



Product brief

OPTIGA™ Trust M Express



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

OPTIGA™ Trust M Express offers rock-solid security for IoT devices every step of the way from manufacturing through cloud provisioning to field deployment.

The cryptographic identity of OPTIGA™ Trust M Express is provisioned in a certified and secured Infineon fab. It is protected from exposure at all stages during the product lifetime. This off-the-shelf solution removes the need for secured ID injection during IoT device manufacturing. This allows you to enhance the security of your IoT devices and their cloud connectivity while simplifying the production flow, accelerating time-to-market, and increasing cost efficiency.

OPTIGA™ Trust M Express is offered in combination with CIRRENT™ Cloud ID – an Infineon cloud service that automates IoT device certificate registration and the provisioning of the device in the product cloud at scale with zero manual intervention. This saves time and resources, protects against human error, and makes the process highly scalable.

OPTIGA™ Trust M Express reduces complexity and costs while increasing security:

Pre-provisioning: A unique device identity (x.509 certificate) is injected into OPTIGA™ Trust M Express in a security-certified Infineon facility to enable secured cloud authentication and secured communication with Azure, AWS, and other private clouds.

Ready to use: OPTIGA[™] Trust M Express is delivered off-the-shelf and requires no additional programming during the manufacturing process.

Zero-touch cloud onboarding: Support for automated onboarding of IoT devices to the cloud with CIRRENT™ Cloud ID.

Hardware-based security: Hardware is certified to CC EAL 6+ with state-of-the-art cryptography.

Robustness: Up to 20 years' lifetime for industrial and infrastructure applications.

Open source: MIT-licensed software framework on GitHub: github.com/Infineon/OPTIGA-Trust-M.

Main use cases: Secured cloud authentication, secured cloud communication, crypto offloads, secured software updates, etc.

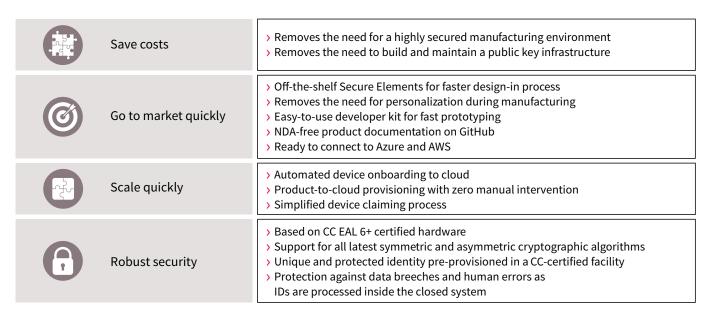
Key features

- > Pre-provisioned with ready-touse certificates and keys for AWS multi-account registration and Azure IoT Hub pre-registration
- > CIRRENT™ Cloud ID support for automated provisioning of IoT devices in the product cloud
- > CC EAL6+ (high) certified high-end security controller
 - ECC: NIST curves up to P-521,
 Brainpool r1 curve up to 512 bits
 - RSA with keys up to 2048 bits
- AES key up to 256 bits, HMAC up to SHA-512
- TLS v1.2 PRF and HKDF up to SHA-512
- True/Digital random number generators (TRNG/DRNG)
- Cryptographic toolbox commands for SHA-256, ECC and RSA® features, AES, HMAC and key derivation
- > Device certificate tracking
- > I²C interface with shielded connection
- > Hibernate mode for zero power consumption
- > Extended temperature range: -40... +105°C
- > PG-USON-10 package (3 x 3 mm)
- > Up to 10 kB user memory
 - Protected updates
 - Usage counters
 - Dynamic object (e.g. credentials) locking
- > Configurable device security monitor
- Lifetime of 20 years for industrial and infrastructure applications

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

OPTIGA™ Trust M Express

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



Product summary

Туре	Description	Temperature range [°C]	Package
SLS32AIA010ML	Ready-to-use security solution for IoT devices	-40+105	PG-USON-10
Evaluation kit	OPTIGA™ Trust M IoT Security Development Kit	-	Board

Applications



Smart city

> Street light



Smart mobility

> EV charging

> E-scooter



Smart building

Commercial smart HVAC



Smart home

> Residential aircon

Large home appliances



Industrial IoT

> Cyber security



Healthcare

 Connected dental equipment

Connected toothbrush



www.infineon.com

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

© 2022 Infineon Technologies AG All rights reserved.

Date: 07/2022

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.