Product Brief

CIPURSE™move – SLM 10TLC002L

CIPURSE™L Profile compliant security product

The CIPURSE™move is a ready-to-use cost optimized contactless security product and offers secure storage of AES-128 keys in hardware for 3-pass mutual authentication and communication. It targets single application and provides 304 Byte of user memory for application data storage.

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

The CIPURSE™move 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.

The CIPURSE™move is the ideal product to support migration 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
› Limited Use Ticket (LUT), Limited Use Card (LUC)
› Account based Ticket, Single Ride 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 single application
› CIPURSE™ certified

Main features
› CIPURSE™L Profile compliant
› 304 Byte (2.4 kbit) user memory
› One application configurable
› One PxSE application configurable
› Limited Refund feature
› NFC Forum Type 4 Tag support
› ISO/IEC 14443 Type A contactless interface
› 17 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 sequence integrity protection for APDUs

www.infineon.com/transport-ticketing

CIPURSE™move

SLM 10TLC002L

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

Memory organization
› ISO/IEC 7816-4 file system
› Binary, linear record and value-record files
› One CIPURSE™ and one PxSE application configurable
› Up to 3 elementary files within the CIPURSE™ application configurable

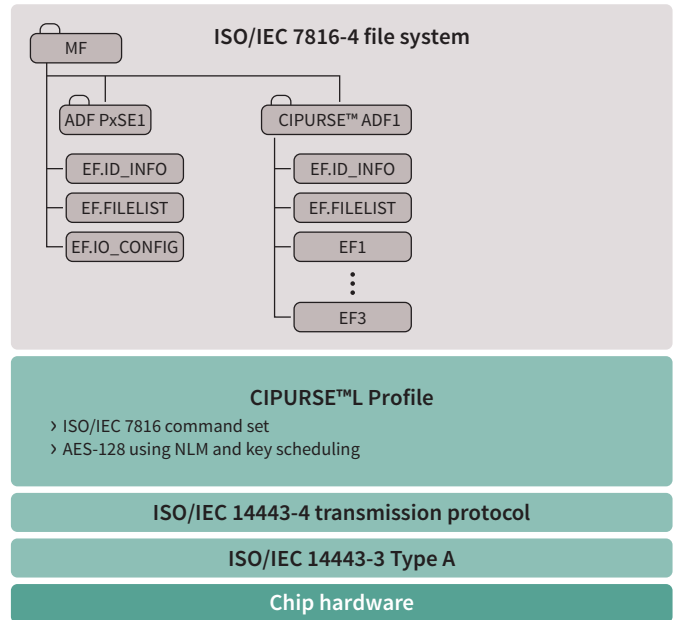### NFC Forum Type 4 Tag
› Technical specification version 2.0

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 sequence integrity protection for APDUs
› Flexible access rights and secure messaging rules configurable for each file
› Two 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

```
        ISO/IEC 7816-4 file system
   MF

   ADF PxSE1              CIPURSE™ ADF1
   EF.ID_INFO             EF.ID_INFO
   EF.FILELIST            EF.FILELIST
   EF.IO_CONFIG           EF1
                          ⋮
                          EF3
```

CIPURSE™L Profile
› ISO/IEC 7816 command set
› AES-128 using NLM and key scheduling

ISO/IEC 14443-4 transmission protocol

ISO/IEC 14443-3 Type A

Chip hardware

Ordering information

Sales name	Description
SLM 10TLC002L	NB (sawn wafer 75 µm, NiAu bump 20 µm)
SLM 10TLC002L	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

Please note!
THIS DOCUMENT IS FOR INFORMATION PURPOSES ONLY AND ANY INFORMATION GIVEN HEREIN SHALL IN NO EVENT BE REGARDED AS A WARRANTY, GUARANTEE OR DESCRIPTION OF ANY FUNCTIONALITY, CONDITIONS AND/OR QUALITY OF OUR PRODUCTS OR ANY SUITABILITY FOR A PARTICULAR PURPOSE. WITH REGARD TO THE TECHNICAL SPECIFICATIONS OF OUR PRODUCTS, WE KINDLY ASK YOU TO REFER TO THE RELEVANT PRODUCT DATA SHEETS PROVIDED BY US. OUR CUSTOMERS AND THEIR TECHNICAL DEPARTMENTS ARE REQUIRED TO EVALUATE THE SUITABILITY OF OUR PRODUCTS FOR THE INTENDED APPLICATION.

WE RESERVE THE RIGHT TO CHANGE THIS DOCUMENT AND/OR THE INFORMATION GIVEN HEREIN AT ANY TIME.

Additional information
For further information on technologies, our products, the application of our products, delivery terms and conditions and/or prices, please contact your nearest Infineon Technologies office (www.infineon.com).

Warnings
Due to technical requirements, our products may contain dangerous substances. For information on the types in question, please contact your nearest Infineon Technologies office.

Except as otherwise explicitly approved by us in a written document signed by authorized representatives of Infineon Technologies, our products may not be used in any life-endangering applications, including but not limited to medical, nuclear, military, life-critical or any other applications where a failure of the product or any consequences of the use thereof can result in personal injury.