WHITEPAPER

Creating Matter-enabled smart home devices simpler and more secure

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

Table of contents

Creating Matter-enabled smart home devices simpler and more secure

The concept of the “smart home” (Figure 1) is no longer in the realm of science fiction but is now a reality of our everyday lives. From smart lights and ovens to washing machines and smart locks, smart devices are connected to each other, and they are controlled using a smartphone or tablet via wireless technologies like Wi-Fi, Thread or Bluetooth. Smart home devices continue to proliferate, and they will soon be required to have the ability to communicate across various smart home ecosystems, many of which are currently incompatible. Matter is a new interoperability standard developed by the Connectivity Standards Alliance (CSA) to meet the challenge of enabling smart devices to connect reliably and securely with each other. It is based on the Internet Protocol (IP) and enables communication across different smart home ecosystems and wireless networking technologies. It has been developed by collaborative partners using an open-source methodology to simplify development for manufacturers and improve compatibility and ease-of-use for consumers.

However, as the number of devices connected to the cloud increases, so too does the risk of cyberattacks. This has the potential to make consumers reluctant to adopt more smart devices in their homes. This white paper discusses:

- The reasons why security is critical for smart home devices
- How Matter is now raising the bar for security, privacy and ease of use for the end users
- The steps for creating Matter-enabled smart devices and the shortcomings in legacy implementations
- How Infineon’s OPTIGA™ Trust M MTR Secure Element now offers OEMs an innovative way to make their existing smart device designs Matter-compliant
- How the OPTIGA™ Trust M MTR provides greater flexibility for developing multiple variants of new products
- How Infineon’s OPTIGA™ Trust M MTR protects smart devices against cyberattacks

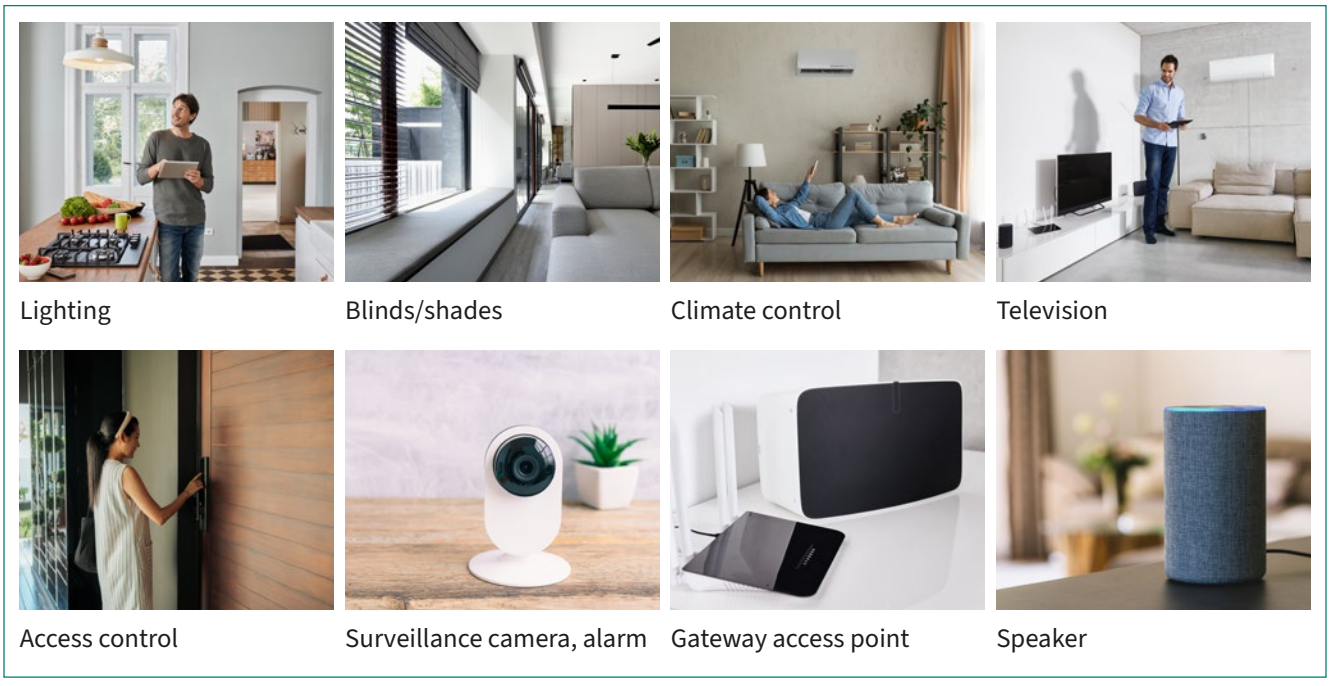

Figure 1 Smart home devices have a diverse range of applications

Matter and security go hand in hand

Security is an essential requirement for smart devices to prevent attackers from using them to gain access to private networks. For homeowners, cyberattacks on their smart home devices could potentially result in disrupted services, privacy violations or even impact their personal safety. For smart device manufacturers, attacks could result in serious financial loss due to reputational damage or as a result of liability. Consumers are aware of the potential for unauthorized access attacks through poorly protected smart home devices and these concerns are a significant impediment to their widespread adoption.

Thankfully, according to the CSA, Matter is raising the bar for IoT device security and privacy by providing:
- Easy, secured, and flexible device commissioning
- Validation that each device is authentic and certified
- Up-to-date information via distributed compliance ledger
- Strong device identity so that only authorized devices can join a smart home network
- Secured communications between devices and cloud
- Multiple administrators and controllers to maximize choice
- Verified access controls to prevent unauthorized actions
- Secured, standard software updates
- Verification of software integrity

Building Matter-enabled smart home devices

According to the Matter specification, every smart home device must have a Device Attestation Certificate (DAC), containing a Product ID (PID) and a Vendor ID (VID) which are used to enable the verification, authenticity and trustworthiness checks of each device commissioned in the Matter ecosystem. Matter DAC provisioning and security capabilities are essential for designing Matter-enabled smart home devices because DAC provisioning establishes trust among devices while security measures protect against a variety of threats. This is established through the Matter hierarchy shown in Figure 2 in which the:

- Product Attestation Authority (PAA) is a CSA-certified member, authorized to issue Matter PAIs
- Vendor Product Attestation Intermediate (PAI) includes the member`s CSA vendor ID (VID). The Product ID (PID) can be optionally included when generating a DAC
- Vendor Device Attestation Certificates (DAC) are provided by the PAI which is certified to sign DACs which include a PID and VID. Each product requires a specific DAC assigned by the PAI

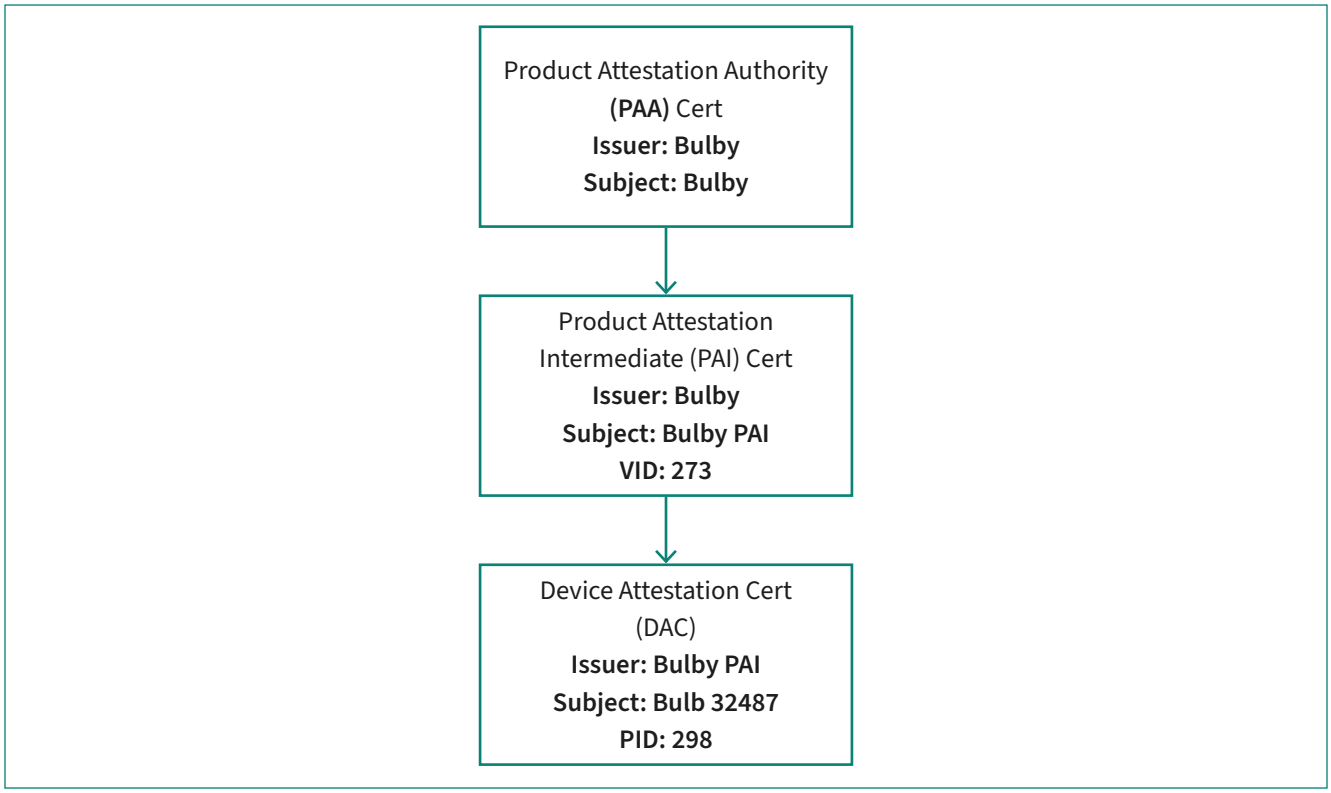

Figure 2 Matter hierarchy for allocating a DAC to a smart device

For OEMs, the legacy approach to building Matter-enabled devices, shown in Figure 3 can be expensive, complex, risky, and disruptive.

Figure 3 Legacy approach to building Matter enable devices

OPTIGA™ Trust M MTR makes building Matter devices simpler and more secure

OPTIGA™ Trust M MTR is Infineon's Matter-certified OPTIGA™ Trust M discrete Secure Element (dSE) which has been designed to support Matter provisioning. It is tamper-resistant and can be added to new and existing smart device designs to provide a superior security solution and to offload the processing overhead associated with security-related functions from the system microcontroller unit (MCU) or microprocessor (MPU) as shown in Figure 4.

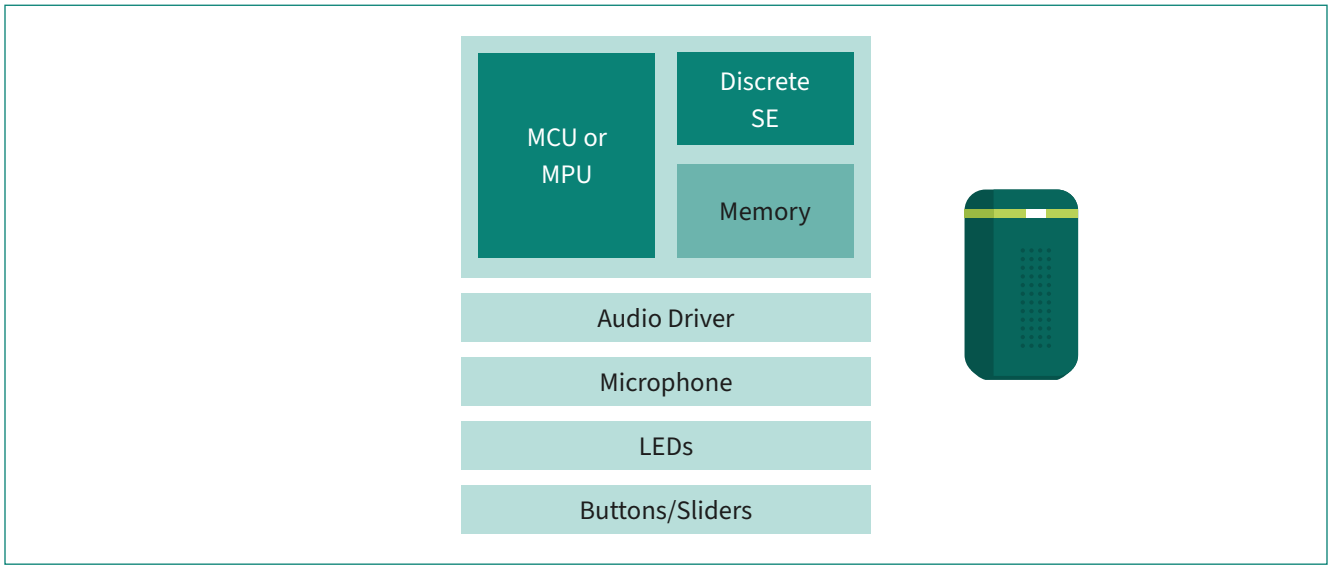

Figure 4 OPTIGA™ Trust M MTR accompanies MCU to perform security functions

OPTIGA™ Trust M MTR meets all the requirements and solves the challenges of designing Matter-enabled smart home devices and can be rapidly adopted in applications ranging from smart door locks, home appliances, various sensors and many other smart home devices.

Late-stage provisioning allows a personalized DAC can be injected right before the final manufacturing and shipment of the end product. This provides OEMs with the flexibility to create product variants right up until the final stage of the manufacturing process. OPTIGA™ Trust M MTR simplifies the entire flow of the customer journey using the quick and scalable 4-step process as shown in Figure 5.

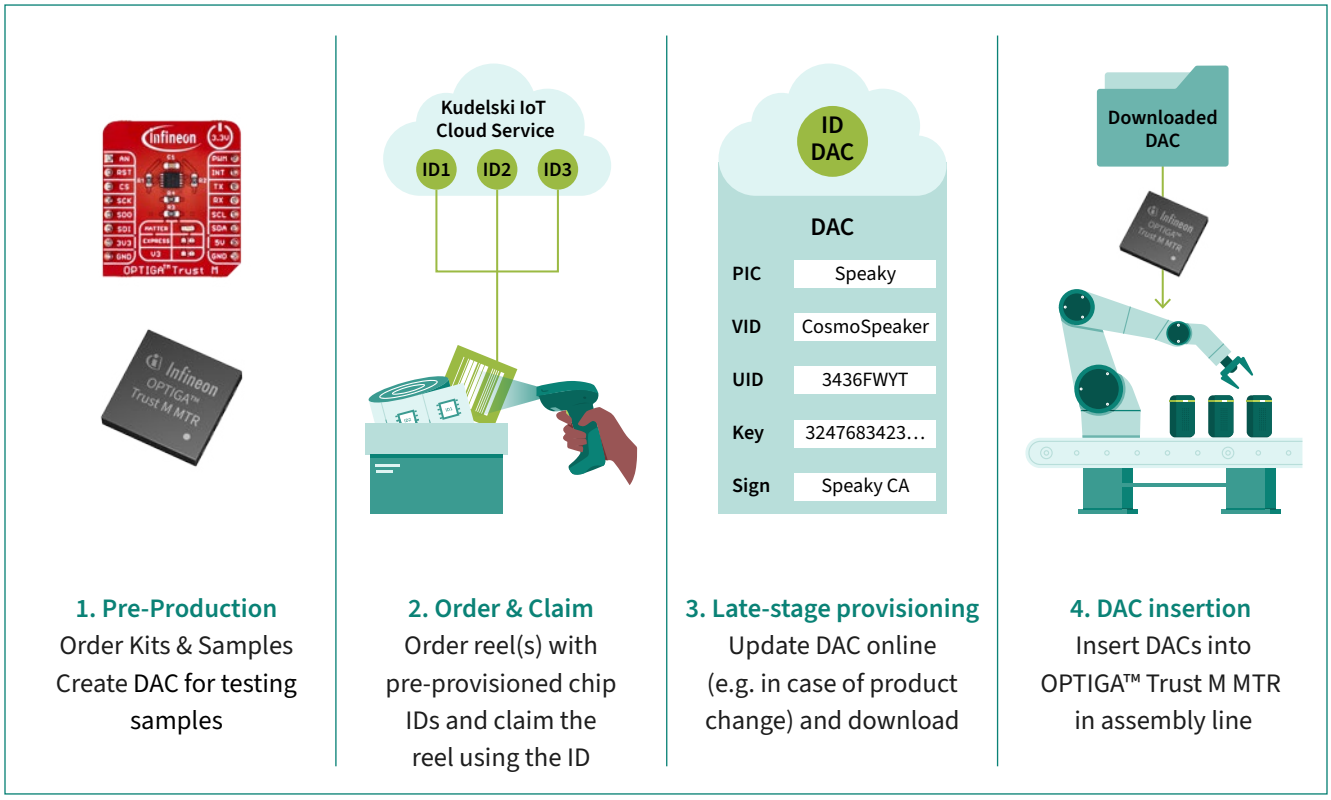

Figure 5 Four quick and scalable steps to building Matter-enabled IoT devices using OPTIGA™ Trust M MTR

- First, early in the product development cycle, an OEM creates a DAC which allows them to evaluate prototypes developed using OPTIGA™ Trust M MTR kits and samples available from Infineon
- Next, the OEM orders a reel of OPTIGA™ Trust M MTR chips which are pre-provisioned in an Infineon Common Criteria certified fabrication facility. Here private and public encryption keys can be injected into each device with the private key being protected by highly efficient security features. Once the OEM has finished the evaluation phase and starts building their Matter ecosystem, a personalized Matter certificate is defined
- Each reel of OPTIGA™ Trust M MTR is shipped with an associated barcode which represents the Reel ID. Infineon shares device and reel IDs with Kudelski IoT, a CSA approved and established PAA. The OEM scans the barcode to claim their devices through cloud services provided by Kudelski IoT, who then facilitates the download of test or production DACs corresponding to the vendor and the product
- Finally, a personalized DAC from the bundle file is transferred to the OPTIGA™ Trust M MTR device at the factory level

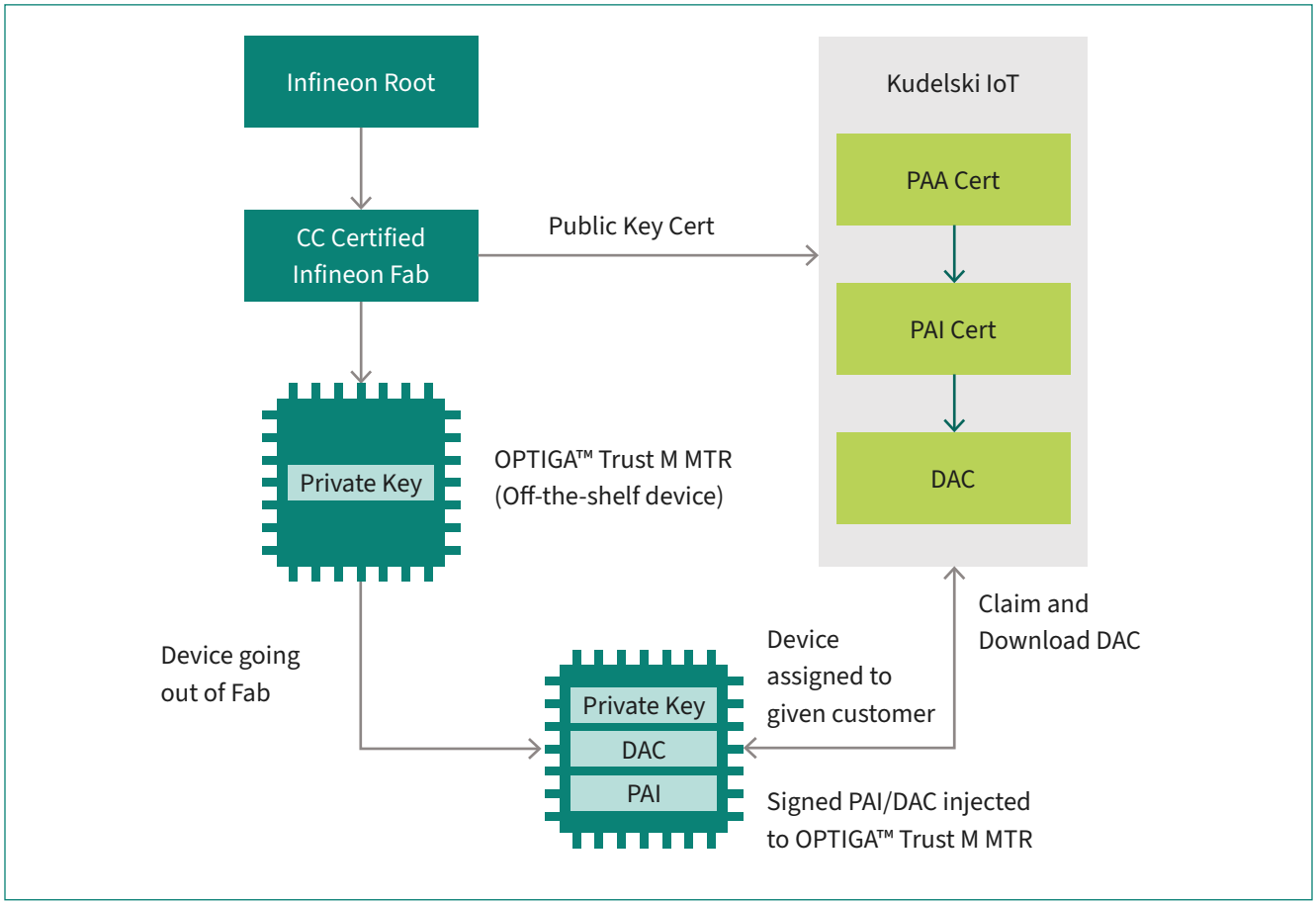

Figure 6 How Infineon and Kudelski IoT work in partnership to enable late-stage DAC provisioning

OPTIGA™ Trust M MTR device features

OPTIGA™ Trust M MTR is pre-provisioned with ECC and RSA certificates to enable fast provisioning using Matter-Certified public key infrastructure (PKI) services provided by Kudelski IoT. Specifically, Matter Device Attestation and the corresponding certificates use ECDSA based on the NIST P256 curve. The OPTIGA™ Trust M MTR supports this and other cryptography techniques like (up to) ECC-521, RSA-2k, AES-256, SHA256, which are based out of Common Criteria (CC) EAL6+(high) certified hardware. OPTIGA™ Trust M MTR features an I2C port for serial communication which is optionally encrypted (Shielded Connection). The OPTIGA™ Trust M MTR contains multiple slots to store various keys and certificates. It has four dedicated slots for X.509 certificates, three for Trust Anchors and seven slots to store keys for AES, RSA and ECC. A Matter device only requires a single DAC, leaving the remaining slots free to store multiple certificates and keys for more complex applications.

OPTIGA™ Trust M MTR sample applications

Smart display

A Matter enabled smart display can function as a hub (or center console) for controlling all other smart devices within a home, enabling interoperability between devices from multiple vendors using different ecosystems. Given its central role, security understandably becomes even more important, since a compromised hub could potentially allow an intruder to access every other device connected to it.

In the smart display application shown in Figure 7, OPTIGA™ Trust M MTR can be used to provide a Root-of-Trust which allows the device to boot up securely. It can additionally encrypt the communications channel to make it difficult for intruders to compromise data flowing between the display and the server to which it is connected. All communication between the display and the server is encrypted within the device before it is transmitted to the server. The server also encrypts its response, which is decrypted in turn using keys stored in the Secure Element (SE).

OPTIGA™ Trust M MTR connects to the MCU (or MPU) over a shielded I2C channel. Communication between the two begins at boot time and a secured connection to the cloud is then established by verifying the authenticity of both parties.

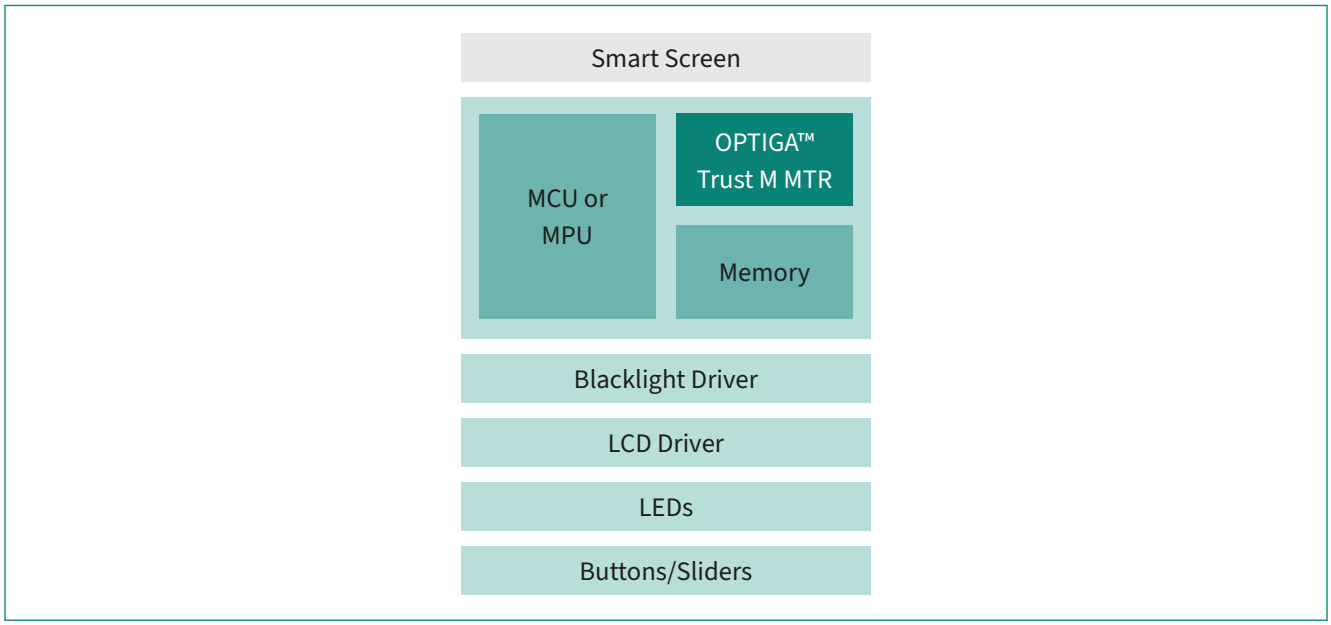

Figure 7 Smart screen application for the OPTIGA™ Trust M MTR

Smart Lock

A smart lock (Figure 8) is critical for securing a premises, meaning it places very stringent security demands on the devices used for connecting it to the cloud. Here, the OPTIGA™ Trust M MTR again provides a Root of Trust to allow a secured boot process and robustly encrypts the communication channel between the lock and remote server.

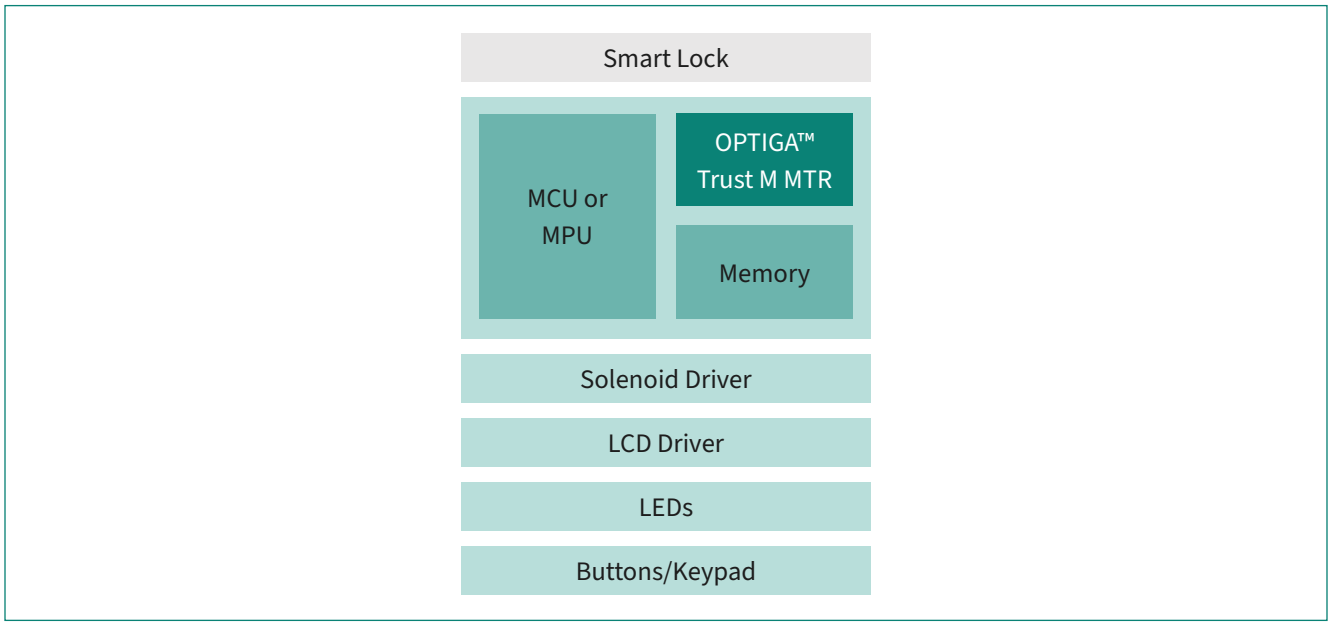

Figure 8 Smart lock application for the OPTIGA™ Trust M MTR

OPTIGA™ Trust M MTR Design Resources and Supporting Collaterals

To reduce time-to-market for smart device applications, Infineon provides a comprehensive range of hardware and software supports for OPTIGA™ Trust M MTR which are intended to allow users to accelerate their Matter device implementations. These include:

OPTIGA™ Trust M MTR Shield

OPTIGA™ Trust M MTR Shield (Figure 9) is an ideal way to evaluate the OPTIGA™ Trust M family of discrete Secure Elements (SE). It comes in a popular mikroBus layout which makes it easy to prototype with any MCU or MPU platform. The OPTIGA™ Trust M MTR Shield can be evaluated using the PSoC™ 62S2 Wi-Fi BT Pioneer Kit and the OPTIGA™ Trust Adapter.

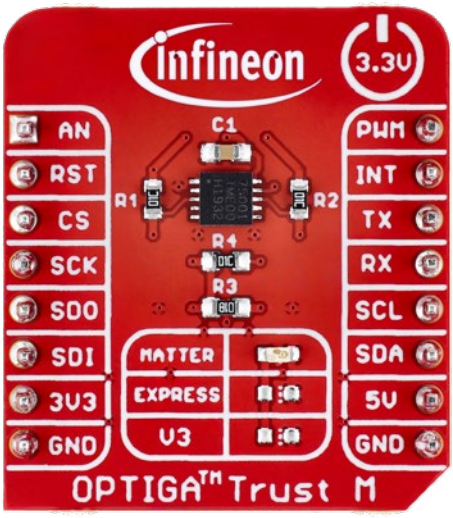

Figure 9 Infineon's OPTIGA™ Trust M MTR Shield

OPTIGA™ Trust Adapter

The OPTIGA™ Trust Adapter (Figure 10) for Arduino is a PCB adapter which can be used to connect OPTIGA™ Trust M shields, to microcontroller evaluation kits using Arduino-compatible connectors. Add-on boards can be connected to the adapter via the Shield2Go or mikroBUS connector.

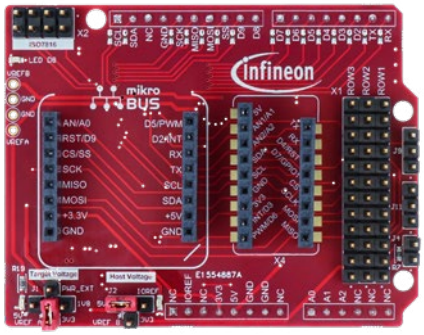

Figure 10 Infineon's OPTIGA™ Trust Adapter

PSoC™ 62S2 Wi-Fi BT Pioneer Kit

The PSoC™ 62S2 Wi-Fi BT Pioneer Kit (CY8CKIT-062S2-43012) is a feature rich hardware evaluation platform that enables the development of applications based on the PSoC™ 62 series MCU. The kit also includes a wireless module based on the AIROC™ CYW43012 combo device to develop cloud connected IoT applications including Matter over Wi-Fi applications.

Software support

Infineon provides a public software framework on Github which includes drivers, software, library/certificate(s) and key pairs.

Why use Infineon's OPTIGA™ Trust M MTR for Matter provisioning

OPTIGA™ Trust M MTR offers significant advantages these include:

- OPTIGA™ Trust M MTR is an "off-the-shelf product" which allows the PID to be changed right up until production is about to commence, thereby allowing multiple variants of a product to be developed
- OPTIGA™ Trust M MTR can work alongside any MCU/SoC, meaning existing product designs can still be used. The build-in crypto accelerator offloads cryptographic operations from the MCU to make the system more power-efficient
- As it is based on Common Criteria (CC) EAL6+(high) certified hardware, the OPTIGA™ Trust M MTR delivers consistent tamper-resistant protection
- OPTIGA™ Trust M MTR is the easy way to add Matter to any connected device.
- Product documentation can be provided to customers without the requirement for them to sign a non-disclosure agreement (NDA)

Conclusion

Matter is a new interoperability standard developed by the CSA to meet the challenges of connecting smart home devices securely and reliably. It is intended to be an industry-unifying standard to deliver reliable, seamless, and secured connectivity across various ecosystems. Security is an essential requirement for smart home devices because perceived threats by intruders has the potential to negatively impact adoption by consumers and this is one of the reasons why Matter is now raising the bar for IoT device security. The legacy approach used by OEMs to Matter provision their smart device designs was expensive, complex, risky, and disruptive, resulting in increased time to market and making it difficult to quickly modify existing designs to create product variants with different features. However, Infineon's OPTIGA™ Trust M MTR is a discrete security solution that combines a late-stage Matter provisioning service that works with any MCU or SoC, making it the easy way to add secured Matter compatibility to existing designs. Using this Matter-certified solution, DACs can be downloaded right up the time when an OEM is ready to commence production. This late-stage Matter provisioning approach offers the flexibility to quickly adapt existing designs to offer multiple product variants, even after a reel of secure elements has been ordered. OPTIGA™ Trust M MTR is based on Common Criteria (CC) EAL6+(high) certified hardware and offers tamper-resistant protection in line with Matter security principles.

Published by
Infineon Technologies AG
Am Campeon 1-15, 85579 Neubiberg
Germany

Public

Version: V1.0_EN
Date: 10/2024

Stay connected!

Scan QR code and explore offering
www.infineon.com

Please note!
This Document is for information purposes only and any information given herein shall in no event be regarded as a warranty, guarantee or description of any functionality, conditions and/or quality of our products or any suitability for a particular purpose. With regard to the technical specifications of our products, we kindly ask you to refer to the relevant product data sheets provided by us. Our customers and their technical departments are required to evaluate the suitability of our products for the intended application.

We reserve the right to change this document and/or the information given herein at any time.

Additional information
For further information on technologies, our products, the application of our products, delivery terms and conditions and/or prices, please contact your nearest Infineon Technologies office (www.infineon.com).

Warnings
Due to technical requirements, our products may contain dangerous substances. For information on the types in question, please contact your nearest Infineon Technologies office.

Except as otherwise explicitly approved by us in a written document signed by authorized representatives of Infineon Technologies, our products may not be used in any life-endangering applications, including but not limited to medical, nuclear, military, life-critical or any other applications where a failure of the product or any consequences of the use thereof can result in personal injury.