



## Product Brief

# SLS 32TLC100(M)

## CIPURSE™ Security Controller

The SLS 32TLC100(M) is a dedicated security controller for transport ticketing applications featuring CIPURSE™ functionality and Mifare compatibility. It is therefore the ideal product to upgrade existing Mifare compatible systems towards more advanced CIPURSE™ security based on AES-128. The product is the very first of a range of CIPURSE™ compliant contactless products optimized for a variety of form factors such as limited use tickets, multiapplication and payment cards.

The SLS 32TLC100(M) is based on Infineon's SLE 7x SOLID FLASH™ family successfully used in many applications. It offers support for the CIPURSE™T profile of CIPURSE™V2 and can hold several ticket applications.

With communication rates up to 848 kbits/sec, fast CIPURSE™ transactions are possible, offering the travelling public a convenient, flexible device that can be used by transport operators for various purposes from concessionary passes to commercial tickets for extended period travel. CIPURSE™ eases also the deployment of NFC solutions by operating on standard infrastructures.

Additionally, the Mifare compatible emulation supports existing applications while the CIPURSE™ functionality allows migration towards state of the art security based on AES-128. Having Mifare compatibility and CIPURSE™ functionality in one device further allows transport and local authorities to stay with existing legacy systems where needed while still being able to migrate demanding applications towards CIPURSE™ security.

### Applications

- Transport Products: concessionary travel, multiple stored travel rights
- Employees: staff cards, building access, vending and photocopying
- General Public Services e.g. for Libraries, Leisure, e-money, cashless catering, etc

Mifare is only used as an indicator of product compatibility to the respective technology.

### Benefits

- Migration product for existing systems towards CIPURSE™
- “Ready-To-Go” solution: Integrated application
- Ready for personalization
- Multi-application card support

### Main Features

- ISO/IEC 14443 compliant interface
- Mifare compatibility
- CIPURSE™T compliant
- NFC Forum™ Type 4 Tag A configurable

### CIPURSE™ Defines

- A feature set, that allows to set up and operate dedicated applications
- A mutual authentication scheme using AES-128
- A secure messaging protocol
- Mandatory file types (binary, record, cyclic record, value)
- Mandatory command set
- Keys and associated structure of file access conditions

### Tools

- CIPURSE™ Evaluation & Development Kit
  - CIPURSE™Explorer with sample scripts for card personalization and operation
  - Sample cards
- CIPURSE™ Terminal Secure Messaging Application Note & source code

### Certification

- CC EAL5+ (high)
- CIPURSE™ certification

# SLS 32TLC100(M)

## CIPURSE™ Security Controller

### Hardware

- Chip hardware based on SOLID FLASH™ 16-bit security controller
- Operation temperature range -25°C to +85°C
- Crypto accelerator supporting AES-128 algorithm
- Available as contactless module MCC8 or wafer
- Other delivery forms on request

### Contactless I/O Management

- ISO/IEC 14443-3 Type A
- ISO/IEC 14443-4 protocol
- Data rate up to 848 kbit/s
- 4-byte reused / non-unique / Random ID, 7-/10-byte UID

### Memory Organization

- User Memory: 8 kByte EEPROM
- File system according to ISO/IEC 7816-4
- Up to 8 applications configurable
- Up to 32 files per application configurable
- Binary files, linear record files, cyclic record files and linear value-record files
- Consistent transaction mechanism for each file type

### Optional Support of Mifare Compatibility

- 1 KB Mifare compatibility: 16 sectors of 64 bytes (4 blocks)
- 4 KB Mifare compatibility: 32 sectors of 64 bytes (4 blocks) and 8 sectors of 256 bytes (16 blocks)
- Two keys per sector
- Mutual three pass authentication
- Encrypted data transfer
- Improved random number (i.e. TokenRB) for cryptography providing more robustness against known attacks

### Security

- Eight 128-bit AES keys per application configurable
- Flexible access rights and secure messaging rules configurable for each file
- Mutual authentication (3-pass as per ISO/IEC 9798-2), using AES
- Secure messaging supporting AES-MAC and AES-encryption
- Data exchange protocol inherently DPA and DFA resistant
- Sequence integrity protection for APDUs
- Security attack countermeasures for all critical operations using both hardware and software controls
- Active shield technology
- Anti-snooping features

### Certification Level

- CIPURSE™V2 certification
- CC EAL5+ (high)



Infineon's SLS 32 CIPURSE™ Security Controller wins the prestigious Sesames Award 2012 in the category "Transportation"

Published by  
Infineon Technologies AG  
85579 Neubiberg, Germany

© 2015 Infineon Technologies AG.  
All Rights Reserved.

Visit us:  
[www.infineon.com](http://www.infineon.com)

Order Number: B180-I0099-V1-7600-EU-EC  
Date: 02 / 2015

### Attention please!

The information given in this document shall in no event be regarded as a guarantee of conditions or characteristics ("Beschaffheitsgarantie"). With respect to any examples or hints given herein, any typical values stated herein and/or any information regarding the application of the device, Infineon Technologies hereby disclaims any and all warranties and liabilities of any kind, including without limitation warranties of non-infringement of intellectual property rights of any third party.

### Information

For further information on technology, delivery terms and conditions and prices please contact your nearest Infineon Technologies Office ([www.infineon.com](http://www.infineon.com)).

### Warnings

Due to technical requirements components may contain dangerous substances. For information on the types in question please contact your nearest Infineon Technologies Office. Infineon Technologies Components may only be used in life-support devices or systems with the express written approval of Infineon Technologies, if a failure of such components can reasonably be expected to cause the failure of that life-support device or system, or to affect the safety or effectiveness of that device or system. Life support devices or systems are intended to be implanted in the human body, or to support and/or maintain and sustain and/or protect human life. If they fail, it is reasonable to assume that the health of the user or other persons may be endangered.