Product Brief

CIPURSE™SAM – SLF 9630

CIPURSE™ Secure Access Module supporting migration

The CIPURSE™SAM is a ready-to-use Secure Access Module and offers secure storage of keys in hardware for 3-pass mutual authentication and communication. It offers a dedicated key management system with flexible key diversification and secured key loading for user card authentication, personalization and SAM administration.

The CIPURSE™SAM is based on the high-performance SLE 78 security controller with Integrity Guard digital hardware security which is used for e-ID documents of Governments and successfully achieved Common Criteria EAL 6+ security certification as an independent evidence of its outstanding security level.

It is compliant to the CIPURSE™ SAM Specification and to the CIPURSE™ Operation and Interface Specification. CIPURSE™ is an Open Standard of the OSPT™ Alliance and provides interoperability and easy integration of CIPURSE™ certified products.

The CIPURSE™SAM incorporates the CIPURSE™ security architecture and is compliant to the CIPURSE™ Cryptographic Protocol using AES-128, augmented by a combination of hardware and software security measures. Commands and transmitted data can be secured using the CIPURSE™ Cryptographic Protocol which is inherently resistant against physical attacks like DPA and DFA and was honored in 2012 with the German IT Security Award.

A typical CIPURSE™ secured transaction will take less than 100 ms.
Further, the CIPURSE™SAM can be used to communicate with 1 k and 4 k cards using Mifare compatible technology.

The CIPURSE™SAM is the ideal product to support the upgrade from existing nonsecure or systems using Mifare compatible technology towards a more advanced, state-of-the-art and future proven security architecture such as the Open Standard CIPURSE™.

Applications

- Public Transport Ticketing
- Automatic Fare Collection (AFC) system
- Account based Ticket, Event Ticket
- Access management, Hospitality
- Loyalty and identification
- Closed-loop Micropayment
- NFC

www.infineon.com/transport-ticketing

Benefits

- Ready-to-use for personalization
- Future proven cost effective solution for security application
- CIPURSE™ certified
- CC EAL 6+ (high) for HW

Main features

- CIPURSE™ SAM specification compliant
- Supporting CIPURSE™T with Consistent Transaction Mechanism (CTM), CIPURSE™S, CIPURSE™L Profiles
- Enables secured authentication between a reader and CIPURSE™ smart cards using AES-128 based authentication schemes or cards using Mifare compatible technology
- Dedicated key management system including key derivation and key upload
- Online and offline modes
- Up to 8 SAM applications (ADF) configurable
- Up to 512 reloadable 128-bit keys across all key files for SAM operations

Security features

- Secure storage of keys
- Secured 3 pass mutual authentication
- Secured communication using AES-128 and session key derivation mechanism
- Data exchange protocol inherently DPA and DFA resistant offering AES-MAC and AES-encryption and sequence integrity protection for APDUs

CIPURSE™SAM

SLF 9630

Hardware

› High-performance 16-bit SLE 78 security controller with “Integrity Guard” and CC EAL 6+ (High) certification according to Common Criteria 3.1 and protection profile PP0035
› Unique chip identification number for each chip
› Operation temperature range -25 °C to +85 °C
› Available as ID-1/ID-000 chip card with SIM module, VQFN-8

Integrated peripherals

› ISO/IEC 7816 contact-based interface

Security

› Fully encrypted data path
› Calculation with encrypted data path in the CPU itself
› Comprehensive digital error correction over the complete data path
› Self-checking dual CPU
› Mutual authentication scheme using AES-128 (3-pass as per ISO/IEC 9798-2)
› Data exchange protocol inherently DPA and DFA resistant, offering AES-MAC and AES-encryption, and also providing sequence integrity protection for APDUs
› Flexible access rights and secure messaging rules configurable for each file
› Up to eight 128-bit AES keys per CIPURSE™SAM application configurable

Generic crypto application

› Supports symmetric cryptography – AES-128, AES-192, AES-256 and DES, 3DES

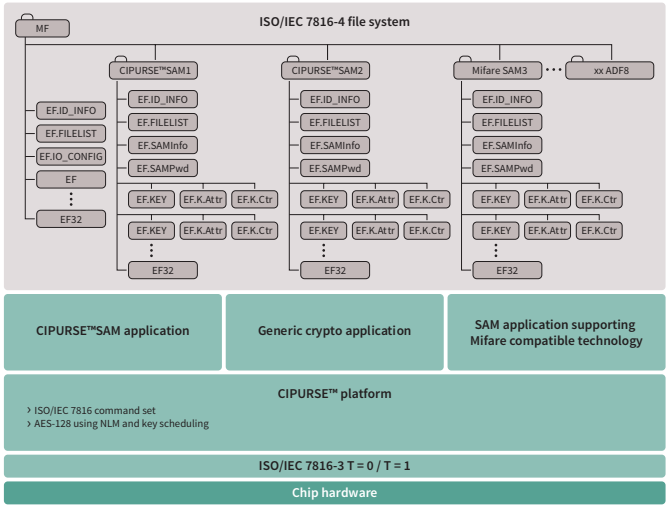
SAM application supporting CIPURSE™ and legacy systems

› Supports terminal for authentication of PICCs
› Support of key diversification
› Mifare compatible technology

Tools

› CIPURSE™ evaluation & development kit
  – CIPURSE™Explorer
  – Scripts for card personalization & operation
  – Scripts for CIPURSE™SAM personalization & key distribution
  – Scripts for NFC Type 4 Tag configuration
  – Terminal application note
  – CIPURSE™ sample cards

Memory & block diagram



Ordering information

Sales name	Description
SLF 9630	ID (ID-1/ID-000 Chip Card with SIM Module)
SLF 9630	VQFN8 (VQFN-8-4)

CIPURSE™ product portfolio

CIPURSE™move	SLM 10TLC002L
CIPURSE™4move	SLS 32TLC004S(M)
CIPURSE™Security Controller	SLS 32TLC100(M)
CIPURSE™SAM	SLF 9630

Published by
Infineon Technologies AG
85579 Neubiberg, Germany

Order Number: B180-I0111-V4-7600-EU-EC
Date: 08 / 2016