OPTIGA™ Trust P SLJ 52ACA

Programmable Authentication and Device Security

Infineon Technologies' 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, such as authentication, secure updates, key generation and storage, protected storage, memory integrity, secure boot, and access control management.

The OPTIGA™ Trust P is a trust anchor for embedded systems. As a hardware security microcontroller, it provides advanced and efficient protection against side-channel, fault-induction, and physical attacks. It also provides a physical separation and the options for access controls and memory integrity checks to protect against software attacks. A wide range of cryptographic functions can be utilized through applications running on the device's JavaCard operating system. Reference applets and host code enable quick and easy implementation of most common security functions while the included development tools allow the flexibility for full customization into proprietary security systems.

Along with other products in Infineon's OPTIGA™ Trust and OPTIGA™ TPM lines, the SLJ 52ACA enables protection of embedded systems against counterfeiting, unauthorized products, intentional attacks, and unintentional operator errors. It allows for secure control and updating of systems as well as maintaining information confidentiality and user privacy. The OPTIGA™ Trust P is a superior solution to protect revenue retention, brand integrity, and product safety.

Application Use Cases
- Industrial Control Systems
- Energy Generation & Distribution Systems
- Healthcare Equipment and Networks
- Consumer Electronics
- Home Security & Automation
- Network Appliances

www.infineon.com/optiga-trust

Main Features

- 16-bit security controller with built-in MMU and encrypted bus
- 150k user memory
- Common criteria EAL5+
- Unique chip ID
- HW symmetric & asymmetric crypto engine
- True hardware random number generator
- Supported cryptography:
  - RSA up to 2048
  - ECC up to 521
  - AES up to 256
  - TDES up to 256
  - SHA1/224/256/384/512
  - DH/ECDH key agreement
- JavaCard 3.0.4 OS
- GlobalPlatform 2.2.1
- GlobalPlatform ID configuration 1.0
- Multiple SD, delegated management and mandated DAP
- PP JCS Open configuration ANSSI-CC-PP-2010/03
- Reference crypto applets and host source code
- VQFN-32 SMD package (5x5mm)
- ISO7816 UART interface (400kbps)

OPTIGA™ Trust P SLJ 52ACA

Programmable Authentication and Device Security

Embedded security systems' partner of choice

Infineon is an innovative and long-standing supplier of hardware-based security solutions. Leading the security IC and security system market for more than 15 consecutive years, embedded security suppliers can trust on a stable and innovative supplier.

Infineon is the leading manufacturer of TPM (Trusted Platform Module) for the past 10 years. This experience, know-how and market experience greatly support the fulfillment of requirements in the embedded security market and position Infineon as the global leader for security products and solutions.

With a global support network and multiple production sites, Infineon effectively serves projects around the world. Infineon is the preferred supplier for many embedded security solutions. Our continued investments in R&D propel innovation and maintain Infineon's leadership in the market.

Device Authentication
- One-way authentication
- Mutual authentication

Trust Anchor
- Secure boot
- Memory integrity

Secure Channel
- Key generation
- DH/ECDH key exchange

Information Integrity
- Command integrity
- Message integrity

Audit Information
- Incident logs
- Protected storage

Lifecycle Management
- Supply chain tracking
- Lifecycle counter

Secure Updates
- Secure channel
- Access control

Компания «ЭлектроПласт» предлагает заключение долгосрочных отношений при поставках импортных электронных компонентов на взаимовыгодных условиях!

Наши преимущества:
- Оперативные поставки широкого спектра электронных компонентов отечественного и импортного производства напрямую от производителей и с крупнейших мировых складов;
- Поставка более 17-ти миллионов наименований электронных компонентов;
- Поставка сложных, дефицитных, либо снятых с производства позиций;
- Оперативные сроки поставки под заказ (от 5 рабочих дней);
- Экспресс доставка в любую точку России;
- Техническая поддержка проекта, помощь в подборе аналогов, поставка прототипов;
- Система менеджмента качества сертифицирована по Международному стандарту ISO 9001;
- Лицензия ФСБ на осуществление работ с использованием сведений, составляющих государственную тайну;
- Поставка специализированных компонентов (Xilinx, Altera, Analog Devices, Intersil, Interpoint, Microsemi, Aeroflex, Peregrine, Syfer, Eurofarad, Texas Instrument, Miteq, Cobham, E2V, MA-COM, Hittite, Mini-Circuits,General Dynamics и др.);

Помимо этого, одним из направлений компании «ЭлектроПласт» является направление «Источники питания». Мы предлагаем Вам помощь Конструкторского отдела:
- Подбор оптимального решения, техническое обоснование при выборе компонента;
- Подбор аналогов;
- Консультации по применению компонента;
- Поставка образцов и прототипов;
- Техническая поддержка проекта;
- Защита от снятия компонента с производства.

Как с нами связаться

Телефон: 8 (812) 309 58 32 (многоканальный)
Факс: 8 (812) 320-02-42
Электронная почта: org@eplast1.ru
Адрес: 198099, г. Санкт-Петербург, ул. Калинина, дом 2, корпус 4, литера А.