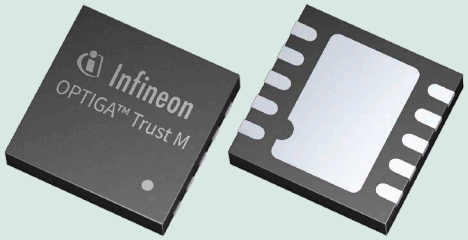

Open source

Product brief

OPTIGA™ Trust M

Secured cloud service provisioning – the easy way!

Cloud services and AI are driving a wave of innovative applications. The number of devices connected to these applications is growing, presenting great opportunities – but also increased security risks.

Responding to a growing focus on embedded systems amongst attackers, Infineon offers the OPTIGA™ Trust M solution, a high-end security controller optimized for connected devices. It provides extremely flexible, high-performance, secured access to any major cloud provider for industrial and building automation, smart home and consumer applications.

Secured zero-touch provisioning
The OPTIGA™ Trust M takes the secured connectivity to the cloud to the next level. It provides secured, fast, and easy access to any major cloud service provider thanks to pre-personalized certificates. The massive leap in performance creates the best possible user experience.

Easy integration
Integration made fast and easy – the turnkey set-up with full system integration minimizes your design, integration and deployment effort. A cryptographic toolbox and protected I2C interface are just two examples that will simplify your work.

Future-proof security
Certificates that exceed their lifetime need to be revoked. OPTIGA™ Trust M certificates can be securely updated in the field. OPTIGA™ Trust M gives every IoT device its own identity. Certificates and key pairs are securely stored in OPTIGA™ Trust M from the very beginning, with key pairs securely injected in Infineon's secured factory.

Performance
Do you need to improve the performance of your device? OPTIGA™ Trust M helps – connecting your device to the cloud up to ten times faster than a software-only solution.

MIT licensed software
Open source advantage – OPTIGA™ Trust M host software and documentation are available on GitHub. Benefit from direct support from developers as well as updates on new versions and features.

Offering ease of integration and a wide range of security features, OPTIGA™ Trust M is the solution of choice for all your embedded projects.

Key features [1)]

- CC EAL6+ (high) certified high-end security controller
  - ECC: NIST curves up to P-521, Brainpool r1 curve up to 512
  - RSA® up to 2048
  - AES key up to 256, HMAC up to SHA-512
  - TLS v1.2 PRF and HKDF up to SHA-512
  - TRNG/DRNG
- I2C interface with shielded connection
- Hibernate mode for zero power consumption
- USON-10 package (3 x 3 mm)
- Standard and extended temperature ranges: -40 to + 105°C
- 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
- Cryptographic ToolBox commands for SHA-256, ECC and RSA® Feature, AES, HMAC and Key derivation
- MIT licensed software framework on GitHub
  github.com/Infineon/optiga-trust-m

1) Features apply to latest product version

www.infineon.com/OPTIGA-Trust-M

OPTIGA™ Trust M

Secured cloud service provisioning – the easy way!

Easy integration	› Turnkey solution for fast and easy system integration › Zero-touch provisioning – unique credentials preprogrammed per chip › Open source code available on GitHub
Performance	› Up to 10 times faster connection to the cloud than software-only solutions
Enhanced security	› High-end security controller certified to CC EAL6+ (high) › Advanced asymmetric cryptography (ECC & RSA) in a single-chip solution › AES128-CCM encrypted communication between the host and the security controller
Flexibility	› Fast and easy access to any cloud provider thanks to pre-personalized certificates

Product summary

Type	Description	Temperature range [°C]	Package
SLS32AIA010MK	Embedded security solution for connected devices	-25 ... +85	USON-10
SLS32AIA010ML	Embedded security solution for connected devices	-40 ... +105	USON-10
Evaluation kit	XMC4800 IoT Connectivity Kit with OPTIGA™ Trust M	–	Board

OPTIGA™ Trust family of products

OPTIGA™ Trust M is part of Infineon's OPTIGA™ Trust family, a full range of embedded security solutions targeted at connected devices. Other OPTIGA™ Trust family members:

- OPTIGA™ Trust B, a product for device authentication and brand protection
- OPTIGA™ Trust E, an enhanced security solution for device authentication and brand protection
- OPTIGA™ Trust P, a Java Card-based programmable solution with extensive use case support
- OPTIGA™ Trust X, an enhanced security solution for connected devices

Infineon's OPTIGA™ family consists of products and solutions for securing embedded systems. All products are based on secured hardware and software. The overarching product family also includes the OPTIGA™ TPM (Trusted Platform Module) line targeted at embedded designs requiring Trusted Computing Group (TCG) compliance.

Having led the security market for almost 30 years and shipped more than 27 billion security controllers worldwide, Infineon continues to build on its strong expertise to turn security into a success factor for your business.

Published by
Infineon Technologies AG
81726 Munich, Germany

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.

Document number: B189-I0824-V2-7600-EU-EC-P
Date: 11 / 2020

Mouser Electronics

Authorized Distributor

Click to View Pricing, Inventory, Delivery & Lifecycle Information:

Infineon:

OPTIGATRUSTMEVALKITTOBO1 S2GOSECURITYOPTIGAMTOBO1