

Product brief

OPTIGA™ Trust X – SLS 32A1A

The optimized solution for IoT security

As embedded systems are increasingly gaining attention of attackers, Infineon offers the OPTIGA™ Trust X as a turnkey security solution for industrial automation systems, smart homes and consumer devices. This high-end security controller comes with full system integration support for easy and cost effective deployment of high-end security for your assets.

Broad range of benefits

Integrated in your device, the OPTIGA™ Trust X supports the protection of your brand and business case, differentiates your product from your competitors, and adds value to your product making it stronger against cyber-attacks.

Enhanced security

The OPTIGA™ Trust X comes with an advanced security controller built on Elliptic Curve Cryptography (ECC) with 256 bit, AES128 and SHA-256. This new security technology greatly enhances your overall system security. Furthermore the OPTIGA™ Trust X covers a broad range of use cases necessary to protect the authenticity, integrity and confidentiality in your device: mutual authentication, secured communication, data store protection, life-cycle management, secured updates, and also platform integrity protection.

Fast and easy integration

The turnkey set-up with full system integration and all key material preprogrammed reduces your efforts for design, integration and deployment to a minimum. As a turnkey solution, the OPTIGA™ Trust X comes with OS, embedded application and complete host side integration support. The extended temperature range of -40 to +105°C combined with a standardized I²C interface and small USON-10 footprint will enable all your embedded projects.

New: Open Source Host Code for OPTIGA™ Trust X

OPTIGA™ Trust X's host code and documentation is now available as open source on GitHub: <https://github.com/Infineon/optiga-trust-x>

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:

<https://github.com/Infineon/optiga-trust-x/blob/master/LICENSE>

Key features




- > High-end security controller
CC EAL6+ (high) certified
- > Turnkey solution
- > Mutual authentication using ECDSA
- > Secured communication using
TLS/DTLS
- > Compliant with the USB Type-C™
authentication standard
- > I²C interface
- > Up to 10 kB user memory
- > ECC NIST P256 and P384, AES-128,
SHA-256, TRNG, DRNG
- > USON-10 package (3 x 3 mm)
- > Standard & extended temperature
ranges (-40 to +105°C)
- > Full system integration support
- > Crypto ToolBox

Key values

- > Protection of IP and data
- > Protection of business case
- > Protection of company image
- > Safeguard quality and safety

Applications

- > Industrial control and automation
- > Consumer electronics
- > Smart home
- > Medical devices

 <p>Easy integration</p>	<ul style="list-style-type: none"> > Turnkey solution for fast and easy system integration (chip + OS + app + complete host side integration support) > Industry standard I²C interface > Small outline with USON-10 package (3 x 3 mm) > Eval-kit with reference implementation and source code > Industrial temperature range support: -40°C to +105°C
 <p>Cost-effective deployment</p>	<ul style="list-style-type: none"> > All keys and certificates already programmed in security certified production site at Infineon > Unique key pair preprogrammed per chip
 <p>Enhanced security for connected devices</p>	<ul style="list-style-type: none"> > High-end security controller > Advanced asymmetric cryptography (ECC256) in a single-chip solution > Comprehensive coverage of use cases: mutual authentication, secured communication, data store protection, life-cycle management, secured update, and also – from version X2 – platform integrity protection

Product summary

Type	Description	Temperature range [°C]	Package
OPTIGA™ Trust X - SLS 32AIA020X4	Embedded security solution for connected devices	-25 ... +85	USON-10
OPTIGA™ Trust X - SLS 32AIA020X2	Embedded security solution for connected devices	-40 ... +105	USON-10
Evaluation kit	Relax kit		Board

OPTIGA™ Trust family of products

The OPTIGA™ Trust X is part of Infineon’s OPTIGA™ Trust family, a full range of embedded security solutions addressing the market of connected devices. Available products besides the OPTIGA™ Trust X are

- > the OPTIGA™ Trust B SLE95250, a product for device authentication and brand protection
- > the OPTIGA™ Trust E SLS 32AIA, an enhanced security solution for device authentication and brand protection
- > the OPTIGA™ Trust P SLJ 52ACA, a Java Card based programmable solution with extensive use case support

Infineon’s OPTIGA™ family consists of products and solutions for securing embedded systems. All products are based on secured hardware and software. The overall product family also includes the OPTIGA™ TPM line of products (Trusted Platform Module) addressing the embedded market requiring TCG (Trusted Computing Group) compliant products.

Almost 30 years of leading position with nearly 20 billion security controllers shipped worldwide are the result of Infineon’s strong expertise and its commitment to make security a success factor for you.

Published by
Infineon Technologies AG
81726 Munich, Germany

© 2020 Infineon Technologies AG.
All Rights Reserved.

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.