SLS32AIA010MLUSON10XTMA2

Data Sheet

Manufacturers	Infineon Technologies Corporation
Package/Case	PG-USON-10
Product Type	
RoHS	
Lifecycle	

Images are for reference only

General Description

The OPTIGA™ Trust M is a high-end security solution that provides an anchor of trust for connecting IoT devices to the cloud, giving every IoT device its own unique identity. This pre-personalized turnkey solution offers secured, zero-touch onboarding and the high performance needed for quick cloud access.

OPTIGA™ Trust M offers a wide range of security features, making it ideal for industrial and building automation applications, smart homes and connected consumer devices.

The turnkey set-up with full system integration minimizes design, integration and deployment effort.

OPTIGA™ Trust M is available in two temperature ranges:

SLS32AIA010MK standard temperature range of -25 to +85°C for most commercial implementations

SLS32AIA010ML extended temperature range of -40 to +105°C for harsh industrial environments

> Get host code and documentation (github.com/Infineon/optiga-trust-m)

Customers benefit from a direct communication line to developers and will immediately and directly be informed of new versions, features and bug fixes. Be it the integration of standard open-source crypto software libraries or the integration of the host code into other systems – easily possible now. The host code is licensed under the MIT License.

> Get host code and documentation (github.com/Infineon/optiga-trust-m)

Customers benefit from a direct communication line to developers and will immediately and directly be informed of new versions, features and bug fixes. Be it the integration of standard open-source crypto software libraries or the integration of the host code into other systems – easily possible now. The host code is licensed under the MIT License.

> Get host code and documentation (github.com/Infineon/optiga-trust-m)

Customers benefit from a direct communication line to developers and will immediately and directly be informed of new versions, features and bug fixes. Be it the integration of standard open-source crypto software libraries or the integration of the host code into other systems – easily possible now. The host code is licensed under the MIT License.

High-end CC EAL6+ (high) certified 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

OPTIGA™ Trust M's development process is certified according to the security standard IEC62443-4-1 for industrial automation and control systems, acting as an enabler to achieve component level certification according to IEC62443-4-2.

Features apply to latest product version.

Switch to Chinese language for details on a specific OPTIGA™ Trust M version to enable easy integration into Alibaba Cloud IoT.

Smart lightning

Smart Home

Building automation

Industrial robotics

PLC's and Drives

Drones

An IoT device needs to prove its identity to other networked devices and to verify the identity of all other networked devices. The mutual authentication feature of OPTIGA™ Trust M supports secured device authentication.

Many IoT devices collect and store valuable data, while also receiving commands over the IoT network. In order to protect critical data transferred over the network and thus the applications running on the device, OPTIGA™ Trust M offers a secured communication feature. It supports the TLS and DTLS protocols to protect against eavesdropping, tampering and message forgery.

In many cases, software running on a microcontroller contains valuable company IP that may be key to the company’s competitive edge. To protect this IP, OPTIGA™ Trust M supports one-way ECC-384-based authentication.
To activate this IP protection feature, customers can integrate multiple checks into their software, using the one-way OPTIGA™ Trust M authentication capabilities. The code will only ever run if this authentication process is successfully executed. This feature protects customer IP against simple image cloning.

Power efficiency is particularly important in battery-run devices. OPTIGA™ Trust M enables users to set a maximum power consumption limit in a range from 6 to 15 mA. The autonomous go-to-sleep feature also helps to conserve power; it can be set to a delay anywhere in the range between 20 ms and 255 ms.

During software updates, it can be challenging to protect both the software itself and the device that is being updated. Software updates that are protected with dedicated hardware security features achieve a higher level of security.
OPTIGA™ Trust M protects the processing and storage of code by means of encryption, fault and manipulation detection, as well as secured code and data storage.

Device integrity needs to be verified in order to detect unauthorized changes. Protecting the boot process is one of the most effective ways of doing this. Also known as secured, verified or trusted boot, boot access protection blocks unauthorized booting of computing devices to stop compromised devices from exchanging data over the IoT.
OPTIGA™ Trust M offers a set of features to enhance boot protection, also offloading complex, compute-intensive cryptography functions of the IoT device.

IoT environments can make it difficult for manufacturers to protect their ecosystem. For example, if a manufacturer produces both a main system and a smaller accessory or spare part, they may be keen to harden the main system against lower-quality counterfeit products.
OPTIGA™ Trust M offers a one-way authentication feature so that the main device or server can easily authenticate the new accessory or spare part.

Secured data storage and key provisioning

Lifecycle management

Features

High-end security controller with CC EAL6+ (high) certification

Turnkey solution ›ECC NIST P256/P384, SHA-256, TRNG, DRNG, RSA® 1024/2048

Cryptographic toolbox

I2C interface with shielded connection

Hibernate mode for zero power consumption

Up to 10 kB user memory

USON-10 (3 x 3 mm)

Temperature range up to -40°C to +105°C

Software framework on GitHub

Device security monitor

Lifetime of up to 20 years for industrial and infrastructure applications

Application

industrial and building automation

smart home

consumer devices

drones

Related Products

SAH-C164SL-8RM

Infineon Technologies Corporation

QFP-80

BSL303SPE

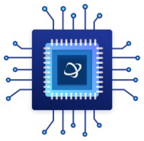
Infineon Technologies Corporation

TSOP-6

SLS32AIA010MKUSON10XTMA2

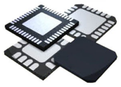
Infineon Technologies Corporation

PG-USON-10



SLS32AIA010MSUSON10

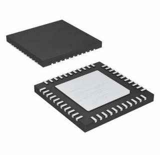
Infineon Technologies Corporation



SLB9670VQ20

Infineon Technologies Corporation

QFN



SLB9673XU20FW2610XTMA1

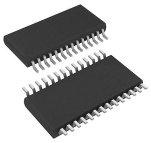
Infineon Technologies Corporation

PG-UQFN-32

SLB0587G

Infineon Technologies Corporation

SOP-8



SLB9660TT1.2

Infineon Technologies Corporation

TSSOP28