Product Brief

CIPURSE™Security Controller

CIPURSE™T Profile compliant security controller supporting migration

The CIPURSE™Security Controller is a ready-to-use cost optimized contactless security controller and offers secure storage of AES-128 keys in hardware for 3-pass mutual authentication and communication. It targets multi-applications and is available with 8 kByte user memory for application data storage of up to 8/16 custom applications.

CIPURSE™ is an Open Standard of the OSPT™ Alliance and provides interoperability and easy integration of CIPURSE™ certified products.

The CIPURSE™Security Controller incorporates the CIPURSE™ security architecture using AES-128. Commands and data can be secured using the CIPURSE™ Cryptographic Protocol which is inherently resistant against physical attacks like Differential Power Analyses (DPA) and Differential Fault Analysis (DFA) and was honored in 2012 with the German IT Security Award. A typical CIPURSE™ secured transaction will take less than 100 ms.

It offers optional support of 1 kByte or 4 kByte Mifare compatible emulation.

The CIPURSE™Security Controller 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 payment
- NFC

Benefits

- Ready-to-use for personalization
- Future proven cost effective solution for multi-application
- CIPURSE™ certified
- CC EAL 5+ (high) for HW and SW

Main features

- CIPURSE™T Profile compliant
- Consitent Transaction Mechanism
- 8 kByte user memory
- Up to 8/16 applications configurable
- Up to 4/8 PxSE applications configurable
- Optional support of 1 kByte or 4 kByte Mifare compatible emulation
- Limited refund feature
- NFC Forum Type 4 Tag support
- ISO/IEC 14443 Type A contactless interface
- 27 pF chip input capacitance
- Data rates up to 848 kbit/s
- Available as sawn, bumped wafer or contactless module MCC8

Security features

- Secure storage of AES-128 keys
- Secured 3 pass mutual authentication using AES-128
- 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

www.infineon.com/transport-ticketing

SESAMES AWARDS WINNER

cipurse™ CERTIFIED

CIPURSE™Security Controller

SLS 32TLC100(M)

Contactless I/O management

› ISO/IEC 14443-3 Type A Initialization and anticollision
› ISO/IEC 14443-4 transmission protocol
› 4/7/10-byte fixed UID, 4-byte random UID configurable

Memory organization

› ISO/IEC 7816-4 file system
› Binary, linear record, cyclic record, linear value-record files
› Up to 8/16 applications configurable
› Up to 4/8 PxSE applications configurable
› Up to 32 elementary files per CIPURSE™ application configurable

Interface

› Optional support of 1 kByte or 4 kByte Mifare compatible emulation

NFC Forum Type 4 Tag

› Technical specification version 2.0

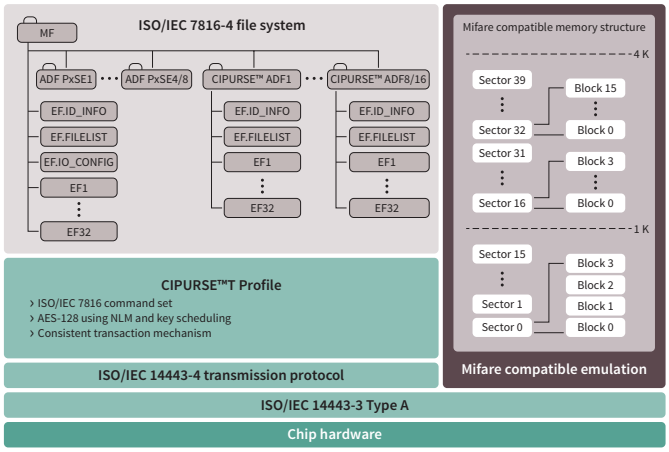
Security

› Security attack preventions for all critical operations using both hardware and software countermeasures
› Mutual authentication (3-pass as per ISO/IEC 9798-2), using AES-128
› Data exchange protocol inherently DPA and DFA resistant offering AES-MAC and AES-encryption and 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™ application configurable

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
SLS 32TLC100(M)	NB (sawn wafer 75/150 µm, NiAu bump 20 µm)
SLS 32TLC100(M)	MCC8 (contactless module)

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-I0099-V3-7600-EU-EC-P
Date: 08 / 2016