



# OPTIGA™ Trust M MTR

The easiest way to add Matter and security to smart home devices

**Steve Hanna**, Distinguished Engineer, Infineon Technologies

22 February 2024



**Steve Hanna** is a Distinguished Engineer at Infineon Technologies. On a global basis, he is responsible for **IoT security strategy and technology**.

As a security expert, Steve is a leader in many standards groups. Within the **Matter Working Group in the Connectivity Standards Alliance**, he is the Vice Lead of the Threat Model Tiger Team, the Lead of the Security Design Tiger Team, and the Lead of the Security Use Cases Tiger Team. He is also **Director on the Alliance's Board and the Chair of the Product Security Working Group**.

Within the Trusted Computing Group, he co-chairs the IoT Work Group. Within the Internet Engineering Task Force (IETF), he is a member of the Security Area Directorate.

Steve Hanna has a deep background in information security, especially in software and systems. He is an inventor or co-inventor on 48 issued patents, the author of innumerable standards and white papers, and a regular speaker at industry events. He holds a Bachelor's degree in Computer Science from Harvard University.



**Steve Hanna**,  
Distinguished Engineer,  
Infineon Technologies

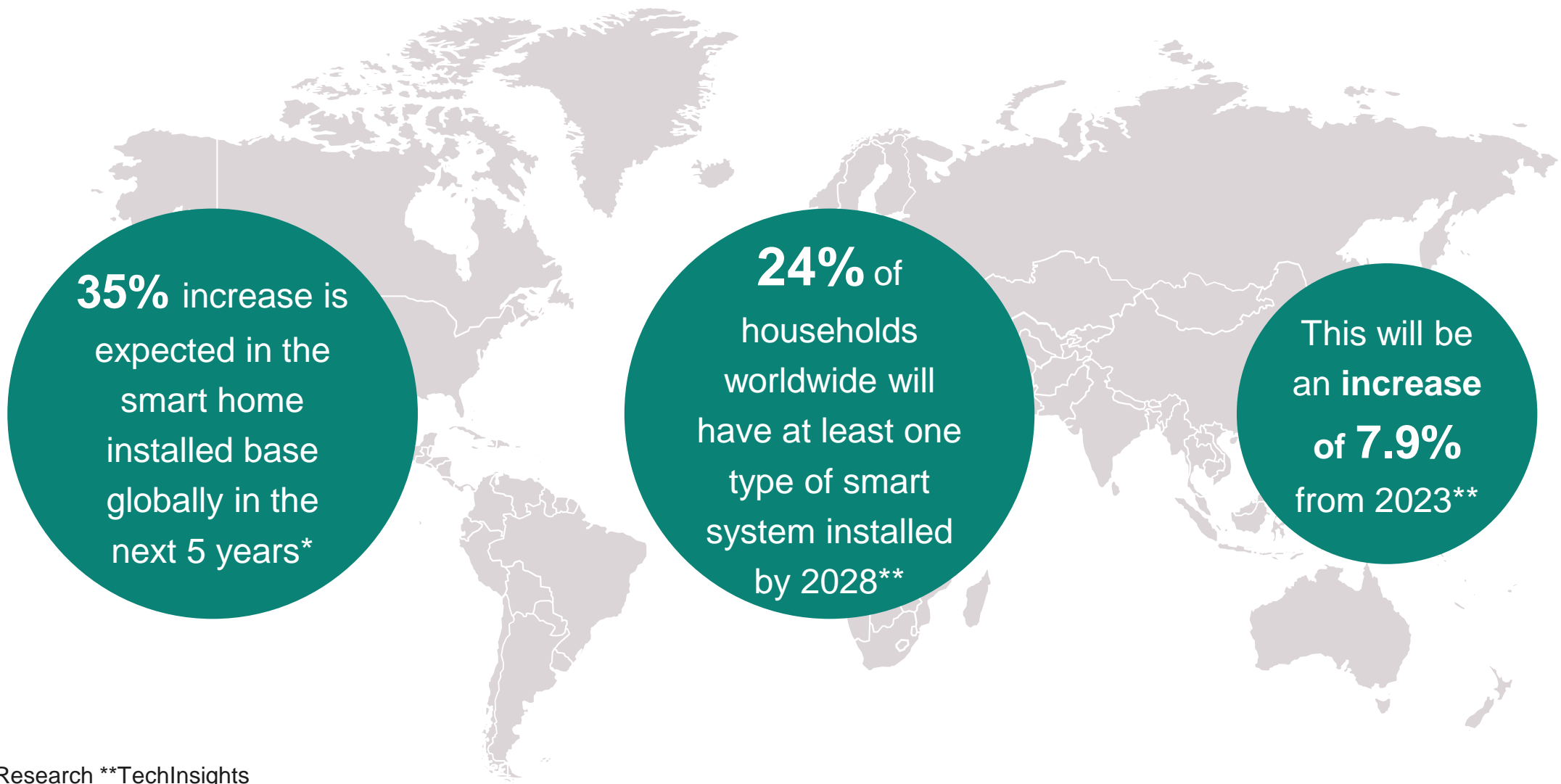
# Table of contents

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	8
3	Challenges in enabling Matter-based smart home devices	11
4	Introducing OPTIGA™ Trust M MTR	14
5	Getting started	20
6	Key takeaways	22

# Table of contents

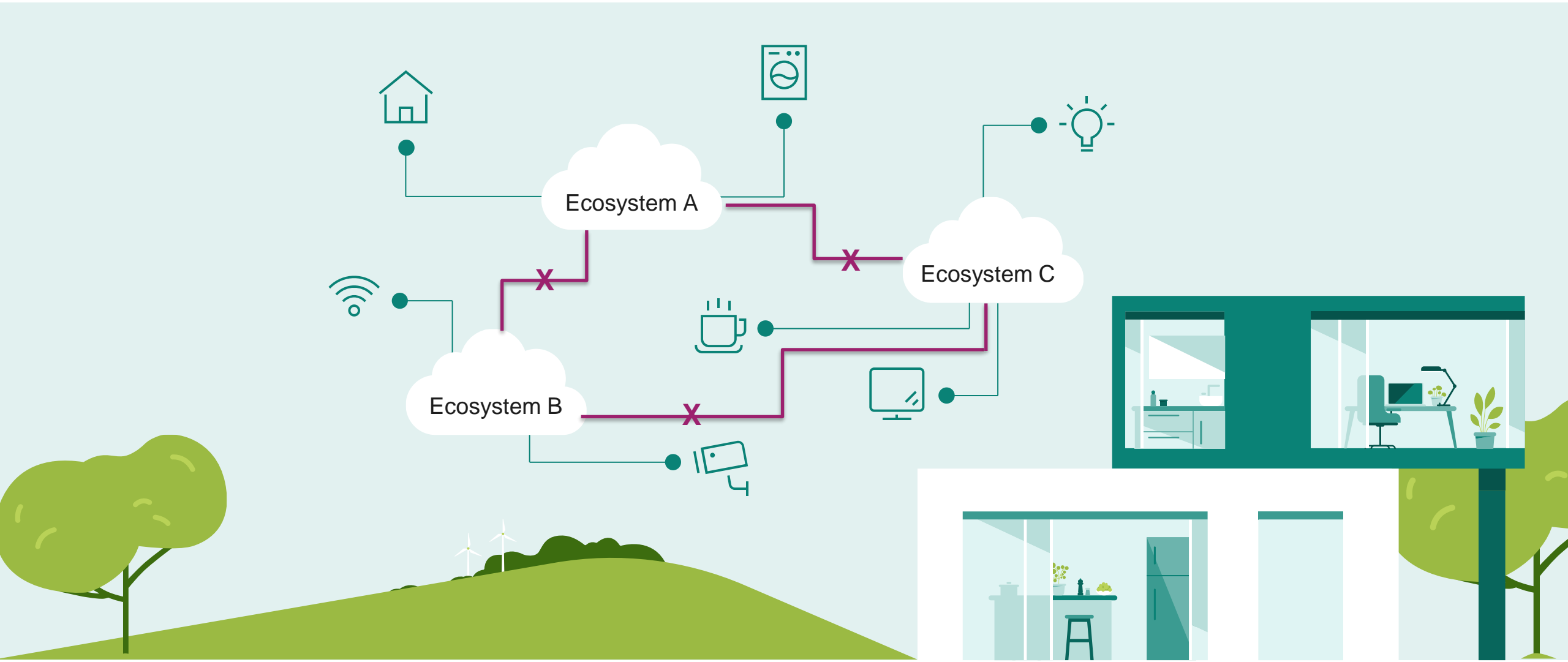
<b>1</b>	<b>A matter of simplicity - introduction to the Matter smart home standard</b>	<b>3</b>
<b>2</b>	A matter of security - how Matter gives you a peace of mind	8
<b>3</b>	Challenges in enabling Matter-based smart home devices	11
<b>4</b>	Introducing OPTIGA™ Trust M MTR	14
<b>5</b>	Getting started	20
<b>6</b>	Key takeaways	22

# The smart home market is growing



\*ABI Research \*\*TechInsights

# Lack of interoperability is still an issue in smart homes



# Matter

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

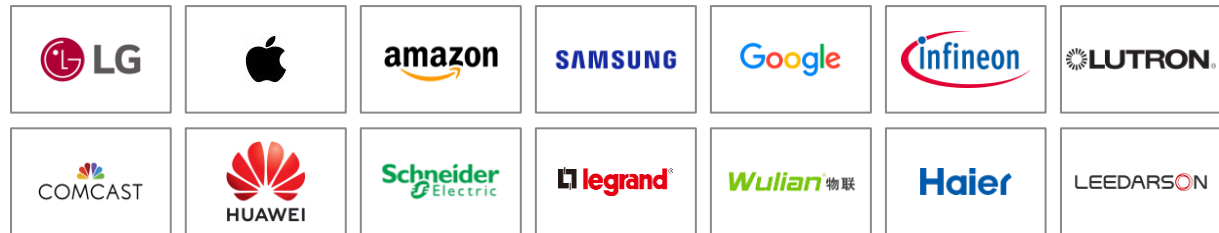
Matter defines a set of principles in support of consistent security and privacy measures for the smart home.



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<sup>1</sup>

## Some of CSA's key members and promoters of Matter<sup>2</sup>



<sup>1</sup>Source: ABI research, Matter and its smart home impact, Jan 21, 2022

<sup>2</sup>Source: <https://csa-iot.org/members/>

# Matter rollout

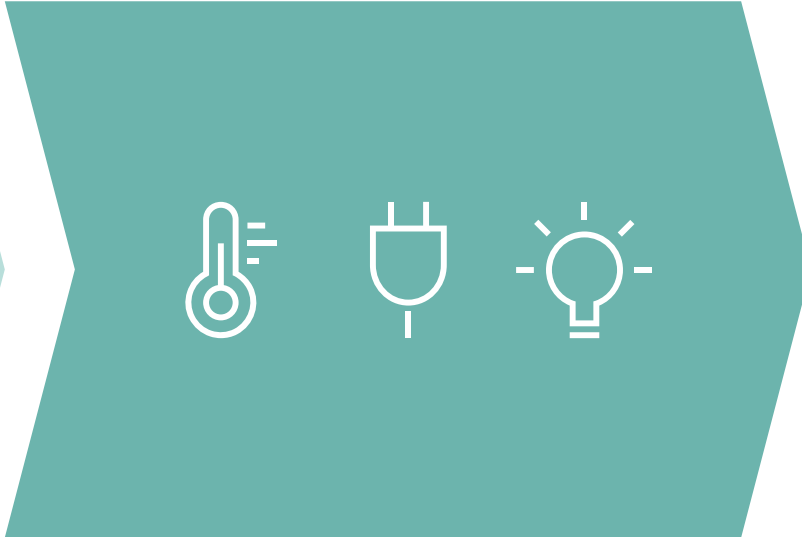
## Phase 1

Controllers and commissioners  
Fall 2022



## Phase 2

Early device makers  
Spring 2023



## Phase 3

Larger product manufacturers  
Fall 2023





# Table of contents

1	A matter of simplicity - introduction to the Matter smart home standard	3
2	<b>A matter of security - how Matter gives you a peace of mind</b>	<b>8</b>
3	Challenges in enabling Matter-based smart home devices	11
4	Introducing OPTIGA™ Trust M MTR	14
5	Getting started	20
6	Key takeaways	22

# 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

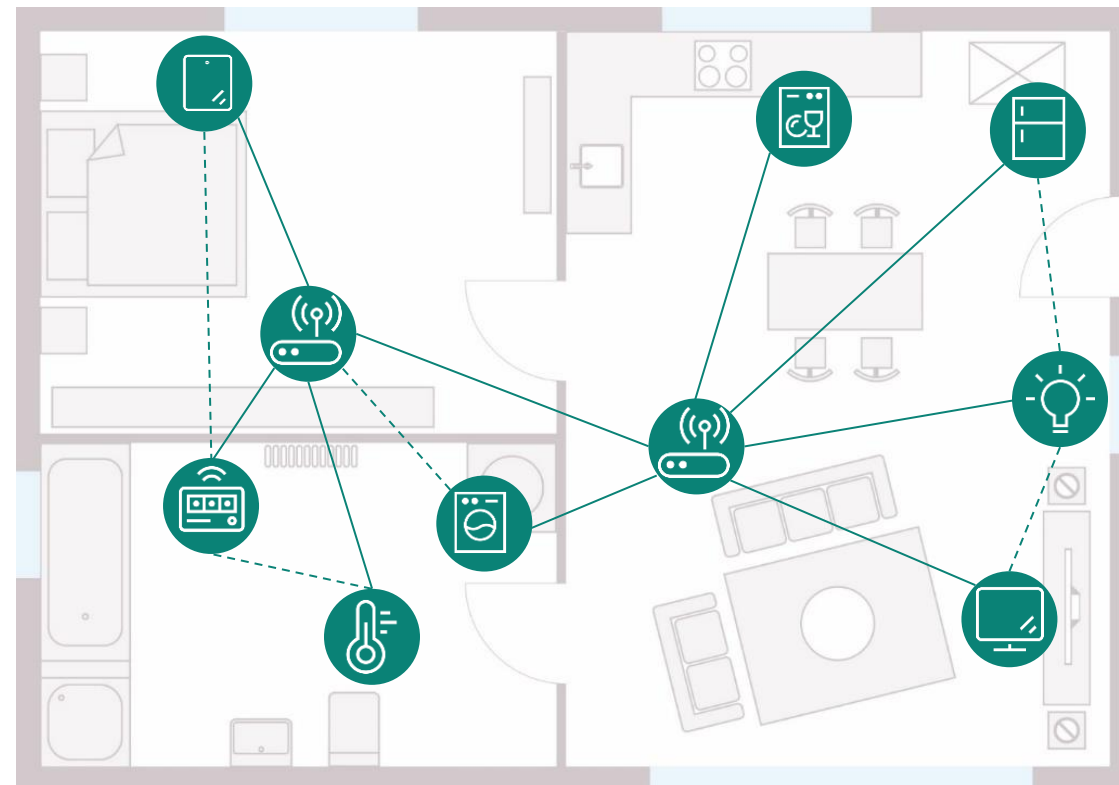
## Potential impacts on brands

- Reputation damage
- Financial loss
- Liability

# 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



\*Source: Connectivity Standards Alliance (CSA)

# 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	8
3	<b>Challenges in enabling Matter-based smart home devices</b>	<b>11</b>
4	Introducing OPTIGA™ Trust M MTR	14
5	Getting started	20
6	Key takeaways	22

# Matter's identity problem

## Every Matter device must come with a unique identity

Known as a Device Attestation Certificate (DAC)

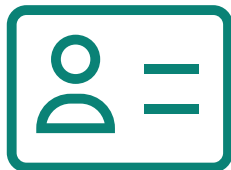
### DAC



PID	Speaky
VID	CosmoSpeaker
UID	3436FWYT
Key	3247683423 ...
Sign	Speaky CA

### What is a DAC?

- Like a driver's license
- Includes identity information
  - Vendor ID (VID), Product ID (PID), unique identity (UID), and public key
- Signed by a trusted authority



### Why include a DAC?

- Verifies that this is a certified and authentic Matter device
  - Protects consumers against counterfeit or uncertified products



### Why are DACs a problem?

- Installing DACs complicates the device manufacturing process
- Securely creating, installing, and managing DACs is difficult
- Many device makers are struggling with DACs



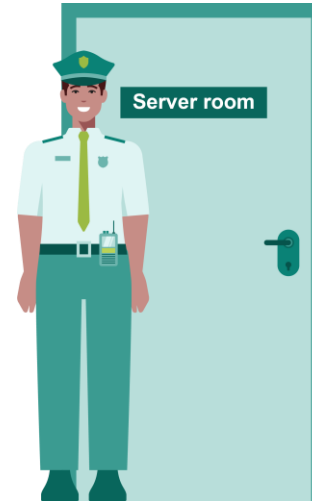
# Building Matter devices the old way



**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



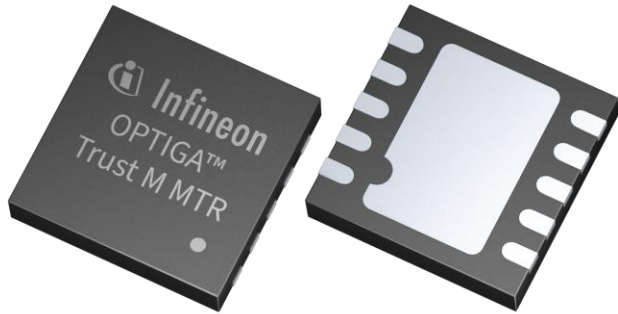
**4. Install DACs**  
Generate DACs and install into  
devices in factory

## Expensive, complex, risky, and disruptive

# 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	8
3	Challenges in enabling Matter-based smart home devices	11
4	<b>Introducing OPTIGA™ Trust M MTR</b>	<b>14</b>
5	Getting started	20
6	Key takeaways	22

# Introducing OPTIGA™ Trust M MTR



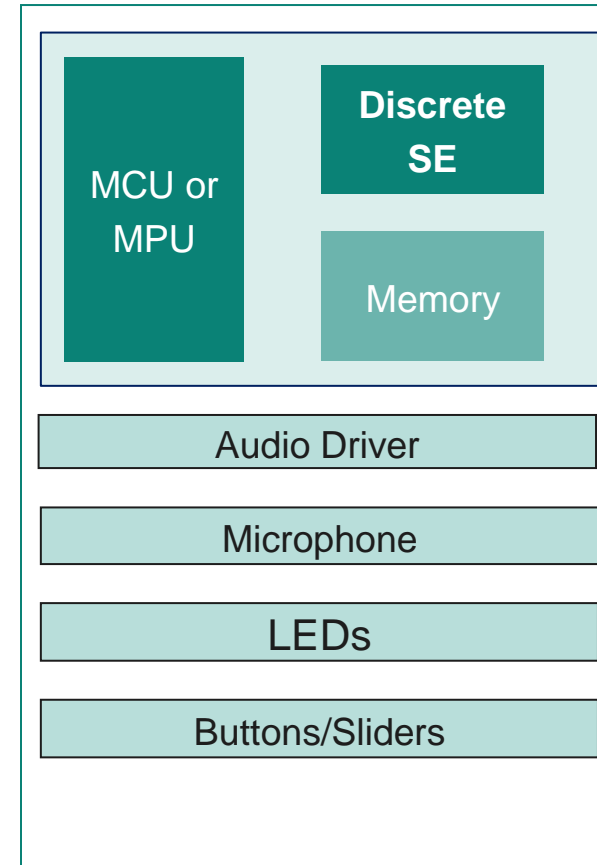
OPTIGA™ Trust M MTR is Infineon's  
OPTIGA™ Trust M discrete security solution  
with a Matter provisioning service

The easiest way to add  
secured Matter  
compatibility to your  
existing design



# 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



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



## Challenges

Provisioning of Matter certificates

Time to market

Flexibility

Security of smart home devices



## Solution

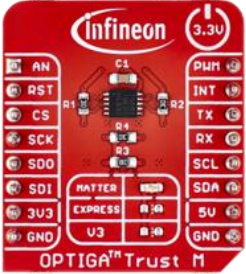
OPTIGA™ Trust M MTR is a pre-provisioned discrete SE which simplifies the process of adding Matter certificates to your devices.

OPTIGA™ Trust M MTR allows to keep your existing design as it can be inserted into any MCU/SoC design

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.

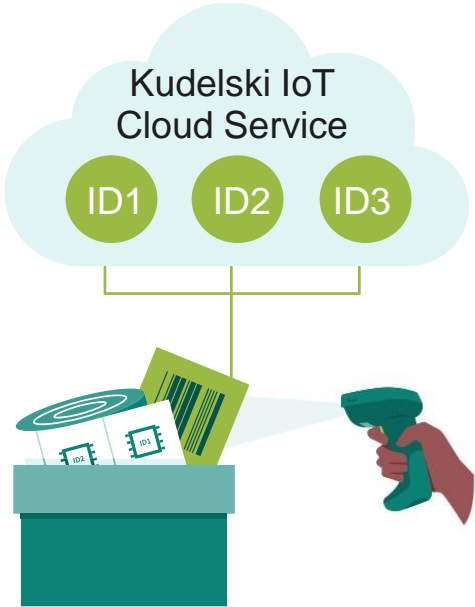
With its Common Criteria (CC) EAL6+ certified hardware, OPTIGA™ Trust M MTR can achieve consistent tamper-resistant protection supported by the Matter standard.

# Building Matter devices with OPTIGA™ Trust M MTR



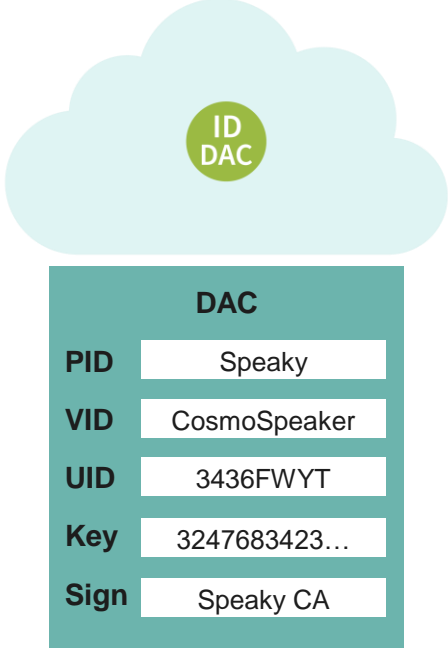
### 1. Pre-Production

Order Kits & Samples  
Create DAC for testing samples



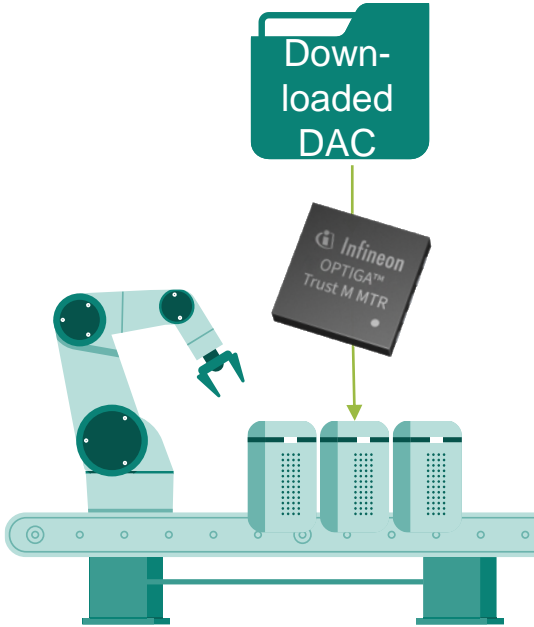
### 2. Order & Claim

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**



**Blindes/Shades**



**Climate Control**



**Television**



**Access Control**



**Surveillance camera, alarm**



**Gateway Access Point**



**Speaker**  
**... and many more**

# Table of contents

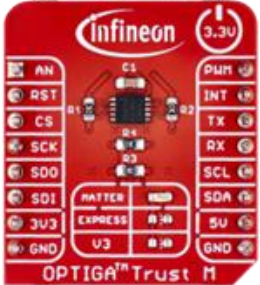
1	A matter of simplicity - introduction to the Matter smart home standard	3
2	A matter of security - how Matter gives you a peace of mind	8
3	Challenges in enabling Matter-based smart home devices	11
4	Introducing OPTIGA™ Trust M MTR	14
5	<b>Getting started</b>	<b>20</b>
6	Key takeaways	22

# Evaluation samples and platforms

## Sample Formfactor

### OPTIGA™ Trust M MTR Shield

- mikroBUS™ Add-on Board
- SP006008195



## Adapters

### OPTIGA™ Trust Adapter

- Arduino Uno ↔ mikroBUS™
- SP006007975



## Platform

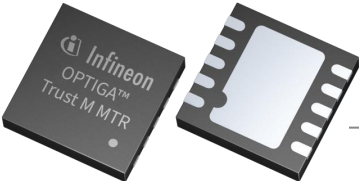
### PSoC62 Pioneer Kit

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



### OPTIGA™ Trust M MTR Engineering Samples

- 10 pcs in Tray
- SP006031931



### MIKROE Pi 4 Click Shield

- Raspberry Pi ↔ MikroBUS
- [Available externally](#)



### Raspberry Pi 4B

- Linux Computer
- [Available externally](#)



# 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	8
3	Challenges in enabling Matter-based smart home devices	11
4	Introducing OPTIGA™ Trust M MTR	14
5	Getting started	20
6	<b>Key takeaways</b>	<b>22</b>

# Key takeaways



OPTIGA™ Trust M MTR is easiest 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 certified to CC EAL 6+ offers a high level of protection



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

[www.infineon.com/OPTIGA-Trust-M-MTR](http://www.infineon.com/OPTIGA-Trust-M-MTR)



## ANY QUESTIONS?

<https://app.sli.do/event/sp9LX3NjppFtq1BtS9no5r>

### Or contact us:

**Ulrike Mittereder**

Media Relations Manager

Mobile: +49 151 547 205 29

Office: +49 89 234 43951

[Ulrike.Mittereder@infineon.com](mailto:Ulrike.Mittereder@infineon.com)

**Veronika Seifried**

Media Relations Manager

Office: +49 89 234 61662

Mobile: +49 151 10458904

[Veronika.Seifried@infineon.com](mailto:Veronika.Seifried@infineon.com)

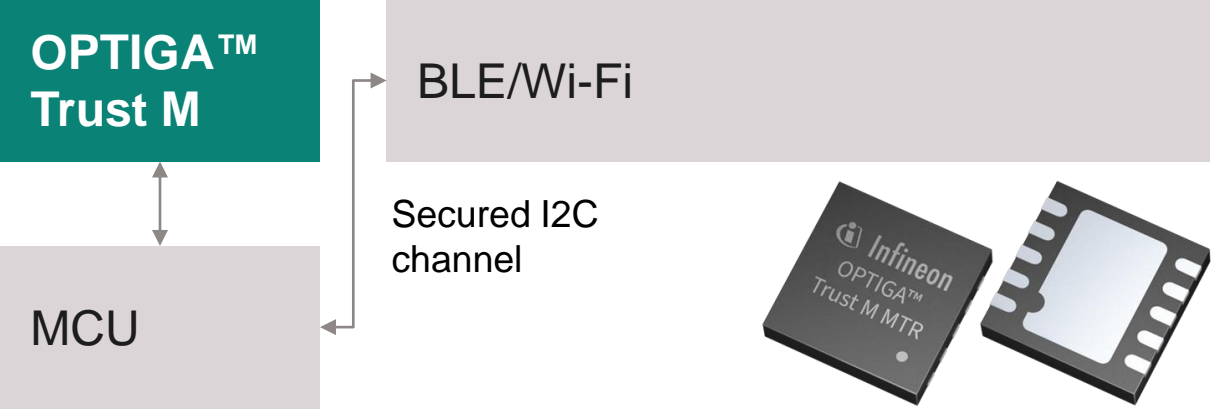
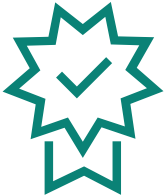




# OPTIGA™ Trust M MTR detailed product overview

## 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



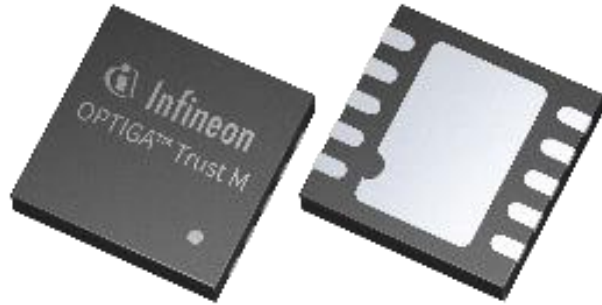
## Product details

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

# OPTIGA™ Trust M is available with different services

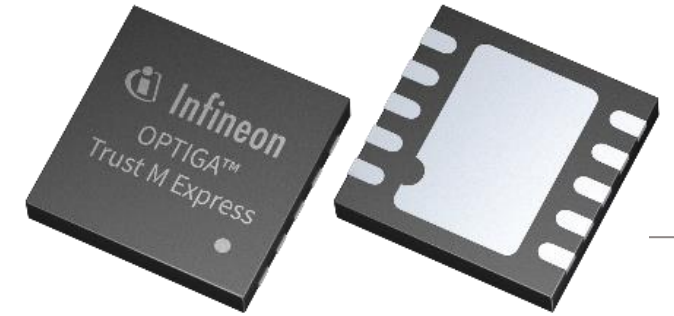
## OPTIGA™ Trust M

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

