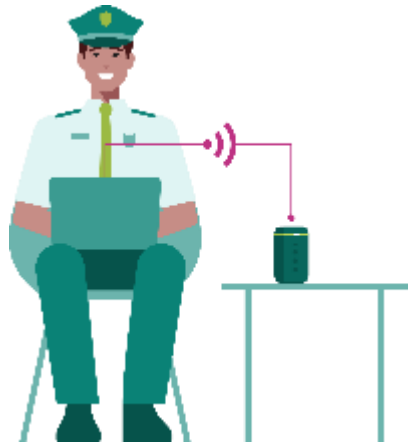
**1. Create Root CA**
Highly secured signer in secured facility



**2. Create Intermediate CAs**
Signers that issue DACs




**3. Install Intermediate CAs**
Place in secured location at each factory with trusted operator



**4. Install DACs**
Generate DACs and install into devices in factory

## Expensive, complex, risky, and disruptive


Copyright © Infineon Technologies AG 2024. All rights reserved.

# Table of contents


1 A matter of simplicity - introduction to the Matter smart home standard 3

2 A matter of security - how Matter gives you a peace of mind 7

3 Challenges in enabling Matter-based smart home devices 10

4 **Introducing OPTIGA™ Trust M MTR** **13**

5 Getting started 24

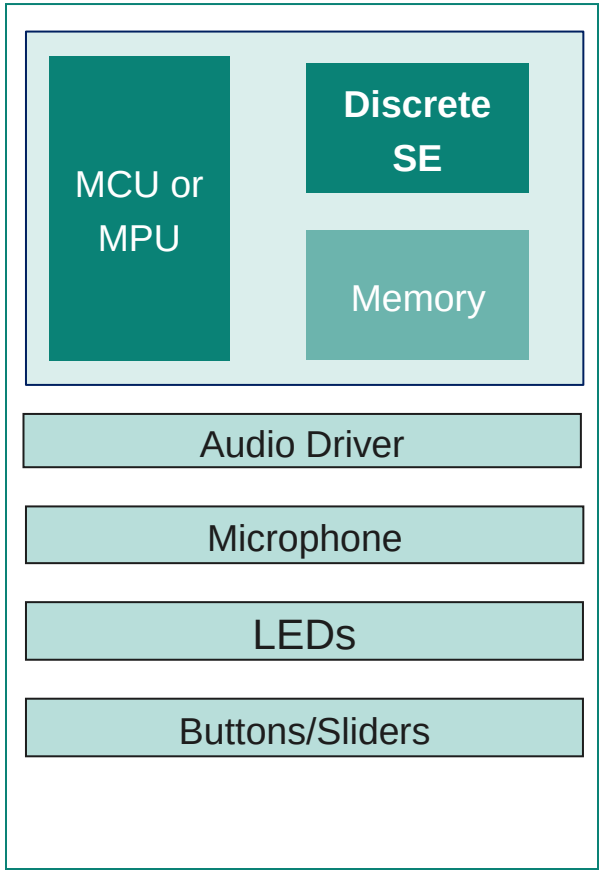
6 Key takeaways 26



Copyright © Infineon Technologies AG 2024. All rights reserved.

# Simplifying the Matter onboarding flow with a discrete Secure Element (SE)

A discrete Secure Element is a specialized, tamper-resistant companion of an MCU that can be added to a system to perform security-related functions

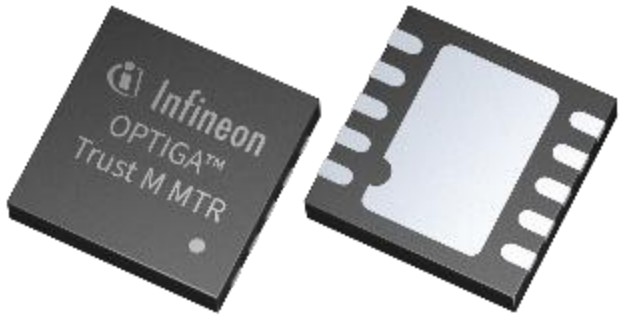






Copyright © Infineon Technologies AG 2024. All rights reserved.

# Introducing OPTIGA™ Trust M MTR

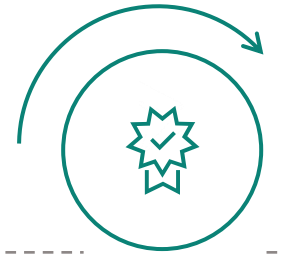
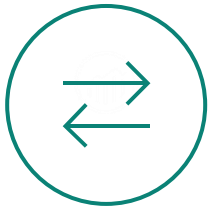



OPTIGA™ Trust M MTR is Infineon's OPTIGA™ Trust M discrete security solution with a Matter provisioning service

## The easy way to add secured Matter compatibility to your existing design

Copyright © Infineon Technologies AG 2024. All rights reserved.

# OPTIGA™ Trust M MTR is the easy way to add secured Matter compatibility to your existing design

| Challenges | | Solution |
|---|---|---|
| Provisioning of Matter certificates |  | OPTIGA™ Trust M MTR is a pre-provisioned discrete SE which simplifies the process of adding Matter certificates to your devices. |
| Time to market |  | OPTIGA™ Trust M MTR allows to keep your existing design as it can be inserted into any MCU/SoC design |
| Flexibility |  | With OPTIGA™ Trust M MTR DACs can be downloaded right up until the start of production. This gives OEMs the flexibility to decide on product variants after ordering the security chips. |
| Security of smart home devices |  | Based on CC EAL 6+ (high) certified hardware, OPTIGA™ Trust M MTR can achieve consistent tamper-resistant protection supported by the Matter standard. |


Copyright © Infineon Technologies AG 2024. All rights reserved.

# Matter hierarchy

Every Matter device must come with a **unique identity**, which shows that this is a certified and authentic Matter device. This is provided by the device attestation certificate

### Matter Product Attestation Authority (PAA)

– PAA is a CSA certified member, authorized to issue Matter DACs

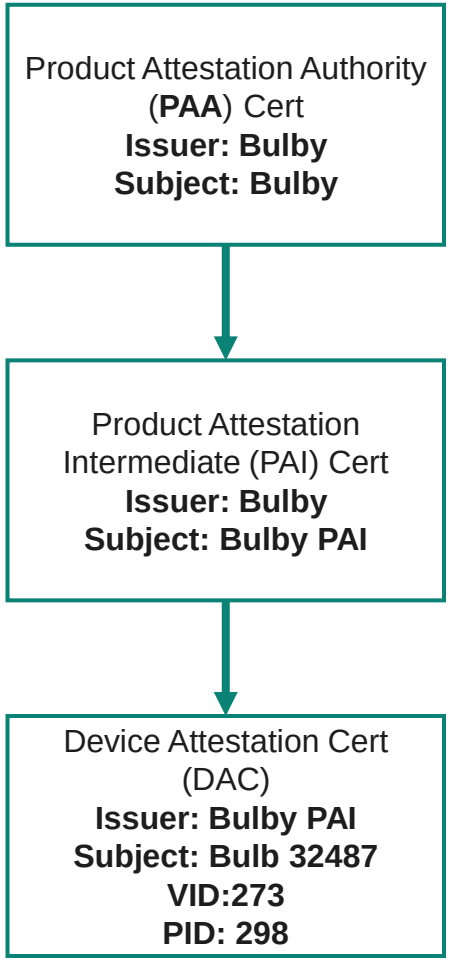
### Vendor Product Attestation Intermediate (PAI)

– PAA issues an intermediate PAI. PAI includes the member`s CSA vendor ID (VID). As an option, the Product ID (PID) can also be included to generate DAC

### Vendor Device Attestation Certificates (DAC)

– PAA provides certificate services for signing DACs, which includes a PID and VID

– Each product will need a specific DAC assigned by the PAI



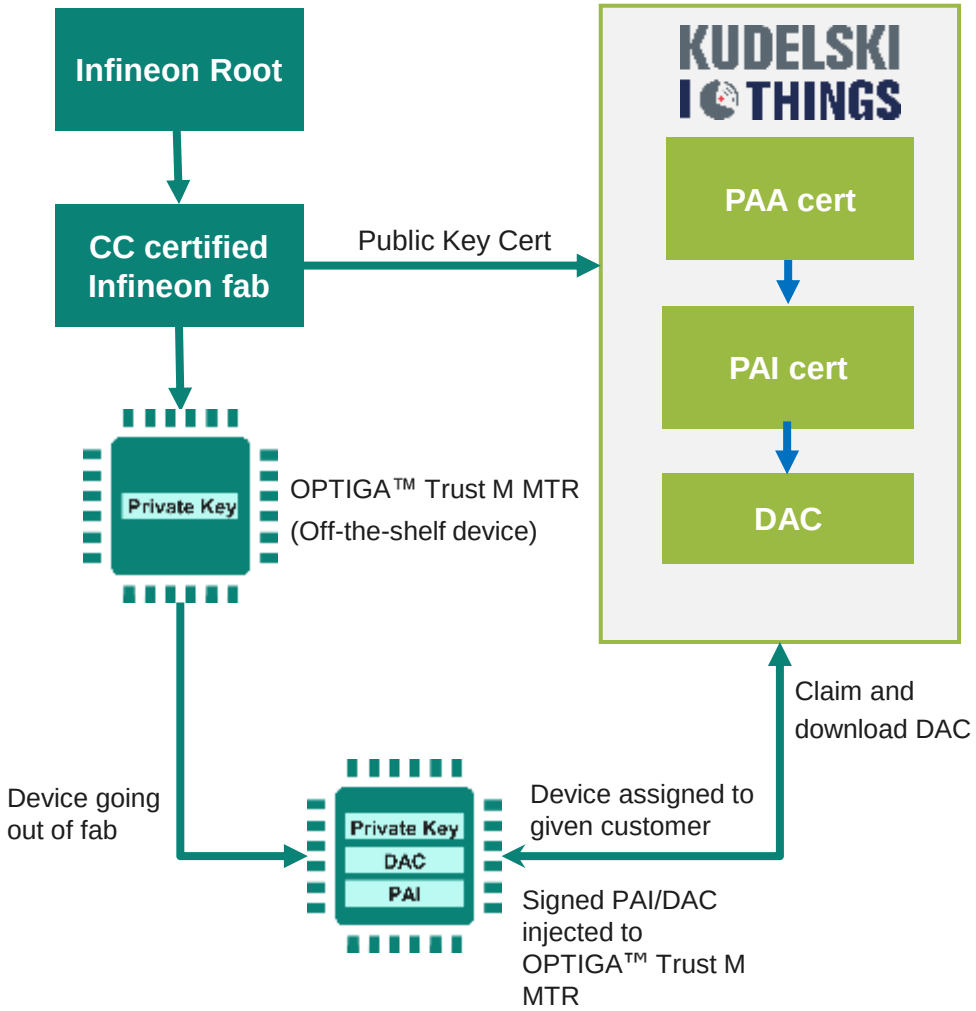


Copyright © Infineon Technologies AG 2024. All rights reserved.

# OPTIGA™ Trust M MTR Public Key Infrastructure (PKI) offering

**Infineon certificates and keys are injected in our CC certified fabs**

- Private and public keys are injected into the device
- Private key protected inside the device, making it highly secure
- Device and reel IDs are shared with Kudelski IoT to generate the corresponding DAC
- OPTIGA™ Trust M MTR is an off-the-shelf product

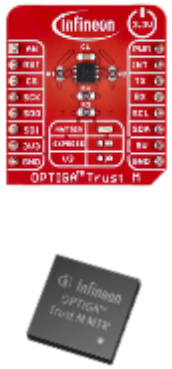



**Late-stage provisioning by Kudelski IoT**

- Late-stage provisioning allows the DACs to be downloaded at the OEM facility during equipment manufacturing.
- PAI and DACs are injected into the device at the OEM's manufacturing facility
- Late-stage provisioning means the PID can be changed right up until the start of production, allowing OEMs to create multiple variants of the end product

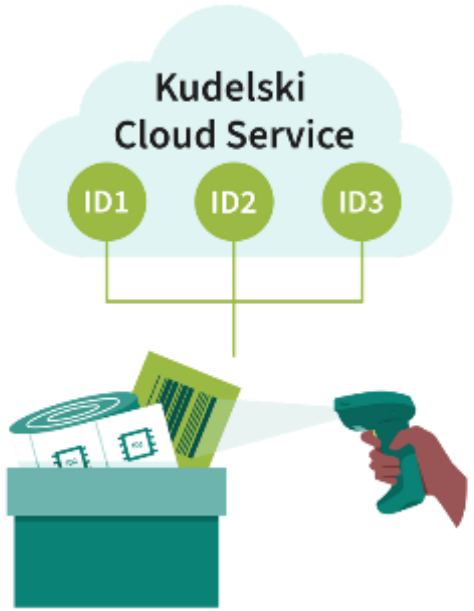

Copyright © Infineon Technologies AG 2024. All rights reserved.

# Building Matter devices with OPTIGA™ Trust M MTR



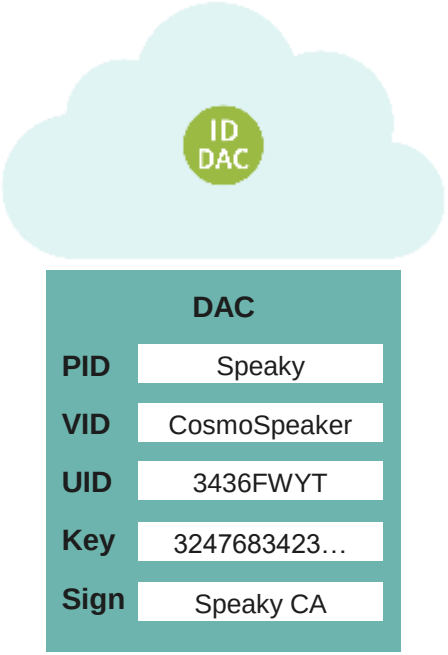
**1. Pre-Production**

Order Kits & Samples
Create DAC for testing samples



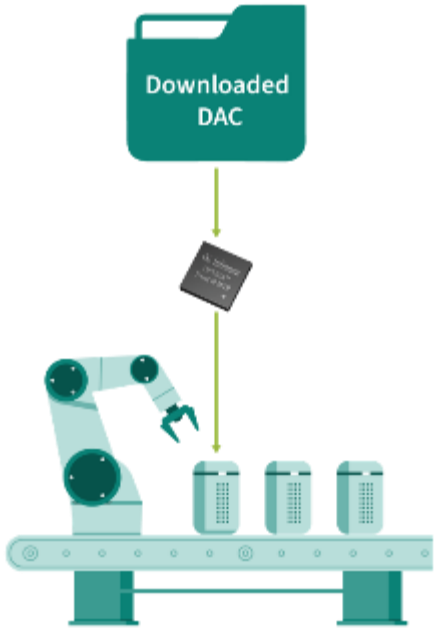

**2. Order & Claim**

Order reel(s) with
pre-provisioned chip IDs
and claim the reel using the ID




**3. Late-stage provisioning**

Update DAC online
(e.g. in case of product change)
and download




**4. DAC insertion**

Insert DACs into
OPTIGA™ Trust M MTR
in assembly line

## Simple, easy, and secured

# OPTIGA™ Trust M MTR can be used for any smart home application



**Lighting**



**Blinds/Shades**



**Climate Control**



**Television**



**Access Control**



**Surveillance camera, alarm**



**Gateway Access Point**



**Speaker**

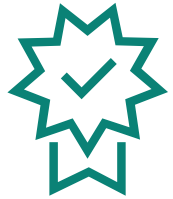
**... and many more**

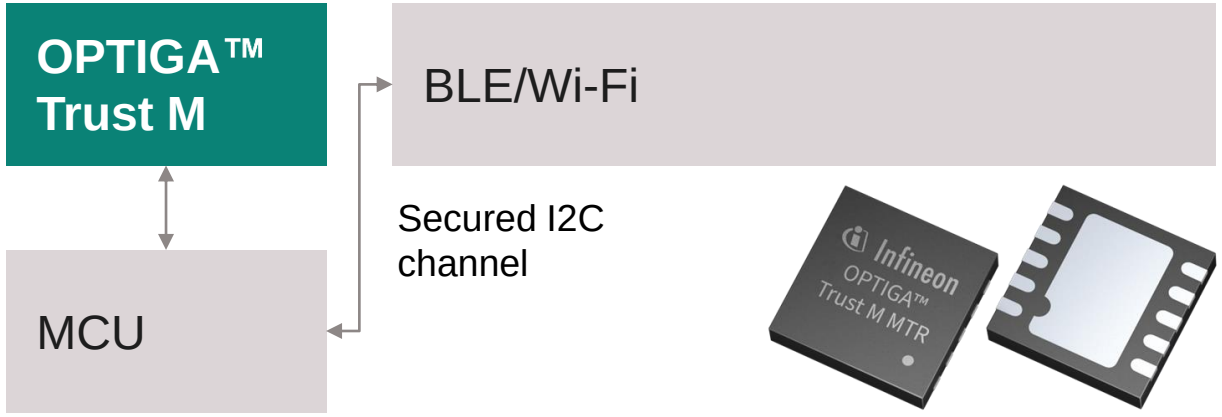

Copyright © Infineon Technologies AG 2024. All rights reserved.

# OPTIGA™ Trust M MTR detailed product overview

## Key Features

- Enabling Matter and Security for Smart Home Devices in a faster way
- Pre-provisioned ECC & RSA Certificates for quick onboarding
- Matter-Certified PKI services offered by Kudelski IoT
- Matter DAC Authentication based on ECDSA NIST P256
- Common Criteria EAL6+ (high) certified hardware
- Cryptography support: (Up to) ECC-512, RSA-2k, AES-256, SHA256
- I2C serial communication
- USON10-2/4 package (3x3mm)
- Extended temperature range available for consumer electronics and industrial applications
- Public Software Framework on Github
- Full turnkey solution incl. drivers/SW library/certificate(s) & key pair(s) implementation






## Product details

| | |
|---|---|
| **Sales codes** | SLS32AIA010MM (standard temperature range) |
| **Application** | Matter Nodes and Hubs |
| **Memory** | Up to 10kB user memory |
| **Cryptography** | ECC-256/RSA-2k/AES-256 |
| **Availability** | Jan 2024 |
| **Temperature** | -25 +85°C |
| **Interface** | I2C |
| **Package** | USON-10 |
| **Size** | 3 x 3 mm |


Copyright © Infineon Technologies AG 2024. All rights reserved.

# OPTIGA™ Trust M is available with different services

## OPTIGA™ Trust M

Provisioned by OEM



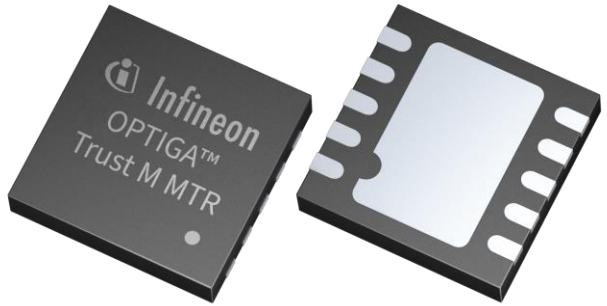

## OPTIGA™ Trust M Express

Pre-provisioned by Infineon




## OPTIGA™ Trust M MTR

Provisioned with Matter certificates




## OPTIGA™ Trust M Fit

Custom provisioning





Copyright © Infineon Technologies AG 2024. All rights reserved.

# The benefits of OPTIGA™ Trust M MTR

- ✓ Easy to add Matter compatibility
- ✓ Works with any MCU/MPU
- ✓ Allows keeping your existing designs
- ✓ Personalized DAC for download
- ✓ High flexibility
- ✓ Allows creation of multiple variants
- ✓ Robust security
- ✓ NDA-free product documentation





Copyright © Infineon Technologies AG 2024. All rights reserved.

# Table of contents


1 A matter of simplicity - introduction to the Matter smart home standard 3

2 A matter of security - how Matter gives you a peace of mind 7

3 Challenges in enabling Matter-based smart home devices 10

4 Introducing OPTIGA™ Trust M MTR 13

5 **Getting started** **24**

6 Key takeaways 26



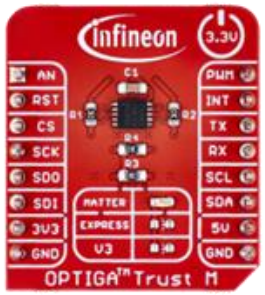
Copyright © Infineon Technologies AG 2024. All rights reserved.

# Evaluation samples and platforms

## Sample Formfactor

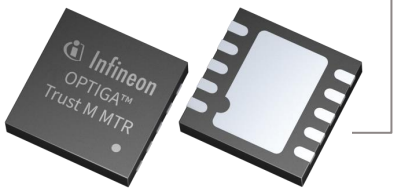
### OPTIGA™ Trust M MTR Shield

- mikroBUS™ Add-on Board
- SP006008195




### OPTIGA™ Trust M MTR Engineering Samples

- 10 pcs in Tray
- SP006031931




## Adapters

### OPTIGA™ Trust Adapter

- Arduino Uno ↔ mikroBUS™
- SP006007975




### MIKROE Pi 4 Click Shield

- Raspberry Pi ↔ MikroBUS™
- Available externally




## Platform

### PSoC62 Pioneer Kit

- PSoC6 with BT/WiFi
- CY8CKIT-062S2-43012
- SP005670449



### Raspberry Pi 4B

- Linux Computer
- Available externally




Copyright © Infineon Technologies AG 2024. All rights reserved.

# Table of contents


1 A matter of simplicity - introduction to the Matter smart home standard 3

2 A matter of security - how Matter gives you a peace of mind 7

3 Challenges in enabling Matter-based smart home devices 10

4 Introducing OPTIGA™ Trust M MTR 13

5 Getting started 24

6 **Key takeaways** **26**



Copyright © Infineon Technologies AG 2024. All rights reserved.

# Key takeaways




OPTIGA™ Trust M MTR is easy way to add secured Matter compatibility to your existing design

OPTIGA™ Trust M MTR is Matter-certified and works across different MCUs/MPUs

OPTIGA™ Trust M MTR offers a novel approach to device attestation: DACs can be assigned right up until the start of production

The pre-provisioned Secure Element is based on CC EAL 6+ (high) certified hardware


Copyright © Infineon Technologies AG 2024. All rights reserved.

# The easy way to add Matter and security to your smart home devices

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




Infineon