CIPURSE™move

Datasheet

CIPURSE™-based contactless memory product for cost-optimized tickets, cards, and wearables in transport ticketing, physical access, and micro-payment applications

Key features

- **Open Standard, CIPURSE™L Profile** compliant
  - **1 CIPURSE™ application** configurable
  - Up to **2 128-bit AES keys** may be assigned to the CIPURSE™ ADF
  - **1 PxSE ADF** configurable
  - **Secured communication** using AES-128 and session key derivation
  - **Mutual authentication** using AES-128
- **304 bytes user memory** for application data storage
- **Limited refund** offering a decrease/increase of the Value Record file limited to the value of the preceding increase/decrease operation
- **ISO/IEC 14443 Type A contactless interface**
- **Chip capacitance of 17 pF**
- **CIPURSE™ certified**

Potential applications

Optimized for **contactless transport ticketing applications**

About this document

Scope and purpose

This document describes the features, functionality, and operational characteristics of SLM 10TLC002L.

Intended audience

This document is primarily intended for system and application designers.

Note: For more details, CIPURSE™move Data Book available under NDA can be requested from Infineon Technologies.

Table of contents

Table of contents

List of tables

List of figures

1 Introduction

The CIPURSE™move is a dedicated contactless CIPURSE™ compatible product developed for a provision of cost-optimized limited use tickets, cards, and wearables in transport ticketing, physical access, and micro-payment applications.

Compliance with the CIPURSE™ specifications fosters interoperability and easy integration with other members of the CIPURSE™ family, reduces the complexity of terminals, and maintains the security level of a transport system.

1.1 System overview

The CIPURSE™move is designed to operate in a CIPURSE™ compatible system. The product is connected to a terminal via contactless interface providing both energy for operation and data exchange. The terminal is application specific and may be either connected to a host system (online terminal) or work standalone (offline terminal).

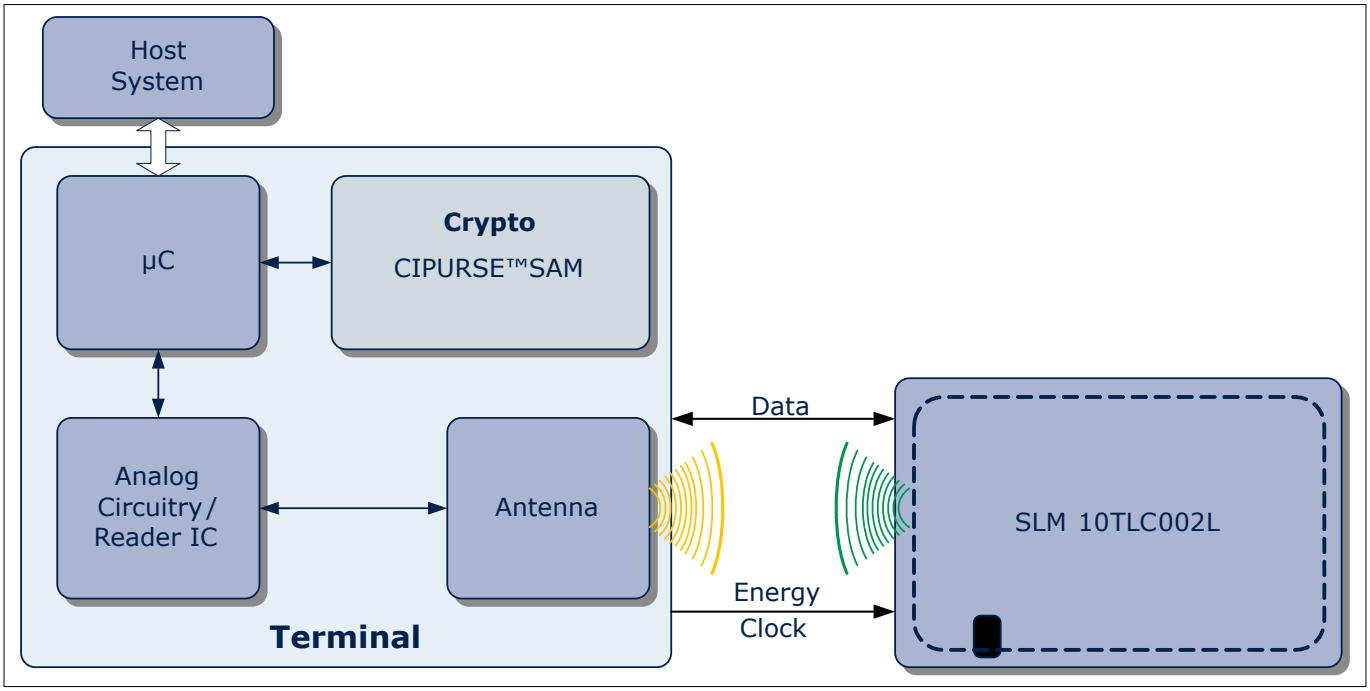

Figure 1 System overview

1.2 Product overview

The CIPURSE™move is a cost-efficient implementation and designed for use in automatic fare collection systems, micro-payment, as access control token, and other smart card security applications.

CIPURSE™move supports anti-collision and selection as per ISO/IEC 14443-3 [7] Type A and transmission protocol (T=CL) as per ISO/IEC 14443-4 [8].

The CIPURSE™move focuses on applications with user memory sizes of up to 2 kbits and offers simplified functionality as well as an optimized file system. It is designed for applications that demand low-cost products such as:

- Electronic limited-use tickets for public transport
- Electronic limited-use ticket for event ticketing

The implemented security mechanisms – such as a strong authentication mechanism based on the Advanced Encryption Standard (AES) 128-bit algorithm and data integrity via session message authentication code (MAC) – counteract different attack scenarios such as unauthorized access or unauthorized manipulation of card data.

1 Introduction

The product allows handling a typical ticketing transaction in less than 100 ms. It is, for example, suited for use in a transportation fare collection scheme or in a ticketing system such as a stadium ticketing. Further, the product offers robust contactless transmission which means that the card with CIPURSE™move may also remain in the wallet of the user even if there are coins in it.

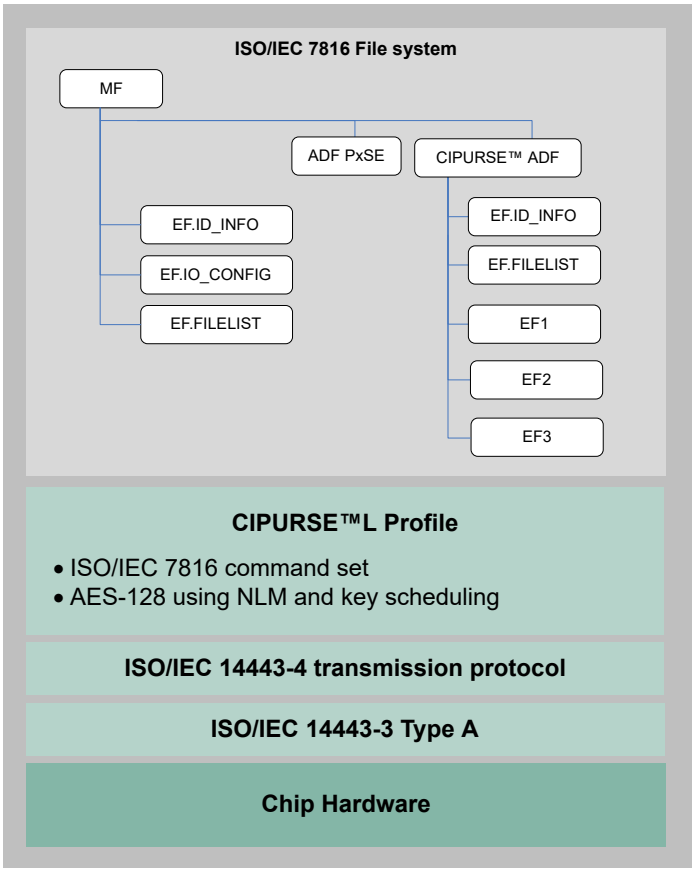

Figure 2 Block diagram in application

General features

- 2432 bits (304 byte) of user memory[1)]
- 17 pF chip input capacitance
- Operating temperature range: -25°C to +70°C (for chip)[2)]
- Storage temperature range: -40°C to +125°C (for chip)

CIPURSE™move application security

The CIPURSE™move supports:

- Up to 2 128-bit AES keys can be assigned to the CIPURSE™ ADF
- Flexible access rights and secure messaging rules configurable for each file
- Mutual authentication using AES 128-bit

1 User memory refers to the file body portion only, that is, only the data area of a file is considered in these numbers. File header, ACG, SMG, Keys, AID, security information field, and so on. are not contributing to User memory and shall be provided from the memory portion outside the user memory

2 For modules according to module specification

- Secure messaging with AES-MAC
- Secure messaging mode configurable for each data exchange
- Data exchange protocol inherently differential power analysis (DPA) and differential fault analysis (DFA) resistant, offering AES-MAC and sequence integrity protection for application protocol data units (APDUs)
- Atomic operations for manipulating value records
- Administrative functionality
  - One 128-bit AES key available for master file (MF) administration
  - MF security architecture is the same as application dedicated file (ADF) security architecture

Note: This product does not support the encryption (ENC) of communication channel, see Chapter 3.2.4.

ISO/IEC 7816-4 file system

The CIPURSE™move implements a CIPURSE™ compliant file system based on ISO/IEC 7816-4 [3]:

- Files are organized logically in the form of two-level dedicated file (DF) tree structure. The MF forms the root of this structure
  - The MF hosts two pre-defined elementary files (EFs) and one application dedicated file
  - One proximity system environment (PxSE) ADF (as specified in Chapter 3.1.2.2) is supported in addition to the CIPURSE™ ADF under the MF
  - A CIPURSE™ application is represented by an ADF identified by its file identifier (FID) and dedicated file (DF) name application identifier (AID). The CIPURSE™ ADF may host up to 3 EFs for application-specific data
- Elementary file types supported are binary files, linear record files and linear value-record files
  - File size up to 304 byte
  - Up to 76 records a 4 byte per record oriented file
  - Record lengths can be 4, 8, or 16 bytes
- Security attributes defining the access rights and secure messaging rules may be assigned to the ADF, to the MF, and to each EF
- The ADF supports up to 16 bytes for proprietary security information
- Up to 304 bytes user memory is available to store an application data. Customers can configure the number of EFs and the corresponding file size

Near field communication (NFC) Forum Type 4 Tag

Supports NFC Forum Type 4 Tag functionality, see Chapter 3.1.2.3.

CIPURSE™move command set

- Multi-level commands
  - SELECT
- Commands for personalization of file system oriented product
  - CREATE_FILE
  - FORMAT_ALL
- Commands for file attribute management
  - READ_FILE_ATTRIBUTES
  - UPDATE_FILE_ATTRIBUTES
  - UPDATE_KEY
  - UPDATE_KEY_ATTRIBUTES

- Security-related commands
  - MUTUAL_AUTHENTICATE
  - GET_CHALLENGE
- Commands for file data management
  - READ_BINARY
  - UPDATE_BINARY
  - READ_RECORD
  - UPDATE_RECORD
  - READ_VALUE
  - INCREASE_VALUE
  - DECREASE_VALUE
  - LIMITED_INCREASE_VALUE
  - LIMITED_DECREASE_VALUE

Contactless interface

- Initialization and anticollision according to ISO/IEC 14443-3 [7] Type A using 4-byte fixed non-unique ID, 4-byte reused-ID, 4-byte random ID, or 7- byte UID(Double-Size UID) as defined in ISO/IEC 14443-3 [7]
- Data rates:
  - PCD to CIPURSE™move: 106 kbit/s, 212 kbit/s, and 424 kbit/s
  - CIPURSE™move to PCD: 106 kbit/s, 212 kbit/s, 424 kbit/s, and 848 kbit/s
- Transmission protocol according to ISO/IEC 14443-4 [8]

Security features

- Active shield technology
- Security attack countermeasures for critical security operations using both hardware and software mechanisms
- Access limitation for manufacturer-specific data (configurable)

Certification level

- CIPURSE™V2 certification

1.3 Coding and notation conventions

The following conventions are used throughout this document:

- All lengths are represented in bytes
- Each byte is represented by bits b8 to b1, where b8 is the most significant bit and b1 the least significant bit
- Multibyte fields and values are presented in big-endian order
- Binary values are specified with the subscript suffix "B" (for example, 0101_B)
- Hexadecimal values are specified with the subscript suffix "H" (for example, $B4_H$)

2 Ordering and packaging information

The portfolio of CIPURSE™move products comprises different products in different packages, which basically have the same functionality but not the same unique identifier (UID) number and UID length. The following table presents the possible products in the portfolio that can be ordered.

Table 1 Ordering information

Type	Package	Delivery state UID	Ordering code
SLM 10TLC002L – MCC8	MCC8-2-6[1)]	7-byte UID[2) 3)]	on request
SLM 10TLC002L – NB	Unsawn/Sawn wafer, NiAu bump[4)]	7-byte UID	on request

1) Pure Contactless Module (MCC8): for standard thickness inlays (330 µm)
2) Unique identifier (UID) of the product can be adjusted by customer from 7-byte UID to a ISO/IEC 14443-3 [7] Type A random ID (RND-ID), see Chapter 3.1.4.3 for more details
3) For a FNUID (Fixed Non-Unique Identity 4-byte number) or a 4-byte reused-ID please contact your local Infineon sales office
4) Wafer thickness: 75 µm and 120 µm with NiAu bump 20 µm

Figure 3 Module contactless card - MCC8-2-6

Figure 4 Pin configuration

Table 2 Pin definitions and functions

Symbol	Function
L_A	Coil connection pin L_A
L_B	Coil connection pin L_B

3 CIPURSE™move application support

The CIPURSE™move operational interface includes the storage of the data objects in the memory, the related command set, as well as the associated security mechanisms, in order to ensure interoperability between a CIPURSE™move product (a card implementing a limited use ticket profile) and CIPURSE™compliant terminals.

3.1 File system of the CIPURSE™move

The file system implemented by the CIPURSE™move is compliant to the file system specified in ISO/IEC 7816-4 [3]. As an example, Figure 5 shows the structure of the file system containing one CIPURSE™V2 application and one PxSE application.

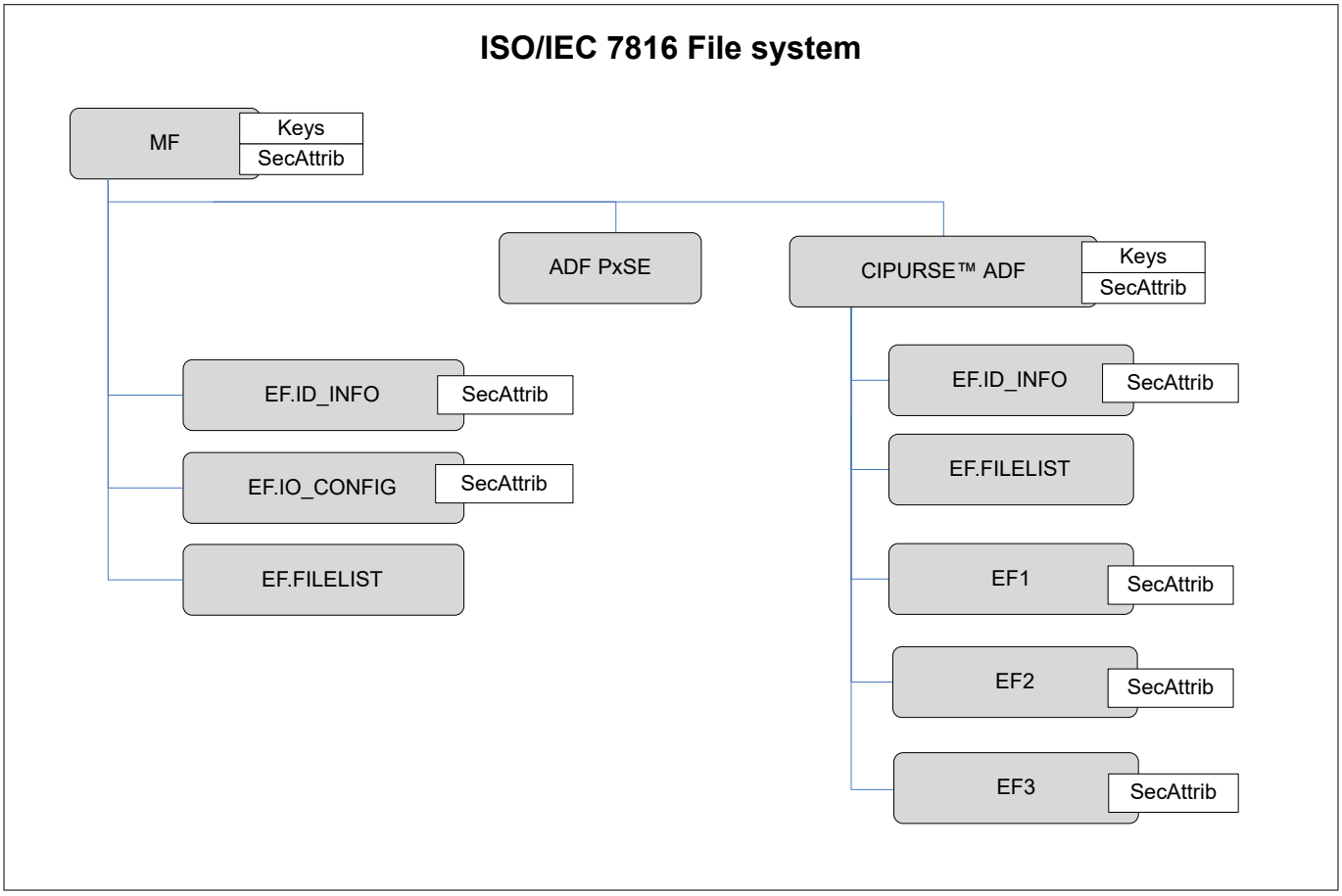

Figure 5 Example of a CIPURSE™move's file system structure

For application operation, the files in the file system are organized logically in form of two-level DF tree structure. The MF forms the root of this structure. The MF hosts three predefined EFs and one 128-bit AES key and it allows creation of one PxSE ADF and one CIPURSE™ ADF.

A CIPURSE™ application is represented by an ADF identified by its FID and DF name (AID). The ADF hosts two predefined EFs and up to two 128-bit AES keys and it allows creation of up to three EFs.

A PxSE ADF is a specific application, which is created without child files and security attributes.

Security attributes defining the access rights and secure messaging rules may be assigned to the CIPURSE™ ADF, to the MF, and to each EF. The file system offers up to 304 bytes memory to store user data.

3.1.1 Master file

MF consists of keys, security attributes, and hosts custom ADFs (see Chapter 3.1.2) in addition to pre-defined EFs (see Chapter 3.1.4) and custom EFs (see Chapter 3.1.3).

The CIPURSE™move supports implicit selection of the MF as a result of radio frequency (RF) initialization and anticollision process.

MF supports the following commands:

- CREATE_FILE (ADF/EF)
- FORMAT_ALL
- GET_CHALLENGE
- MUTUAL_AUTHENTICATE
- UPDATE_KEY
- UPDATE_KEY_ATTRIBUTES
- READ_FILE_ATTIRBUTES
- UPDATE_FILE_ATTRIBUTES
- SELECT (by FID/AID)

3.1.2 Application dedicated files

An ADF is identified by its AID or by its FID.

CIPURSE™move supports three type of ADFs:

- CIPURSE™ ADF
- PxSE ADF
- NFC Type 4 Tag ADF

3.1.2.1 CIPURSE™ ADF

CIPURSE™ ADF consists of keys and security attributes, and it hosts the EFs with application-specific data as described in Chapter 3.1.3 in addition to pre-defined EFs (see Chapter 3.1.4).

CIPURSE™ ADF can be secured or unsecured based on the security attributes defining access conditions and secure messaging, and key values as described in Chapter 3.2.

CIPURSE™ ADF supports the following commands:

- CREATE_FILE (EF)
- GET_CHALLENGE
- MUTUAL_AUTHENTICATE
- UPDATE_KEY
- UPDATE_KEY_ATTRIBUTES
- READ_FILE_ATTIRBUTES
- UPDATE_FILE_ATTRIBUTES
- SELECT (by FID/AID)

3.1.2.2 PxSE ADF

PxSE application registers the segment specific CIPURSE™ applications such as dedicated to transport applications, event ticketing applications, and facility access applications.

PxSE application supports the SELECT (by AID) command only.

The response to SELECT PxSE provides the list of AIDs corresponding to its registered CIPURSE™ applications and one of its registered applications might be implicitly selected.

3.1.2.3 NFC Forum Type 4 Tag ADF

The product supports an NFC type ADF [9] with the same functionality as a CIPURSE™ ADF with the following exceptions during ADF creation:

- EF.ID_INFO is not automatically created
- EF.FILELIST is not automatically created

The creation of EF with the same file ID as EF.ID_INFO or EF.FILELIST is not allowed.

3.1.3 Supported elementary file types

EFs are used to store data and are identified by its FID or by short file identifier (SFID).

The file system supports the following elementary file types:

- Binary file
- Linear record file
- Linear value-record file

EFs can be secured or unsecured based on the security attributes as described in Chapter 3.2.

The commands READ_FILE_ATTRIBUTES and UPDATE_FILE_ATTRIBUTES can be used to read and update the EF attributes.

Binary file:

A binary file represents a series of sequential bytes without specific inner structure. Size of the file is defined at file creation.

On file creation, the data are created and initialized with zeros. The commands READ_BINARY and UPDATE_BINARY can be used to read and update the records.

The maximum size of the binary file is restricted to 304 bytes.

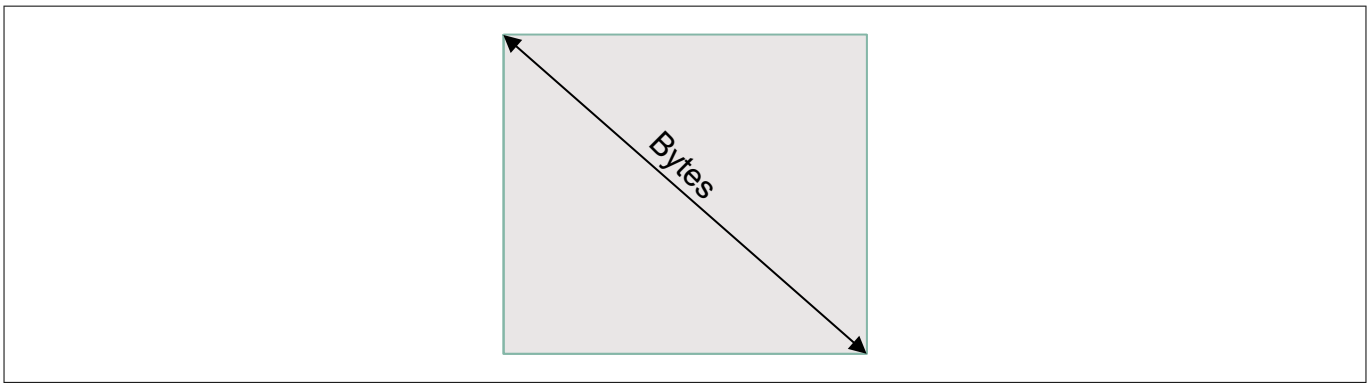

Figure 6 Binary file

Linear record file:

A linear record file represents a linear sequence of records of same size. Size and number of records are defined at file creation.

On file creation, all records are created and initialized with zeros. The commands READ_RECORD and UPDATE_RECORD can be used to read and update the records.

The possible sizes of a record are 4 byte, 8 byte, and 16 byte. A file can contain maximum of 76 records. The maximum size of the linear record file (size of record x number of records) is restricted to 304 bytes.

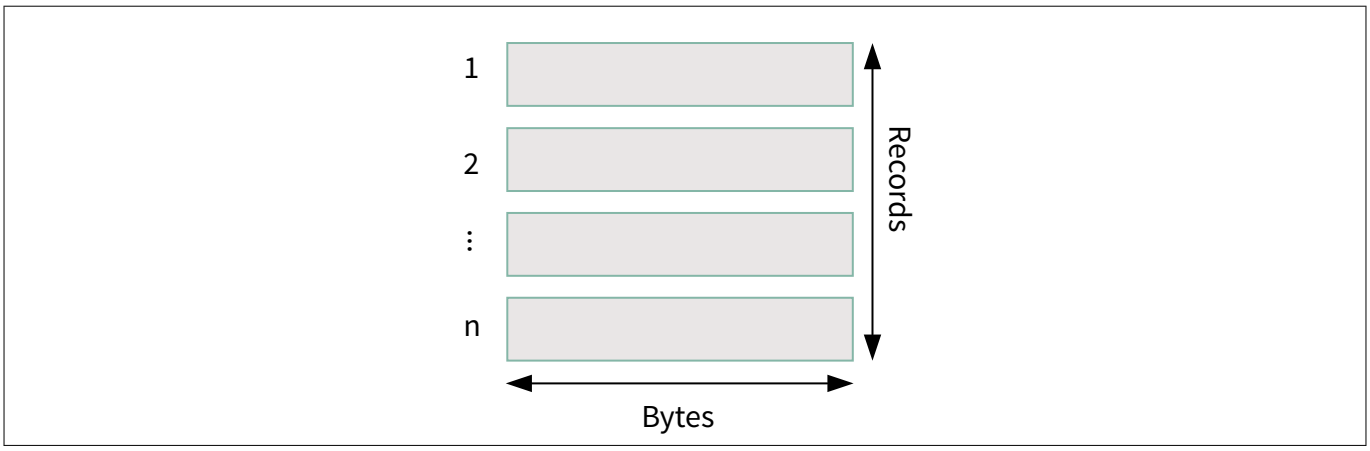

Figure 7 Linear record file

Value-record file:

A value-record file represents a linear sequence of records of 12 bytes. Each value-record contains maximum and minimum limit and a counter value field. Number of records is defined at file creation.

On file creation, all records are created and initialized with 0000 0000_H (counter value), 7FFF $FFFF_H$ (maximum limit), and 8000 0000_H (minimum limit). The commands READ_RECORD and UPDATE_RECORD can be used to read and update the records. The commands READ_VALUE, INCREASE_VALUE, and DECREASE_VALUE can be used to read and manipulate the counter values. If modification of the value violates the limits, the command will be rejected.

The commands LIMITED_INCREASE_VALUE and LIMITED_DECREASE_VALUE can be used to offer a refund functionality that is limited to the number of tokens decreased/increased in last transaction. The value record remembers the last increase or decrease operation and enables refund up to the value that existed before increase or decrease. The commands UPDATE_RECORD, LIMITED_INCREASE_VALUE, and LIMITED_DECREASE_VALUE will reset the information granting limited refund functionality.

A file can contain maximum of 6 records.

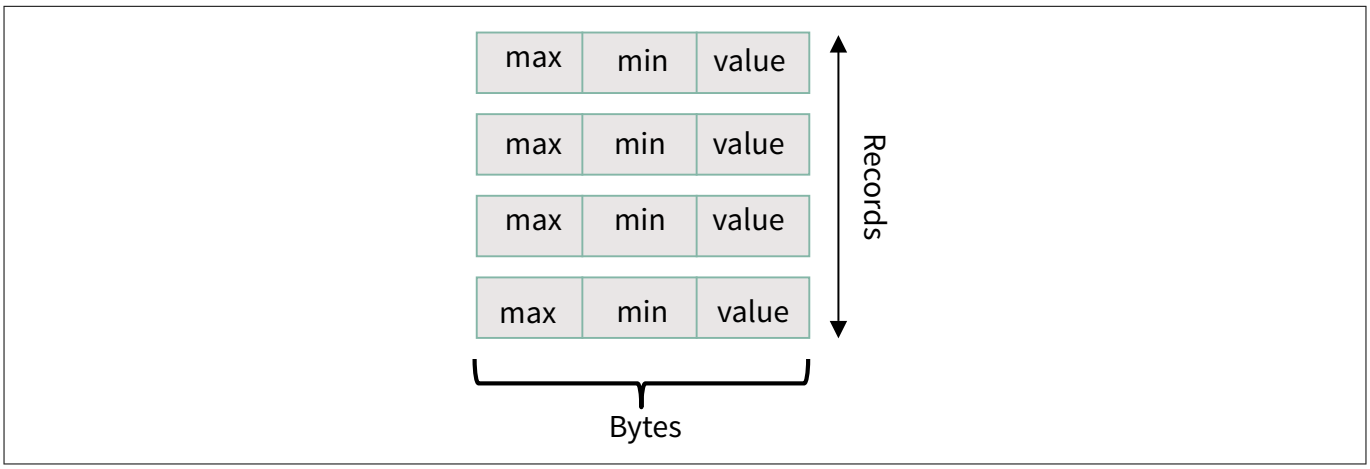

Figure 8 Value-record file

3.1.4 Predefined elementary files

Predefined EFs under the MF are present at delivery state, need not be created and cannot be deleted. The security attributes can be modified.

Predefined EFs under the ADF are implicitly created during ADF creation. Deletion is only possible by deleting the parent ADF. The security attributes can be modified.

Table 3 List of predefined EFs

File name	File type	Description
EF.FILELIST	Binary	Read-only file under the MF/ADF providing list of files under the MF/ADF
EF.ID_INFO	Binary	Read-only file under the MF/ADF providing information about the supported CIPURSE™ version and the features valid for all ADFs as well as product-unique manufacturer specific information
EF.IO_CONFIG	Binary	File under the MF providing information about the parameters used for contactless communication

3.1.4.1 EF.FILELIST

The EF.FILELIST (under the MF/ADF) is read-only file and provides a 4-byte file information for each file present under the MF/ADF. The size of EF.FILELIST varies depending on the number of files currently present in the MF/ADF.

Table 4 Structure and contents of EF.FILELIST

EF.FILELIST	Type: Binary, read-only		
Content		**Length [byte]**	**Description**
File #1	FID	2	File identifier of File #1
	SFID	1	Short file identifier of File #1
	FD	1	File descriptor byte of File #1
		Var.	Further FID || SFID || FD fields...
File #n	FID	2	File identifier of File #n
	SFID	1	Short file identifier of File #n
	FD	1	File descriptor byte of File #n

3.1.4.2 EF.ID_INFO

The predefined file EF.ID_INFO is a read-only file and is available under the MF and CIPURSE™ ADF. EF.ID_INFO files are identical across all applications in one product.

The structure and content of the EF.ID_INFO file are as described Table 5.

Table 5 Structure and content of EF.ID_INFO

EF.ID_INFO	Type: Binary, Read-only
Offset	**Description**
0-7	CIPURSE™ version along with features (file system oriented personalization and profiles) are supported
8	Integrated circuit manufacturer, as per ISO/IEC 7816-6 [4]: • 05_H: Infineon Technologies
9-23	Chip identification data

(table continues...)

Table 5 (continued) Structure and content of EF.ID_INFO

EF.ID_INFO	Type: Binary, Read-only
Offset	**Description**
24-32	Reserved for further manufacturer information
33	Vendor specific data
34-36	Software version
37-39	Product identifier

3.1.4.3 EF.IO_CONFIG

The EF.IO_CONFIG file contains IO configuration parameters as defined in the Table 6. The IO interface configuration of the product can be modified by updating the parameters in this file and is available under the MF.

Table 6 Structure and contents of EF.IO_CONFIG

EF.IO_CONFIG	Type: Binary
Offset	**Description**
0	Baudrate. Indicates supported bit rates by the CIPURSE™move.
1	List of configuration items: • Indicates the reading capability of the EF.FILELIST on MF and ADF level • Indicates the usage of ISO/IEC 14443-3 Type A random ID (RND-ID) number of historical bytes returned as part of the answer to select (ATS) response
2-8	Initial historical bytes: • Controller control byte • Product identifier bytes • Software version bytes
9-15	Additional bytes to allow extending historical bytes. It is recommended to set these bytes to 00_H.

3.1.5 File referencing methods

To access the data, the files in a CIPURSE™ conforming products can be selected by using the following methods (Explicit selection or Implicit selection).

Explicit selection:

- A SELECT command is used for explicit selection mode
- A different combination of the parameters along with the SELECT command will perform the explicit selection such as:
  - For explicit selection of MF, the SELECT command with FID $3F00_H$ can be used
  - For explicit selection of ADF, the SELECT command with AID or an FID can be used
  - For explicit selection of EF, the SELECT command with FID or a command supporting addressing by SFID can be used

Implicit selection:

- RF initialization and anticollision process is used for implicit selection of MF
- Selection of a PxSE application may result in implicit selection of one of its registered ADFs
- Implicit selection of EF is not supported

3.1.6 Reserved file identifiers

Some of the FIDs are reserved to serve a special purpose such as file identifiers of MF and pre-defined EFs.

3.2 Security architecture

The security architecture of this product consists of keys representing the various roles, an authentication mechanism to check the availability of a key, and the file security attributes to grant access to entitled roles only.

The security architecture is intended to restrict the access and operations on the application's data to authorized entities only.

Before executing a command on a secured object, the CIPURSE™move checks if the security requirements are met in terms of file security attributes which are access rights and secure messaging rules.

3.2.1 Keys

AES-128 bit keys are used for authentication. Keys are associated to ADF/MF.

Each key has a set of secure and non-secure attributes as defined below:

- Secure key attributes are used to control the operations permissible with/on this key such as if the key can be updated or is immutable, and if the key is valid or invalid
- Non-secure key attributes hold an additional key information and cryptographic algorithm identifier

3.2.2 Mutual authentication and security state

Figure 9 shows the states and resulting security levels reached when a terminal sends the commands GET_CHALLEGE and MUTUAL_AUTHENTICATE to mutually authenticate both terminal and CIPURSE™move.

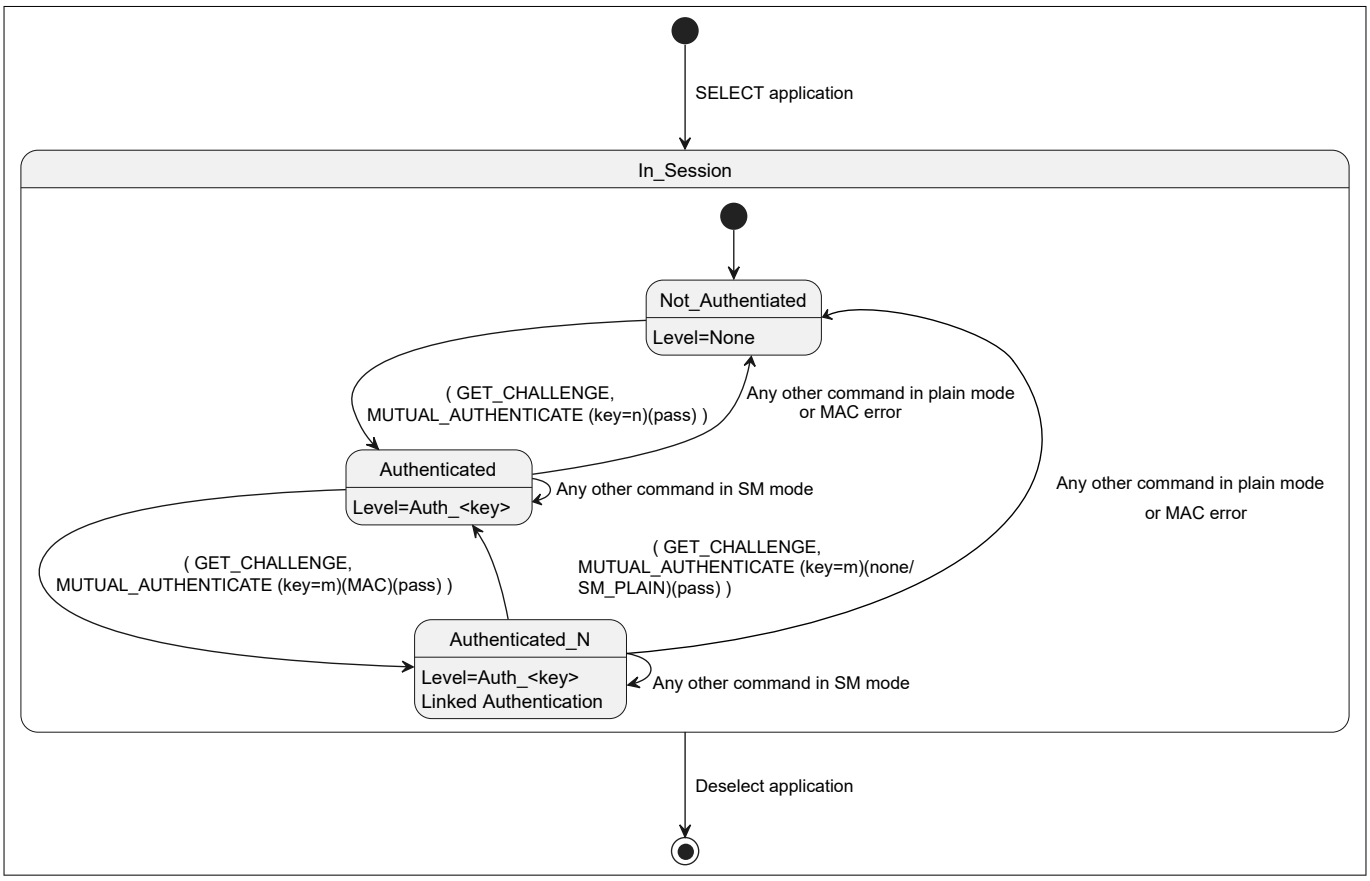

Figure 9 Authentication states and security level

After selection of the application owning the keys, the application is in Not_Authenticated state with security level none.

- A GET_CHALLENGE command followed by MUTUAL_AUTHENTICATE command with valid cryptogram results in a transition to Authenticated state with security level Auth_<key> referencing the key number used for authentication

In Authenticated state, all commands must be transmitted in secure channel mode.

- A GET_CHALLENGE command followed by a MUTUAL_AUTHENTICATE command with valid cryptogram, received in SM_MAC mode, and referencing a new key will result in Authenticated_N state with "linked authentication" where the previous state's security level Auth_<key> is retained and the security level will change from Auth_<old key> to Auth_<new key>

In Authenticated_N state, all commands must be transmitted in secure channel mode.

- A GET_CHALLENGE command followed by a MUTUAL_AUTHENTICATE command with valid cryptogram, received without secure channel or secure messaging with plain data (SM_PLAIN), will result in Authenticated state with no "linked authentication" where the security level will reset to Auth_<new key>

Any command received in plain mode or in secure messaging (SM) mode with invalid cryptogram will reset the state to Not_Authenticated with security level none.

When a security level Auth_<key> is reached, the terminal acquires the right to execute the commands that are granted to this security level, as described in Chapter 3.2.3.

3.2.3 Access rights

Access rights grant each security level rights to execute various commands respective to a file type. Also, it defines unconditional access ("ALWAYS") to enable PCDs to execute commands irrespective of the security level reached and the secure messaging rules assigned to the file, see Chapter 3.2.4.

If none of the rights are enabled, the commands cannot be executed irrespective of the security level.

3.2.4 Secure messaging rules

Secure messaging rules (SMR) define for a file, the minimum secure messaging levels required to execute various commands respective to a file type.

There are two different secure messaging levels available, as follows:

- SM_PLAIN: Data is sent in plain and the transferred command does not include an integrity protection field
- SM_MAC: Integrity-protected communication with a field of MAC in the transferred command and the data is sent in plain

The PCD defines the communication security level applicable for exchanging the messages between PCD and CIPURSE™move.

The CIPURSE™move evaluates if the chosen security level is acceptable for the addressed file and operation.

3.3 Command set

This section defines all the commands available for operation of CIPURSE™ application.

Table 7 Overview of CIPURSE™ commands

Command	Description
Multi-level commands	
SELECT	Selects the file (MF, ADF, or EF)
Commands for personalization of file system oriented product	
CREATE_FILE (ADF, EF)	Creates an ADF or an EF in the CIPURSE™move file system

(table continues...)

Table 7 (continued) Overview of CIPURSE™ commands

Command	Description
FORMAT_ALL	Formats the file system to its initial data state The MF keys, MF key attributes, and the content and attributes of predefined EFs under the MF are not formatted
Commands for file attribute management	
READ_FILE_ATTRIBUTES	Reads the MF, DF, or EF file attributes
UPDATE_FILE_ATTRIBUTES	Updates the MF, DF, or EF file attributes
UPDATE_KEY	Updates the value of a key in the CIPURSE™move
UPDATE_KEY_ATTRIBUTES	Updates the attributes of a key in the CIPURSE™move
Security related commands	
MUTUAL_AUTHENTICATE	Mutual authentication with the CIPURSE™move
GET_CHALLENGE	Retrieves the challenge information from the CIPURSE™move in order to proceed with authentication
Commands for file data management	
READ_BINARY	Reads a data from a binary file
UPDATE_BINARY	Updates a data into a binary file
READ_RECORD	Reads a records from a record file or a value record file
UPDATE_RECORD	Updates a data into an existing record in a record file or a value record file
READ_VALUE	Reads a value from a value record file
INCREASE_VALUE	Increases the value in a value record file
DECREASE_VALUE	Decreases the value in a value record file
LIMITED_INCREASE_VALUE	Increases the value in a value record file within a limited range defined by the previous DECREASE_VALUE operation
LIMITED_DECREASE_VALUE	Decreases the value in a value record file by a limited amount

4 Contactless I/O functionality

The CIPURSE™move supports contactless I/O communication according to ISO/IEC 14443-3 [7] and ISO/IEC 14443-4 [8] and as configured in EF.IO_CONFIG at the time of manufacturing of the product.

4.1 Communication principle

All operations on the CIPURSE™move are initiated by an appropriate reader and controlled by its internal logic. Prior to any application specific operations, the CIPURSE™move has to be selected according to the ISO/IEC 14443-3 [7] Type A anticollision and selection scheme.

After selection, the proximity coupling device (PCD) must send a request for answer to select (RATS) command to enter ISO/IEC 14443-4 [8] transmission protocol processing (T=CL).

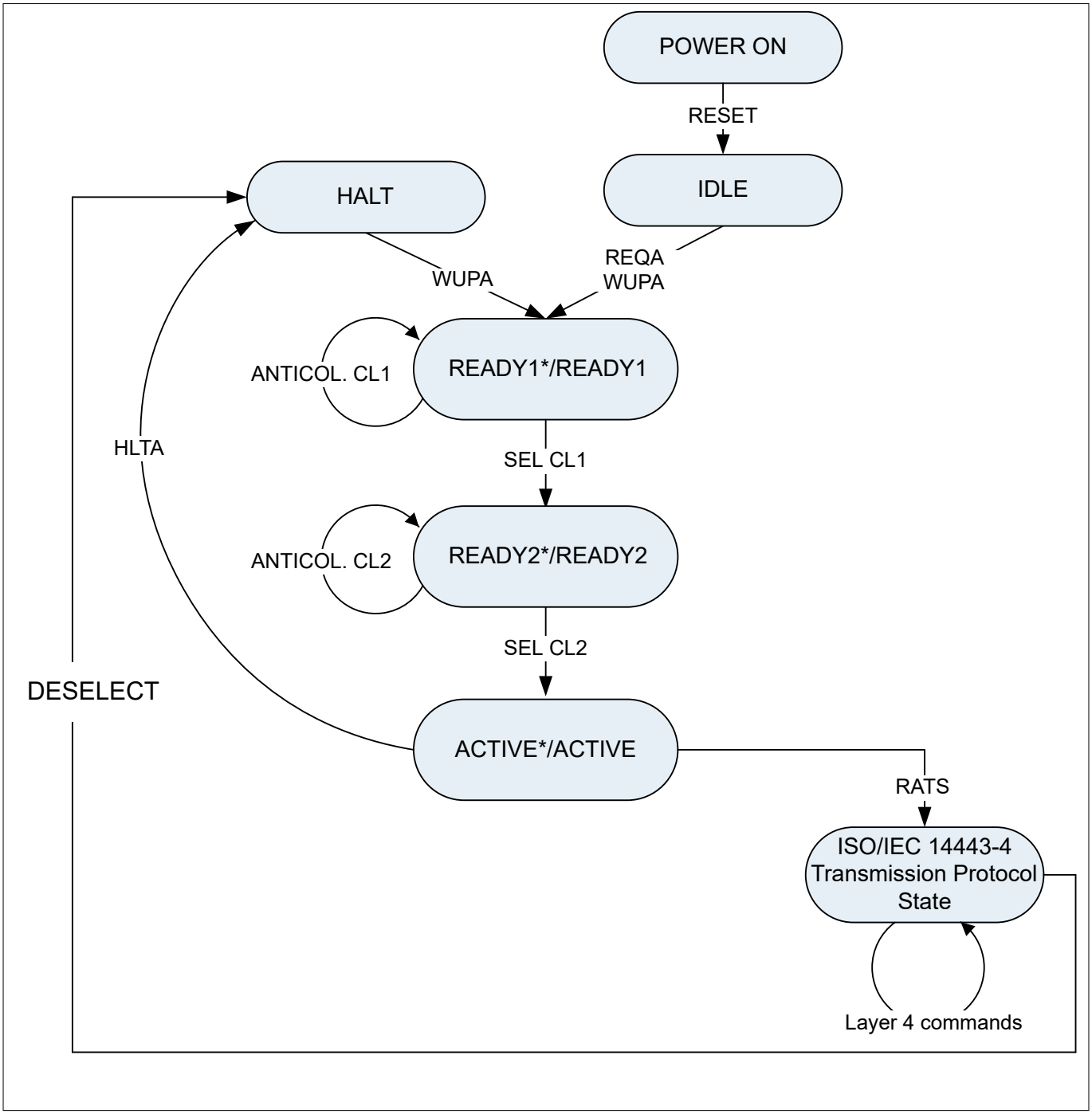

Figure 10 CIPURSE™move communication state diagram

4.2 ISO/IEC 14443 feature set

The following features and types of commands are available:

- Commands for RF initialization and bit frame anticollision as per ISO/IEC 14443-3 [7], Type A
- Commands for operating the half-duplex block transmission protocol as per ISO/IEC 14443-4 [8], with the following feature profile:
  - CIPURSE™move and PCD chaining is supported.
  - Card identifier (CID) is not supported.
  - Node address (NAD) is not supported
  - Power level indication inside the CID is not supported.
- The error handling is performed as defined in ISO/IEC 14443-3 [7] and ISO/IEC 14443-4 [8].

5 Operational characteristics

5.1 Absolute maximum ratings

Stresses above those listed may cause permanent damage to the device. This is a stress rating only and functional operation of the device at these or any other conditions above those indicated in the operational sections of this data sheet is not implied. Exposure to absolute maximum rating conditions for extended periods may affect device reliability, including electrically erasable programmable read-only memory (EEPROM) data retention and write/erase endurance.

Table 8 Absolute maximum ratings

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
Input peak voltage between L_A - L_B	$V_{AB\ peak}$			6	V	
Input current through L_A - L_B	I_{IN}			30	mA	
Junction temperature	$T_{junction}$	-25		+110	°C	
Storage temperature	$T_{storage}$	-40		+125	°C	For chip. For modules according to module specification
ESD protection	V_{ESD}	2			kV	EIA/JESD22-A114-B

5.2 Electrical characteristics

Table 9 Operation range

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
Ambient temperature	$T_{ambient}$	-25		+70	°C	$T_{junction}$ must not be exceeded
Endurance (erase/write cycles)[1)]		10^5				
Data retention (years)[1)]		10				
EEPROM erase and write time	t_{prog}	4			ms	Combined erase and write per EEPROM page (16 byte);$T_{ambient}$ = 25°C

1) Values are temperature dependent. For further information please refer to your Infineon Technologies Office or Representative.

Table 10 Contactless interface characteristics

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
Operating conditions	H	1.5		7.5	A/m	Reference setup according to ISO/IEC 14443-2 [6] and ISO/IEC 10373-1 [5]

(table continues...)

Table 10 (continued) Contactless interface characteristics

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
Chip input capacitance	C_{AB}		17		pF	$V_{AB\ RMS}$ =2 V f_{res} = 13.56 MHz $T_{ambient}$ = 25°C deviation: +/- 10%
Recommended target resonance frequency	f_{res}	13.56		17.5	MHz	ID1 (Class 1) card size

References

CIPURSE™/OSPT

[1] OSPT Alliance: *CIPURSE™V2 , Operation and Interface Specification (Revision 2.0), 2013-12-20, incl. Errata and Precision List (Revision 3.0)*; 2017-09-27

[2] OSPT Alliance: *CIPURSE™V2 , CIPURSE™L Profile Specification (Revision 2.0), 2013-12-20, incl. Errata and Precision List (Revision 1.0)*; 2015-01-22

ISO/IEC

[3] ISO/IEC 7816-4:2020: *Identification cards - Integrated circuit cards - Part 4: Organization, security and commands for interchange (Fourth edition)*; 2020-05

[4] ISO/IEC 7816-6:2016: *Identification cards - Integrated circuit cards - Part 6: Interindustry data elements for interchange (Third edition)*; 2016-06

[5] ISO/IEC 10373-1:2020-10: *Cards and security devices for personal identification – Test methods - Part 1: General characteristics (Third edition)*; 2020-10

[6] ISO/IEC 14443-2:2020: *Cards and security devices for personal identification – Contactless proximity objects - Part 2: Radio frequency power and signal interface (Fourth edition)*; 2020-07

[7] ISO/IEC 14443-3:2018: *Cards and security devices for personal identification – Contactless proximity objects – Part 3: Initialization and anticollision (Fourth edition)*; 2018-07

[8] ISO/IEC 14443-4:2018: *Cards and security devices for personal identification – Contactless proximity objects – Part 4: Transmission protocols (Fourth edition)*; 2018-06

NFC Forum

[9] NFC Forum: *Type 4 Tag Technical Specification (Version 1.1)*; 2019-12-12

Glossary

ACG

access group (ACG)

ADF

application dedicated file (ADF)

AES

Advanced Encryption Standard (AES)
The standard for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001. The algorithm described by AES is a symmetric-key algorithm (i.e. the same key is used for both encryption and decryption).

AID

application identifier (AID)
Used to reference (select) an application.

APDU

application protocol data unit (APDU)
The communication unit between a smart card reader and a smart card.

ATS

answer to select (ATS)

CID

card identifier (CID)

CIPURSE™

Open security standard for transit fare collection systems. CIPURSE™ is a trademark of the Open Standard for Public Transport Alliance.

DFA

differential fault analysis (DFA)
A class of side channel attacks in the field of cryptography, specifically cryptographic analysis. Faults are induced into cryptographic implementations with the intention of revealing information about their internal states.

DF

dedicated file (DF)

DPA

differential power analysis (DPA)
A class of attacks against smart cards and secure cryptographic tokens. The attack involves monitoring how much power a microprocessor uses as it functions, then using advanced statistical methods to determine secret keys or personal identification numbers involved in the computations.

EEPROM

electrically erasable programmable read-only memory (EEPROM)

EF

elementary file (EF)
A file system component containing (user) data.

EIA

Electronic Industry Alliance (EIA)

ENC

encryption (ENC)

ESD

electrostatic discharge (ESD)
The sudden draining of electrostatic charge. Even with small charges, it poses a considerable risk to small semiconductor structures, in particular MOS structures. It is therefore essential to take precautions when dealing with unprotected semiconductors.

FD

file descriptor (FD)
Defines the file type (MF, ADF, type of EF).

FID

file identifier (FID)
Used to reference an elementary file.

FWI

frame waiting time integer (FWI)

ID

identification (ID)

IEC

International Electrotechnical Commission (IEC)
The international committee responsible for drawing up electrotechnical standards.

ISO

International Organization for Standardization (ISO)

MAC

message authentication code (MAC)
Used to prove message integrity.

MCC

module contactless card (MCC)

MF

master file (MF)
The root of the CIPURSE™ file system.

NAD

node address (NAD)

NFC

near field communication (NFC)

OSPT

Open Standard for Public Transport (OSPT)

PCD

proximity coupling device (PCD)
A reader device for NFC cards.

PxSE

proximity system environment (PxSE)
A generic term for various system-environment applications that are specific to the application family.

RATS

request for answer to select (RATS)

RF

radio frequency (RF)

SFID

short file identifier (SFID)

SMG

secure messaging group (SMG)
This belongs to the file security attributes. Commands are clustered into SMGs, where each of them lists one or more commands.

SMR

secure messaging rules (SMR)
Object-specific messaging rules combining four SMGs.

SM

secure messaging (SM)
A secure channel that is established between the secure element and a communication partner to ensure confidentiality and authenticity of the exchanged data.

SM_PLAIN

secure messaging with plain data (SM_PLAIN)
Communication with endpoint internal preparation for integrity verification. Data are sent plain, and the transferred frame does not include an integrity protection field.

UID

unique identifier (UID)

Revision history

Reference	Description
Revision 1.0, 2023-01-05 - Valid for product version V1.1.0 and higher	
All	Initial release

Trademarks

All referenced product or service names and trademarks are the property of their respective owners.

Edition 2023-01-05

Published by

Infineon Technologies AG

81726 Munich, Germany

Do you have a question about any aspect of this document?

Email:
CSSCustomerService@infineon.com

Document reference
IFX-vmi1663221597983

Important notice

The information given in this document shall in no event be regarded as a guarantee of conditions or characteristics ("Beschaffenheitsgarantie").

With respect to any examples, hints or any typical values stated herein and/or any information regarding the application of the product, 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.

In addition, any information given in this document is subject to customer's compliance with its obligations stated in this document and any applicable legal requirements, norms and standards concerning customer's products and any use of the product of Infineon Technologies in customer's applications.

The data contained in this document is exclusively intended for technically trained staff. It is the responsibility of customer's technical departments to evaluate the suitability of the product for the intended application and the completeness of the product information given in this document with respect to such application.

Warnings

Due to technical requirements 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 Infineon Technologies in a written document signed by authorized representatives of Infineon Technologies, Infineon Technologies' products may not be used in any applications where a failure of the product or any consequences of the use thereof can reasonably be expected to result in personal injury.