Product Brief

OPTIGA™ Trust P SLJ 52ACA

Programmable authentication and device security for a wide range of functions

Rising connectivity between people, machines and devices is accentuating the need for IT security. Across a broad application spectrum, device manufacturers are challenged to enhance both security and flexibility.

Infineon's OPTIGA™ Trust P SLJ 52ACA is a high-security and feature-rich member of the OPTIGA™ Trust authentication product family. As a fully programmable chip, it provides a flexible solution for a full range of security functions. These include authentication, secured updates, key generation and storage, memory integrity checks, secured boot and access control management.

Programmable trust anchor
OPTIGA™ Trust P establishes a trust anchor in embedded systems. As a hardware security microcontroller, it provides advanced and efficient protection against side-channel, fault-induction and physical attacks. It also provides the physical separation of all security functions from the main processor and offers options for access controls and memory integrity checks to enable protection against software attacks.

Enhanced security
A wide range of cryptographic functions is available to applications running under the device's Java Card operating system. Reference applets and host code enable quick and easy implementation of most common security functions while the development tools provided support full customization to fit proprietary security systems. A secured implementation and management of the functionalities and applets is enabled based on the Global Platform specifications.

Protection of embedded systems
Along with other products in Infineon's OPTIGA™ Trust and OPTIGA™ TPM lines, OPTIGA™ Trust P enables protection of embedded systems against counterfeiting, unauthorized products, intentional attacks and unintentional operator errors. It supports the secure control and updating of systems, while maintaining information confidentiality and user privacy. OPTIGA™ Trust P is a superior solution to protect revenue streams, brand integrity and product safety.

www.infineon.com/optiga-trust

Key features

- High-end security controller with advanced cryptographic algorithms implemented in hardware (ECC521, RSA2048, TDES, AES)
- Common Criteria EAL 5+ (high) certification
- Programmable Java Card operating system with reference applets for a variety of use cases and host-side support
- 150 KB user memory
- Small footprint VQFN-32 SMD package (5 x 5 mm)
- ISO 7816 UART interface

Customer value

- Confidence in a secured and certified solution
- Increased flexibility based on programmable solution with reference applets to simplify customization and integration
- Protection of system integrity, communication and data

Applications

- Industrial control systems
- Energy generation & distribution systems
- Healthcare equipment & networks
- Consumer electronics
- Home security & automation
- Network applications

OPTIGA™ Trust P SLJ 52ACA

Programmable authentication and device security for a wide range of functions

OPTIGA™ Trust P offers a broad range of security functions:

Device authentication
- One-way authentication
- Mutual authentication

Secured channel
- Key generation
- DH/ECDH key exchange

Audit information
- Incident logs
- Protected storage

Secured updates
- Secured channel
- Access control

Trust anchor
- Secured boot
- Memory integrity

Information integrity
- Command integrity
- Message integrity
- Data integrity

Lifecycle management
- Supply chain tracking
- Lifecycle counter

OPTIGA™ Trust product family

OPTIGA™ Trust P SLJ 52ACA is part of Infineon's OPTIGA™ Trust family, which offers a full range of embedded security products to meet all device authentication needs. Other members of the OPTIGA™ Trust family are:
- OPTIGA™ Trust SLS 10ERE, a product for device authentication and brand protection
- OPTIGA™ Trust E SLS 32AIA, a high-end security solution to protect high-value goods and industrial applications

Infineon's OPTIGA™ family is geared towards the protection of embedded systems. All products are based on secured hardware and software. In addition to OPTIGA™ Trust products, the family also includes the OPTIGA™ TPM (Trusted Platform Module) lineup for embedded applications that require TCG (Trusted Computing Group) compliance.

Published by
Infineon Technologies AG
85579 Neubiberg, Germany

Order Number: B189-I0239-V1-7600-EU-EC-P
Date: 02 / 2016