SLS 32TLC00xS(M)

CIPURSE™4move
Compliant to OSPT™ Alliance CIPURSE™S Profile
Optimized for Contactless Transport & Ticketing Applications

ISO/IEC 14443 Type A Contactless Interface
Optional Mifare Compatible Interface

Security Target

v1.7, 2016-07-19

Chip Card & Security

Edition 2016-07-19

Published by Infineon Technologies AG,

81726 Munich, Germany.

Legal Disclaimer

The information given in this document shall in no event be regarded as a guarantee of conditions or characteristics. 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 the nearest Infineon Technologies Office (**www.infineon.com**).

Warnings

Due to technical requirements, components may contain dangerous substances. For information on the types in question, please contact the nearest Infineon Technologies Office.

Infineon Technologies components may be used in life-support devices or systems only 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.

PUBLIC

Trademarks of Infineon Technologies AG

AURIX™, C166™, CanPAK™, CIPOS™, EconoPACK™, CoolMOS™, CoolSET™, CORECONTROL™, CROSSAVE™, DAVE™, DI-POL™, EasyPIM™, EconoBRIDGE™, EconoDUAL™, EconoPIM™, EconoPACK™, EiceDRIVER™, eupec™, FCOS™, HITFET™, HybridPACK™, I²RF™,ISOFACE™, IsoPACK™, MIPAQ™, ModSTACK™, my-d™, NovalithIC™, OptiMOS™, ORIGA™,POWERCODE™; PRIMARION™, PrimePACK™, PrimeSTACK™, PRO-SIL™, PROFET™, RASIC™,

ReverSave™, SatRIC™, SIEGET™, SINDRION™, SIPMOS™, SmartLEWIS™, SOLID FLASH™, TEMPFET™,thinQ!™, TRENCHSTOP™, TriCore™.

Other Trademarks

Advance Design System™ (ADS) of Agilent Technologies, AMBA™, ARM™, CIPURSE™, OSPT™, MULTI-ICE™, KEIL™,PRIMECELL™, REALVIEW™, THUMB™, µVision™ of ARM Limited, UK. AUTOSAR™ is licensed by AUTOSARdevelopment partnership. Bluetooth™ of Bluetooth SIG Inc. CAT-iq™ of DECT Forum. COLOSSUS™,FirstGPS™ of Trimble Navigation Ltd. EMV™ of EMVCo, LLC (Visa Holdings Inc.). EPCOS™ of Epcos AG.FLEXGO™ of Microsoft Corporation. FlexRay™ is licensed by FlexRay Consortium. HYPERTERMINAL™ of Hilgraeve Incorporated. IEC™ of Commission Electrotechnique Internationale. IrDA™ of Infrared Data Association Corporation. ISO™ of INTERNATIONALORGANIZATION FOR STANDARDIZATION. MATLAB™ ofMathWorks, Inc. MAXIM™ of Maxim Integrated Products, Inc. MICROTEC™, NUCLEUS™ of Mentor Graphics Corporation. MIPI™ of MIPI Alliance, Inc. MIPS™ of MIPSTechnologies, Inc., USA. muRata™ of MURATA MANUFACTURING CO., MICROWAVE OFFICE™ (MWO) of Applied Wave Research Inc., OmniVision™ of OmniVision Technologies, Inc. Openwave™ Openwave Systems Inc. RED HAT™ Red Hat, Inc. RFMD™ RF Micro Devices, Inc. SIRIUS™ of Sirius Satellite Radio Inc. SOLARIS™ of Sun Microsystems, Inc. SPANSION™ of Spansion LLC Ltd. Symbian™ of Symbian Software Limited. TAIYO YUDEN™ of Taiyo Yuden Co. TEAKLITE™ of CEVA, Inc. TEKTRONIX™ of Tektronix Inc. TOKO™ of TOKO KABUSHIKI KAISHA TA. UNIX™ of X/Open Company Limited. VERILOG™, PALLADIUM™ of Cadence Design Systems, Inc. VLYNQ™ of Texas Instruments Incorporated. VXWORKS™, WIND RIVER™ of WIND RIVER SYSTEMS, INC. ZETEX™ of Diodes Zetex Limited.

Miscellaneous

The term "Mifare" in this document is only used as an indicator of product compatibility to the corresponding established technology. This applies to the entire document wherever the term is used.

Last Trademarks Update 2014-05-26

Revision History

Version	Change Description
1.0	Initial version
1.1	Minor updates
1.2	Minor updates
1.3	Section 6.2.2: Note extended
1.4	Section 1.4.2.2: Reference corrected
1.5	Section 1.4.2.2: User guidance updated
1.6	Section 1.4.1: Minor updates
1.7	Changed version of release notes and product version

Table of Contents

1 ST introduction (ASE_INT)

1.1 ST reference

The title of this document is “Security Target SLS 32TLC00xS(M) CIPURSE™4move”. Its version is v1.7 dated 2016-07-19.

1.2 TOE reference

The TOE is a composite based on the M7791 B12 platform (for details see [5]). The name of the TOE is “SLS 32TLC00xS(M) CIPURSE™4move”. It provides a file system oriented operating system. Its version is v1.00.01.

This ST is compatible to [5].

1.3 TOE overview

The TOE provides a file system oriented operating system and is based on the M7791 B12 security controller by Infineon Technologies AG. Its file system meets [ISO/IEC 7816-4]. The TOE is targeted for contactless ticketing and payment applications compliant to CIPURSE™V2. Different and flexible access rights to application functions and secure messaging rules can be configured for each file. CIPURSE™V2 also defines a protocol, which primarily aims at providing mutual authentication and secure messaging between the TOE and a subject e.g. terminal. Secure messaging allows the protection of integrity and/or confidentiality of the exchanged messages.

The major security features of the TOE include:

Supports the creation of applications with up to 8 keys per application, which allows to implement 8 different access levels;128-bit key length for AES encryption

Flexible key management

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 based on [ISO/IEC 7816-4], with AES-MAC or AES-encryption

Secure messaging mode configurable for each data exchange

Data exchange protocol inherently DPA and DFA resistant

Sequence integrity protection

The TOE is a smartcard device based on the M7791 B12 hardware and supports contactless I/O communication in [ISO/IEC 14443-4] Type A. The device contains a software part compliant to CIPURSE™V2, which provides a file system according to [ISO/IEC 7816-4] with flexible access rights, a mutual authentication method (3-pass as per [ISO/IEC 9798-2]) using AES with a terminal and secure messaging for integrity and confidentiality (AES-MAC or AES-encryption).

Optionally the TOE provides a Mifare compatible system in addition. The Mifare compatible system does not contribute to the security features of the TOE.

The TOE 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). After anti-collision and selection as per [ISO/IEC 14443-3], the terminal may either enter Mifare compatible emulation or [ISO/IEC 14443-4] transmission protocol to transmit e.g. CIPURSE™V2 compatible commands to the TOE.

1.4 TOE description

1.4.1 Logical scope of the TOE

Figure 1 provides an overview of the TOE’s logical components:

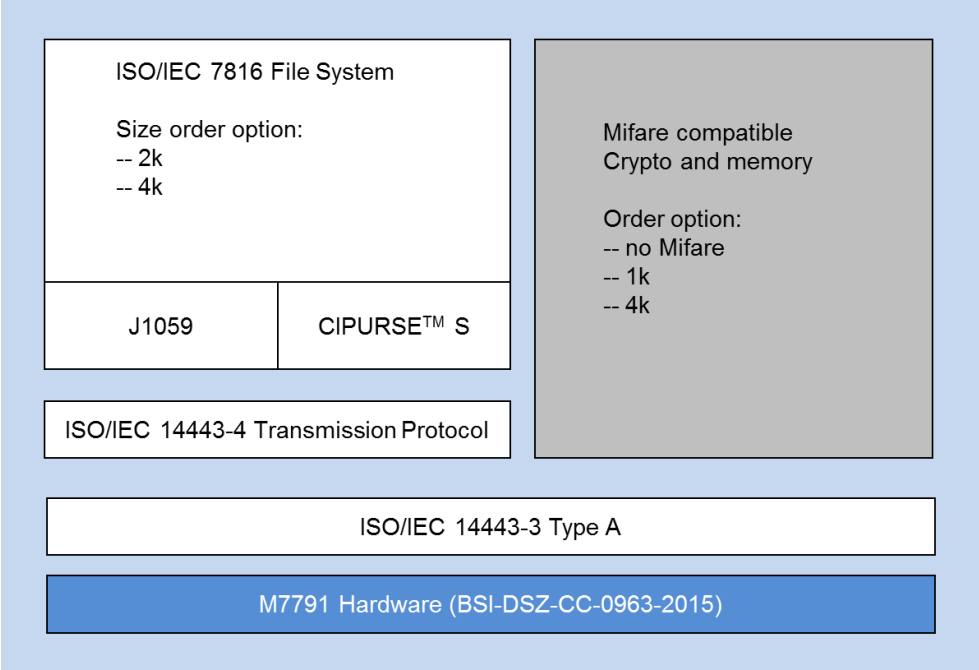

Figure 1 TOE logical components overview

The TOE is a smartcard device based on the M7791 B12 hardware (dark blue rectangle) and supports contactless I/O communication in [ISO/IEC 14443-4] Type A. The device contains a software part compliant to CIPURSE™V2, which provides a file system according to [ISO/IEC 7816-4] with flexible key management, flexible access rights, a mutual authentication method (3-pass as per [ISO/IEC 9798-2]) using AES with a terminal and secure messaging for integrity and confidentiality (AES-MAC or AES-encryption).

The CIPURSE™V2 file system based operating system further provides commands and features particularly for personalisation and administration. The command set for application operation complies with [ISO/IEC 7816-4] and [ISO/IEC 7816-9], completed with proprietary coded commands in [ISO/IEC 7816-4] APDU format. Furthermore the J1059 block offers additional commands not covered by the CIPURSE™ specification but that are described in SLS 32TLC00xS(M) Cipurse™4move Data Book [12], chapter 3.3. It also provides enhanced functionality for several commands from the CIPURSE™ specification.

The File System is available in two different sizes: 2k and 4k depending on the customer`s requirement.

The TOE may also contain a Mifare compatible system to support migration to CIPURSE™V2 (dark grey area). Whether the Mifare compatible system is part of the TOE and whether 1k or 4k functionality is provided depends on the customer`s choice and is an ordering option. In case the Mifare compatible system is part of the TOE, the external subject communicating with TOE decides during the startup phase of the TOE, whether the CIPURSE™V2 file system based operating system or the Mifare compatible system is started. The Mifare compatible system does not provide any TSF. Neither does it interfere with any of the TSF provided by the TOE. Logically all TSF of the TOE belong to the white area.

If the Mifare compatible system is part of the TOE, Mifare area is accessible by CIPURSE™ using Mifare Elementary Files and Dedicated Files with are mapped to Mifare sectors at creation time.

1.4.2 Physical scope of the TOE

The TOE consists of a hardware part, firmware part, software part and the user guidance. The hardware and firmware parts are described in [5]. The optionally available SCL software from [5] is not part of this TOE. Table 1 describes the platform configuration used for this TOE.

Table 1 Platform configuration

Module / Feature	Values
Memories	
SOLID FLASH™	100 kBytes

RAM for the user	4 kBytes
Modules	
µSCP	Available
Interfaces	
RFI – ISO 14443 generally	Available
RFI Input Capacity	27pF, 56pF, 78pF
ISO 14443 Type A card mode	Available
ISO 14443 Type B card mode	Available
ISO 14443 Type C card mode (1)	Available
Advanced Communication Mode	Available/unavailable
Mifare-Compatible availability	Available/unavailable
Mifare Hardware support card mode	Available/unavailable
Advanced Mode for Mifare-Compatible Technology (AMM)	Available/unavailable
SW support for Mifare compatible 4k cards	Available/unavailable
SW support for Mifare compatible 1k cards	Available/unavailable
Direct data transfer (DDT)	Available/unavailable
Miscellaneous	
maximum System Frequency	33MHz to 45MHz
metal configuration number	0x0
FW Version	V77.014.11.2

(1) Also known as ISO 18092 (card mode)

1.4.2.1 Software of the TOE

The software uses the hardware and firmware as platform. It is stored on the hardware NVM and builds the file system based operating system. Its version is v1.00.01.

1.4.2.2 User guidance

The user guidance comprises:

- **CIPURSE™4move Data Book, Revision 1.2, 2015-12-08**

This document is a description of the SLS 32TLC00xS(M) CIPURSE™4move

- **CIPURSE™V2 Operation and Interface Specification, Revision 2.0, 2013-12-30**

This document specifies the feature set available to all members of the CIPURSE™V2 family

- **CIPURSE™V2 Operation and Interface Specification Errata and Precision List, Revision 1.0, 2014-09-18**

This document specifies the Errata and Precisions for CIPURSE™V2 Operation and Interface Specification.

- **CIPURSE™V2 CIPURSE™ S Profile Specification, Revision 2.0, 2013-12-20**

This document focuses on the application level, personalization and administration features that shall be supported by a CIPURSE™S PICC.

- **CIPURSE™V2 Cryptographic Protocol, Revision 1.0, 2012-09-28**

This document specifies the cryptographic mechanisms of cards (i.e. PICCs) and terminals (i.e. PCDs) compliant to this CIPURSE™ specification

- **CIPURSE™V2 Cryptographic Protocol R1.0 Errata and Precision List, Revision 1.0, 2014-09-18**

This document specifies the Errata and Precisions for The CIPURSE™V2 CIPURSE™ Cryptographic Protocol

- **CIPURSE™4move Personalization Manual, Revision 1.2, 2015-12-01**

This document provides information to developers to ease personalization of SLS 32TLC00xS(M) devices

- **SLS 32TLC00xS(M) CIPURSE™ Chip Identification Guide, Version 1.0, 2015-08-13**

This document provides guidance, how to identify the platform of the TOE

- **SLS 32TLC00xS(M) CIPURSE™4move SLS 32TLC00xS(M) V1.0.1 Release Notes, Revision 1.0, 2016-07-07**

This document provides a summary of product key features and operational hints to the user

1.4.3 Interfaces to the TOE

The physical interface of the TOE to the external environment is the entire surface of the IC.

The RF interface (radio frequency power and signal interface) enables contactless communication between a PICC (proximity integration chip card, PICC) and a terminal reader/writer (proximity coupling device, terminal). The transmission protocol meets [ISO/IEC 14443-4]. Commands for RF initialisation and bit frame anticollision meet [ISO/IEC 14443-3] and [ISO/IEC 14443-4] type A. Furthermore the TOE implements the shortcut anticollision support to be compatible to the legacy Mifare infrastructure.

The command interface to the TOE is provided by the CIPURSE™ operating system.

1.4.4 Lifecycle and delivery

The lifecycle of the TOE consists of 4 phases

1.4.4.1 Phase 1: Development

This phase includes the development of IC, firmware and software.

1.4.4.2 Phase 2: Manufacturing

This phase includes the production of the IC containing firmware and software. It may also include dicing, packaging and antenna mounting, however these processes are optional. The TOE can be delivered in the form of complete modules, as plain wafers, in an IC case (e.g. DSO20) or in bare dies.

1.4.4.3 Phase 3: Personalization

The personalization process contains 2 sub-stages as follows:

1. Personalization of MF and predefined files under the MF
2. Personalization of other initialisation data: this includes e.g. configuration of access rights, secure messaging rules, file content and AES keys. This sub stage prepares the TOE for operational use by consumers. It may overlap with phase 4, e.g. the TOE's personalization phase might be finished during its operational use.

1.4.4.4 Phase 4: Operational use

Subjects within the TOEs environment can make use of the TOE depending on the TOE´s configuration and the subjects' authority. The TOE in this phase contains relevant and integrity and/or confidentiality protected file content.

1.4.4.5 Delivery of the TOE

The TOE is delivered after sub-stage 1 of phase 3. Phase 3 sub-stage 2 and phase 4 are not part of this evaluation process.

1.4.4.6 Lifecycle roles

There are three roles during the lifecycle: Producer, Personalization Agent and User. The producer covers phase 1 and 2 and is Infineon Technologies AG. The Personalization Agent covers phase 3. The user may be any subject, who makes use of the TOE within its operational environment (e.g. system administrator, consumer).

2 Conformance Claims (ASE_CCL)

2.1 CC Conformance Claim

This Security Target and the TOE is Common Criteria version v3.1 part 2 [3] conformant and Common Criteria version v3.1 part 3 [4] conformant.

2.2 PP Claim

This TOE is a composite based on M7791 B12. The M7791 B12 Security Target [5] is in strict conformance to the Security IC Platform Protection Profile [1].

2.3 Package Claim

The assurance level for the TOE is EAL5 augmented with the components ALC_DVS.2 and AVA_VAN.5.

3 Security Problem Definition (ASE_SPD)

3.1 Assets

The table as follows provides an overview of the assets to be protected:

Table 2 Assets of the TOE and their protection level

	Protection kind	
Asset	**Integrity**	**Confidentiality**
Keys	X	X
Security attributes	X	-
Security services	X	-
System file content	X[1]	X[1]
User file content	X[2]	X[2]
UID	-	X[3]

[1]security services enable the system provider to protect file content. It´s up to the system provider to decide, which system file content to protect.

[2]security services enable the user to protect file content. It´s up to the user to decide, which user file content to protect.

[3]a security service allows a user to hide the UID during a transaction. If this service is used the UID is only protected in case the Mifare compatible system is not part of this TOE.

The keys include the authentication keys, session keys and frame keys used for secure messaging.

The security attributes consist of:

The key security attributes for the authentication keys, which define the rights for updating the key

The access rights assignments, which assign the right to execute particular commands to a dedicated set of authentication keys

The secure messaging rules, which define the communication security levels for transferring data between an external subject and TOE

The Security Services include:

Secure messaging

Access rights protection and Secure Messaging rules enforcement

Mutual authentication

Command Level Atomicity

3.2 Threats

The TOE faces threats as follows:

T.Access

Unallowed execution of commands and unallowed access of assets

Adverse action:

Bypassing or manipulating access control.

Threat agent:

Attacker with attack potential high

Targeted asset:
all assets

T.Access_UID
Access UID by non authorised terminals to link and trace user sessions
Adverse action:
Non authenticated terminals link user sessions to specific TOE users via UID
Threat agent:
Attacker with attack potential high
Targeted asset:
UID

T.Forge-Auth
An attacker may try to forge authentication data to obtain unallowed authorisation
Adverse action:
Obtain unallowed security user role by forging authentication data or manipulating the authentication mechanism
Threat agent:
Attacker with attack potential high
Targeted asset:
All assets

T.Hijack-Session
An attacker may hijack an authorised session of a subject e.g. by a man-in-the middle or replay attack.
Adverse action:
Hijack an existing authorised session to obtain a security user role without having to present authentication data
Threat agent:
Attacker with attack potential high
Targeted asset:
All assets

T.Tearing
An attacker may try to create an inconsistent state within the TOE to compromise an asset
Adverse action:
Interrupt power supply of the TOE to create an inconsistent state within the TOE. E.g. an attacker may try to interrupt during a memory write operation in order to manipulate its content.
Threat agent:
Attacker with attack potential high
Targeted asset:
All assets

3.3 Organisational Security Policies

none

3.4 Assumptions about the operational environment

Due to the authentication process with an external subject (terminal), two assumptions are necessary for this TOE:

A.Secure-Authentication-Data

CIPURSE™ relies on confidential keys for authentication purposes, which needs to be generated externally and downloaded to the TOE. During this process the operational environment is responsible to keep these keys confidential. These keys are used to derive session keys on the TOE.

A.Terminal-Support

The terminal ensures integrity and confidentiality

The terminal verifies data (e.g. authentication data, MAC) sent by the TOE and follows the minimum communication security level defined by the TOE to ensure integrity and confidentiality of the transferred data.

4 Security Objectives (ASE_OBJ)

4.1 Security Objectives of the environment of the TOE

Due to the assumptions of this TOE, environmental objectives are defined as follows:

OE.Secure-Authentication-Data

Generation of secure authentication data

Secure and confidential keys for authentication purposes shall be generated by the environment. These values are then personalised onto the TOE during phase 3.

OE.Terminal-Support

Integrity and confidentiality of data exchanged

The terminal shall verify data (e.g. authentication data, MAC) sent by the TOE and follow the minimum communication security level defined by the TOE to ensure integrity and confidentiality of transferred data.

4.2 Security Objectives of the TOE

The TOE security objectives are defined as follows:

O.Access-Control

The TOE shall provide a mechanism to restrict access to user data, security attributes and authentication keys to dedicated subjects.

O.Authentication

The TOE shall provide a mechanism to differentiate between authorised and non-authorised subjects and also to allow a dedicated attribution of access rights to authorised subjects. Further the TOE shall provide verification data to allow external subjects to validate the authenticity of the TOE.

O.Confidentiality

The TOE shall provide a functionality to exchange confidential messages by means of encryption via the communication interface. Security attributes shall allow to enforce the encryption of certain messages.

O.Integrity

The TOE shall provide a functionality to exchange integrity protected messages via the communication interface. Therefore the TOE shall send verification data to the recipient in order for the recipient to check its integrity.

O.Command-Atomicity

The TOE shall provide a mechanism for tearing safe execution of commands. This means during an execution of a command either all the updates to the data stored on the TOE are successfully performed or no data are changed in case of command execution interruption.

O.No-Trace

The TOE shall offer a configuration option, which does not allow user traceability by a “none” authorised subject in case the CIPURSE™V2 file system based operating system is activated during startup.

4.3 Security Objectives Rationale

The security objectives rationale from [1] and [5] are also applicable to this ST. Table 3 provides a mapping of the additional threats and policies to the objectives of the TOE. The rationale explains how the objectives cover the threat or policy.

Table 3 Security Objectives mapping and Rationale

Threat/Policy/assumption	Security Objective	Rationale
T.Access	O.Access-Control O.Confidentiality O.Integrity O.Authentication	O.Access-Control uses the outcome of the authentication process to limit accessibility. O.Confidentiality and O.Integrity protect the communication between terminal and TOE O.Authentication provides access to functions to authorised users.
T.Access_UID	O.No-Trace	O.No-Trace hides the UID
T.Forge-Auth	O.Authentication	Definition of O.Authentication directly upholds this threat
T.Hijack-Session	O.Authentication O.Confidentiality O.Integrity	O.Authentication requests resistance against man-in-the-middle and replay attacks. O.Confidentiality and O.Integrity protect the communication between terminal and TOE
T.Tearing	O.Command-Atomicity	Objective prevents inconsistent memory content in case of unexpected command interruption.
A.Secure-Authentication-Data	OE.Secure-Authentication-Data	Objective directly upholds assumption
A.Terminal-Support	OE.Terminal-Support	Objective directly upholds assumption

5 Extended Component Definition (ASE_ECD)

There are no extended components defined for this TOE.

6 Security Requirements (ASE_REQ)

6.1 TOE Security Functional Requirements

The security functional requirements (SFR) for this TOE are defined in this chapter.

Table 4 lists all SFRs used for this ST and refinements, if available:

Table 4 TOE SFRs

TOE SFRs	
FMT_SMR.1	Not refined
FMT_SMF.1/CIPURSE	Not refined
FMT_MSA.1/CIPURSE	Not refined
FMT_MSA.3/CIPURSE	Not refined
FDP_ACF.1/CIPURSE	Not refined
FDP_ACC.1/CIPURSE	Not refined
FPT_FLS.1/CIPURSE	Not refined
FIA_UID.2	Not refined
FIA_UAU.2	Not refined
FIA_UAU.3	Not refined
FIA_UAU.5	Not refined
FPR_UNL.1	Not refined
FPT_RPL.1	Not refined
FTP_TRP.1	Not refined
FCS_COP.1/CIPURSE/AES	Not refined
FCS_CKM.4	Not refined
FCS_CKM.1	Not refined

There are no refinements available.

6.2 SFRs of this ST

The software part of this composite TOE provides additional functionality compared to [5]. Therefore an iteration operation (see [2] section 8.1.1 “The iteration operation”) is used on several SFRs, which are already selected and assigned in either [1] or [5]. All iterations within this ST are uniquely identified using the naming convention “<SFR>/CIPURSE”.

6.2.1 SFRs related to access control

The TOE shall meet the requirement “Security roles (FMT_SMR.1)” as specified below.

FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles

Key_x_ART_y: Each Key x of each access right assignment y defines a security role with dedicated access rights.

NonAuth: this role refers to a non-authenticated user

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

The TOE shall meet the requirement "Specification of management functions (FMT_SMF.1/CIPURSE)" as specified below.

FMT_SMF.1/CIPURSE Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1/CIPURSE The TSF shall be capable of performing the following management functions:

TSF data management: Changing authentication keys;

Security attribute management: Changing key security attributes, secure messaging rules and access right assignments;

The TOE shall meet the requirement "Management of security attributes (FMT_MSA.1)" as specified below:

FMT_MSA.1/CIPURSE Management of security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control or
FDP_IFC.1 Subset information flow control]
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.1.1/CIPURSE The TSF shall enforce the *"CIPURSE™ Access control and security management policy" (see chapter 6.2.7)* to restrict the ability *to modify* the security attributes *all security attributes* to *any role.*

The TOE shall meet the requirement "Static attribute initialisation (FMT_MSA.3)" as specified below.

FMT_MSA.3/CIPURSE Static attribute initialisation

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1/CIPURSE The TSF shall enforce the *"CIPURSE™ Access control and security management policy" (see chapter 6.2.7)* to provide

- *ART: permissive for MF and read/modify for EF.IO_CONFIG and read only for all other predefined EFs*
- *key security attributes: permissive*
- *SMRs: SM_PLAIN for Command and Response SM-APDU for MF and all predefined EFs*

default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the[1] *no role* to specify alternative initial values to override the default values when an object or information is created.

Application Note: The only security attributes with default or initial values are the ones for the predefined files including MF. For all other security attributes explicit initial values have to be provided by the external subject during their creation.

The TOE shall meet the requirement "Security attribute based access control (FDP_ACF.1/CIPURSE) specified below.

FDP_ACF.1/CIPURSE Security attribute based access control

Hierarchical to: No other components.

[1] the should be ~~the~~

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1/CIPURSE The TSF shall enforce the *"CIPURSE™ Access control and security management policy" (see chapter 6.2.7)* to objects based on the following:

access rights assignment

FDP_ACF.1.2/CIPURSE The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

allowance exists, if an object´s corresponding security attribute "access rights assignment" grants a subject's identity to perform the targeted operation.

FDP_ACF.1.3/CIPURSE The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: *none.*

FDP_ACF.1.4/CIPURSE The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *none.*

Application Note: Objects of the TOE are card toplevel, application and elementary file. Card toplevel, application and elementary file objects can only be accessed using commands provided by this TOE.

Subject in this context refers to the terminal

The TOE shall meet the requirement "Subset access control (FDP_ACC.1)" as specified below.

FDP_ACC.1/CIPURSE Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/CIPURSE The TSF shall enforce the *"CIPURSE™ Access control and security management policy" (see chapter 6.2.7) on all subjects, objects and security attributes.*

6.2.2 SFR related to command atomicity

The TOE shall meet the requirement "Failure with preservation of secure state (FPT_FLS.1)" as specified below.

FPT_FLS.1/CIPURSE Failure with preservation of secure state

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_FLS.1.1/CIPURSE The TSF shall preserve a secure state when the following types of failures occur:

(1) Command execution interruption during execution of following commands:

a. UPDATE_BINARY
b. UPDATE_RECORD
c. APPEND_RECORD
d. INCREASE_VALUE
e. DECREASE_VALUE
f. ACTIVATE_FILE (ADF)
g. DEACTIVATE_FILE (ADF)
h. UPDATE_FILE_ATTRIBUTES
i. UPDATE_KEY
j. UPDATE_KEY_ATTRIBUTES
k. LIMITED_INCREASE_VALUE
l. LIMITED_DECREASE_VALUE

m. *CREATE_FILE*
n. *FORMAT_ALL*
o. *DELETE_FILE*

Note: *Any changes to Mifare mapped memory area is not protected with command level atomicity [affected commands are UPDATE_RECORD and FORMAT_ALL]. Command level atomicity is also not supported for Mifare compatible emulation configuration changes done on EF.IO_CONFIG [affected commands are FORMAT_ALL and UPDATE_BINARY]*

6.2.3 SFR related to randomized UID

FPR_UNL.1 Unlinkability

Hierarchical to: No other components.

Dependencies: No dependencies.

FPR_UNL.1.1 The TSF shall ensure that *none authorized subjects* are unable to determine whether *any two operations of the TOE were caused by the same user.*

Note: this SFR is only enforced, if the Mifare compatible system is not part of the TOE, i.e. in case the order option "No Mifare compatible" is selected.

6.2.4 SFR related to cryptography

Preface regarding Security Level related to Cryptography

The strength of the cryptographic algorithms was not rated in the course of the product certification (see [24] Section 9, Para.4, Clause 2). But Cryptographic Functionalities with a security level of lower than 100 bits can no longer be regarded as secure without considering the application context. Therefore for these functionalities it shall be checked whether the related crypto operations are appropriate for the intended system. Some further hints and guidelines can be derived from the 'Technische Richtlinie BSI TR-02102', www.bsi.bund.de.

Any Cryptographic Functionality that is marked in column '*Security Level above 100 Bits*' of the following table with '*no*' achieves a security level of lower than 100 Bits (in general context).

Table 5 TOE cryptographic functionality

Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security level above 100 Bits
Session key agreement	AES	[16], section 5.3 "Session Key Derivation and Authentication Algorithm"	$\|K_{ID}\| = 128$	yes
Authentication	AES	[16], section 5.3 "Session Key Derivation and Authentication Algorithm" and [16], section 6.3 "Integrity Protection"	$\|K\| = 128$	yes
Secure Messaging for Integrity	MAC based on AES	[16], section 6.3 "Integrity Protection"	$\|K\| = 128$	no
Secure Messaging for Confidentiality	AES	[16], section 6.4 "Confidential Communication"	$\|K\| = 128$	yes

The AES Operation of the TOE shall meet the requirement "Cryptographic operation (FCS_COP.1)" as specified below.

FCS_COP.1/CIPURSE/AES Cryptographic operation

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/CIPURSE/AES

The TSF shall perform *encryption and decryption* in accordance to a specified cryptographic algorithm *Advanced Encryption Standard (AES)* and cryptographic key sizes of *128 bit* that meet the following standards:
U.S. Department of Commerce, National Institute of Standards and Technology, Information Technology Laboratory (ITL),

Advanced Encryption Standard (AES), FIPS PUB 197, modes of usage: [16] section 5.2 "Session Key Derivation", [16] section 6.2 "Key Derivation for the first Frame", [16] section 6.3 "Integrity Protection", [16] section 6.4 "Confidential Communication"

6.2.5 SFRs related to authentication and secure messaging

The TOE shall meet the requirement "User identification before any action (FIA_UID.2)"

FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

Dependencies: No dependencies.

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Note: "None" authentication is also an authentication method. Identification in this context means determining the user's role.

The TOE shall meet the requirement "User authentication before any action (FIA_UAU.2)" as specified below

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.2.1: The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Note that "None" authentication is also an authentication method.

The TOE shall meet the requirement "Unforgeable authentication (FIA_UAU.2)" as specified below

FIA_UAU.3 Unforgeable authentication

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.3.1 The TSF shall *detect and prevent* use of authentication data that has been forged by any user of the TSF.

FIA_UAU.3.2 The TSF shall *detect and prevent* use of authentication data that has been copied from any other user of the TSF.

The TOE shall meet the requirement "Multiple authentication mechanisms (FIA_UAU.5)" as specified below

FIA_UAU.5 Multiple authentication mechanism

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1 The TSF shall provide *none, three-way cryptographic authentication protocol* to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to *the rules described below:*

None: Any subject, which does not go through an explicit authentication protocol is authenticated to have access to commands clustered in ACGs with the flag "ALWAYS" for MF, secured ADFs and EFs and some dedicated further commands[1]*. In case of unsecured ADFs or EFs, there are no access restrictions.*

Three-way cryptographic authentication protocol: three-way challenge-and-response protocol, cf [ISO9798], Part 2 section 5.2.2 "Three pass authentication", and [16] section 5 "Authentication"

The TOE shall meet the requirement "Replay detection (FPT_RPL.1)" as specified below

FPT_RPL.1 Replay detection

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_RPL.1.1 The TSF shall detect replay for the following entities: *three way cryptographic authentication; secure messaging for integrity and confidentiality.*

FPT_RPL.1.2 The TSF shall perform *output of failure and rejection to enter security state*[2] when replay is detected.

The TOE shall meet the requirement "Trusted Path (FTP_TRP.1)" as specified below.

FTP_TRP.1 Trusted Path

Hierarchical to: No other components.

Dependencies: No dependencies

FTP_TRP.1.1 The TSF shall provide a communication path between itself and *remote* users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from *disclosure and/or modification*.

FTP_TRP.1.2 The TSF shall permit *remote users* to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for *data exchanges between external subject and TOE according to "CIPURSE™ access control and security management policy" (see chapter 6.2.7) based on the security attribute "Secure messaging rules"*

6.2.6 SFRs related to key generation/destruction

The TOE shall meet the requirement "Cryptographic key generation (FCS_CKM.1)" as specified below.

FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *Session key and secure messaging key generation policy (see chapter 6.2.7.7)* and specified cryptographic key sizes *128 Bit* that meet the following:

CIPURSE™ Cryptographic Protocol [16]

The TOE shall meet the requirement "Cryptographic key destruction (FCS_CKM.4)" as specified below.

FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]

[1] SELECT, GET_CHALLENGE, MUTUAL_AUTHENTICATE

[2] A security state of the TOE is entered by successful authentication terminal to TOE with a valid key

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *Session key and secure messaging key destruction policy (see chapter 6.2.8)* that meets the following: *None*.

6.2.7 CIPURSE™ Access Control and security management Policy

6.2.7.1 Objects

Objects of the TOE are card toplevel, application and elementary file. Card toplevel, application and elementary file objects can only be accessed using commands provided by this TOE.

6.2.7.2 Security attributes

CIPURSE™ access control is based on the security attributes

access rights assignment

key security attributes

secure messaging rules

Security attributes exist on three different levels: card toplevel, application level and elementary file level.

6.2.7.3 Mutual Authentication

A security state is entered by a successful three-way challenge-and-response protocol between an external subject and TOE with a valid key.

By this, the external subject acquires the right to execute all commands on objects that are restricted to exactly this authentication key, as given in the access rights assignment (see section 6.2.7.4). The security state is linked to exactly one key and one application or card top-level.

Mutual authentication is done by virtue of a three-way challenge-and-response protocol plus verification by the terminal of a MAC'ed PICC response. Both TOE and external subject are in the possession of a common secret k_{ID}, from which another commonly known temporary secret k_0 is dynamically derived. k_0 is different in each session, hence it is called the *session key*. It is then used as an AES key for encrypting random values, that are passed between the two parties. The responses to the random challenges are verified by the two parties, followed by an acceptance or rejection of the terminal by the PICC. An acceptance or rejection of the PICC by the terminal is completed once a MAC'ed PICC response is verified by the terminal.

6.2.7.4 Access rights assignment

See [12] section 3.2.2 "Access rights assignment"

See [14] section 4.2.2 "Access rights assignment"

See [15] section 5.2.2 "Access rights assignment"

6.2.7.5 Key security attributes

See [14] section 4.2.1 "Keys"

6.2.7.6 Secure Messaging Rules

See [14] section 4.2 "Security Architecture",

See [14] section 4.2.3 "General Secure Messaging Rules",

See [14] section 4.2.4 "Object-specific Secure Messaging Rules"

6.2.7.7 Session key and secure messaging key generation policy

See [16] section 5.2 "Session Key Derivation",

See [16] section 5.3 “Session Key Derivation and Authentication Algorithm”

See [16] section 6.2 “Key Derivation for the first Frame”

See [16] section 6.3 “Integrity Protection”

See [16] section 6.4 “Confidential Communication”

6.2.8 Session key and secure messaging key destruction policy

The session key K_0 is destroyed after H_0 is generated by memory overwrite with a 128-bit random value. All secure messaging keys are destroyed after they have been used by memory overwrite with a 128-bit random value.

Each 128-bit random value used for key destruction is only used once.

6.3 Consistency of SFRs

Following table lists the dependencies of SFRs and shows, that all SFRs are met within this ST.

Table 6 Dependencies of SFRs

SFRs	Dependencies	Met by
FMT_SMR.1	FIA_UID.1	FIA_UID.2
FMT_SMF.1/CIPURSE	none	-
FMT_MSA.1/CIPURSE	FDP_ACC.1 or FDP_IFC.1 FMT_SMF.1 FMT_SMR.1	FDP_ACC.1/CIPURSE FMT_SMF.1/CIPURSE FMT_SMR.1
FMT_MSA.3/CIPURSE	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1/CIPURSE FMT_SMR.1
FDP_ACF.1/CIPURSE	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1/CIPURSE FMT_MSA.3/CIPURSE
FDP_ACC.1/CIPURSE	FDP_ACF.1	FDP_ACF.1/CIPURSE
FPT_FLS.1/CIPURSE	none	-
FPR_UNL.1	none	-
FCS_COP.1/CIPURSE/AES	FCS_CKM.1 or (FDP_ITC.1 or FDP_ITC.2), FCS_CKM.4	FCS_CKM.1, FCS_CKM.4
FIA_UID.2	none	-
FIA_UAU.2	FIA_UID.1	FIA_UID.2
FIA_UAU.3	none	-
FIA_UAU.5	none	-
FPT_RPL.1	none	-
FTP_TRP.1	none	-
FCS_CKM.4	FCS_CKM.1 or FDP_IFC.1	FCS_CKM.1
FCS_CKM.1	FCS_CKM.2 or FCS_COP.1	FCS_COP.1/CIPURSE/AES

6.4 Rationale for the Security Functional Requirements

Following table provides a mapping between objectives and SFRs:

Table 7 Objectives <-> SFR mapping

Security objectives	SFRs
O.Access-Control	FMT_SMR.1: access rights are based on security roles FMT_MSA.1/CIPURSE: access to security attributes is restricted FMT_MAS.3/CIPURSE: definition of initial values for security attributes FDP_ACF.1/CIPURSE: access rights are based on security attributes FDP_ACC.1/CIPURSE: scope of access control FMT_SMF.1/CIPURSE: Specification of Management Functions
O.Authentication	FCS_COP.1/CIPURSE/AES: cryptographic algorithm AES used for authentication FIA_UID.2, FIA_UAU.2: User identification and authentication required before any action FIA_UAU.3: authentication must be unforgeable FIA_UAU.5: multiple authentication mechanism supported FTP_TRP.1: trusted path enables integrity protected messaging
O.Confidentiality	FCS_COP.1/CIPURSE/AES: cryptographic algorithm AES used for secure messaging for confidentiality FPT_RPL.1: requirement to detect replay attacks FTP_TRP.1: trusted path enables confidential messaging FCS_CKM.1: appropriate key generation required for trusted path FCS_CKM.4: appropriate key destruction required for trusted path
O.Integrity	FCS_COP.1/CIPURSE/AES: cryptographic algorithm AES used for secure messaging for integrity FPT_RPL.1: requirement to detect replay attacks FTP_TRP.1: trusted path enables integrity protected messaging FCS_CKM.1: appropriate key generation required for trusted path FCS_CKM.4: appropriate key destruction required for trusted path
O.Command-Atomicity	FPT_FLS.1/CIPURSE: secure state preservation in case of command execution interruption
O.No-Trace	FPR_UNL.1: prevents linking different sessions to the same TOE user by non-authorised subjects

6.5 TOE Security Assurance Requirements

Table 8 lists the TOE's assurance requirements. None of the assurance requirements is refined:

Table 8 TOE assurance requirements

Aspect	Acronym	Description
Development	ADV_ARC.1	Security Architecture Description
	ADV_FSP.5	Complete semi-formal functional specification with additional error information
	ADV_IMP.1	Implementation representation of the TSF
	ADV_INT.2	Well-structured internals
	ADV_TDS.4	Semi-formal modular design
Guidance Documents	AGD_OPE.1	Operational user guidance

Aspect	Acronym	Description
	AGD_PRE.1	Preparative procedures
Life-Cycle Support	ALC_CMC.4	Production support, acceptance procedures and automation
	ALC_CMS.5	Development tools CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.2	Sufficiency of security measures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.2	Compliance with implementation standards
Security Target Evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.3	Testing: modular design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment	AVA_VAN.5	Advanced methodical vulnerability analysis

6.6 Rationale for the Assurance Requirements

The assurance level EAL5 and the augmentation with the requirements ALC_DVS.2, and AVA_VAN.5 were chosen in order to meet assurance expectations explained in the following paragraph.

An assurance level of EAL5 with the augmentations AVA_VAN.5 and ALC_DVS.2 are required for this type of TOE since it is intended to defend against sophisticated attacks. All threat agents in chapter 3.2 are attackers with attack potential high. This evaluation assurance package was selected for a card issuer to gain maximum assurance from positive security engineering based on good commercial practices.

7 TOE Summary Specification (ASE_TSS)

The Security Features of the TOE are described below and the relation to the security functional requirements is shown.

7.1 TOE security features

SF.Authenticate

The TOE provides a Three-way cryptographic challenge-and-response mechanism according to [ISO9798-2] and [16]. After successfully performing this challenge-and-response mechanism the TOE enters a secure communication state. Secure communication state means a security state as defined in chapter 6.2.7.3 .During the authentication a session key is generated by the TOE, which is used to subsequently derive keys for secure messaging activities. The authentication is finished, once a MAC'ed response of the PICC is verified by the terminal.

SF.SM

The TOE supports secure messaging for integrity and confidentiality with AES-MAC and AES-encryption based on [ISO/IEC 7816-4]1), using proprietary secure messaging APDU format (denoted as SM-APDU format, specified in [16]).

SF.Access

The TOE provides flexible access rights and secure messaging rules for each file. Up to 8 keys can be configured per application. Chapter 6.2.7 provides more information.

SF.Command-Atomicity

The TOE supports atomic execution of commands. Either all the updates to the data stored on the TOE are successfully performed or no data are changed in case of interruption during command execution.

SF.NoTrace

According to [ISO/IEC 14443-3], during anticollision the UID can be retrieved. The TOE can be configured such, that a randomized UID is provided instead of a fixed UID. This feature prevents external subjects (e.g. terminals operated by attackers) to trace and localize individual TOEs.

Table 9 provides a mapping between SFs and SFRs:

Table 9 Mapping SFR <-> SF

SFR	SF
FMT_SMR.1	SF.Access
FMT_SMF.1/CIPURSE	SF.Access
FMT_MSA.1/CIPURSE	SF.Access
FMT_MSA.3/CIPURSE	SF.Access
FDP_ACF.1/CIPURSE	SF.Access
FDP_ACC.1/CIPURSE	SF.Access
FIA_UID.2	SF.Authenticate
FIA_UAU.2	SF.Authenticate
FIA_UAU.3	SF.Authenticate
FIA_UAU.5	SF.Authenticate
FPT_RPL.1	SF.SM, SF.Authenticate
FTP_TRP.1	SF.SM

SFR	SF
FCS_CKM.1	SF.SM, SF.Authenticate
FCS_CKM.4	SF.SM, SF.Authenticate
FPT_FLS.1/CIPURSE	SF.Command-Atomicity
FPR_UNL.1	SF.NoTrace
FCS_COP.1/CIPURSE/AES	SF.SM, SF.Authenticate

All SFRs are mapped by SFs. The justification for the SFRs of this TOE to SFs is as follows:

The SFRs FMT_SMR.1, FMT_SMF.1/CIPURSE, FMT_MSA.1/CIPURSE, FMT_MSA.3/CIPURSE, FDP_ACF.1/CIPURSE and FDP_ACC.1/CIPURSE deal with access rights, roles and management of security attributes and are therefore mapped to SF.Access.

Successful replay (FPT_RPL.1) is prevented by the CIPURSE™ secure messaging protocol (SF.SM) with changing frame keys. The CIPURSE™ secure messaging protocol (SF.SM) meets the SFR of a trusted path (FTP_TRP.1). The cryptographic algorithm used for secure messaging is AES, therefore FCS_COP.1/CIPURSE/AES, FCS_CKM.1 and FCS_CKM.4 are also mapped to SF.SM

The family FIA_UAU sets requirements for user authentication. Therefore its components (FIA_UAU.2, FIA_UAU.3, FIA_UAU.5) used for this ST are all mapped to SF.Authenticate. Successful replay (FPT_RPL.1) during the CIPURSE™ authentication process is prevented by using a challenge and response protocol based on random numbers. The cryptographic algorithm used is AES, therefore FCS_COP.1/CIPURSE/AES, FCS_CKM.1 and FCS_CKM.4 are also mapped to SF.Authenticate. Authentication is required to determine the subject´s role. No authentication is defined here as an implicit kind of authentication and casts the user´s role “none”. Therefore the CIPURSE™ authentication process meets the SFR FIA_UID.2.

SF.Command-Atomicity meets the requirements of secure state preservation in case of command execution interruption FPT_FLS.1/CIPURSE.

SF.NoTrace allows to use random instead of fixed UID, which prevents to trace the TOE across sessions. FPR_UNL.1 requires to ensure that none authorized subjects are unable to determine whether any operation of the TOE were caused by the same user. New random UIDs are chosen for each session prevent such user traceability.

8 Statement of compatibility

The TOE indirectly depends on following platform TSFs from [5] to meet its additional SFR requirements:

SF_PS, SF_PMA, SF_PLA and SF_CS (AES part only).

Table 10 provides a mapping of additional TOE SFRs and indirect contribution of platform TSFs:

Table 10 indirect contribution of platform TSFs

Additional TOE SFRs	Contribution of
FMT_SMR.1	SF_PMA, SF_PLA
FMT_SMF.1/CIPURSE	SF_PS, SF_PMA, SF_PLA
FMT_MSA.1/CIPURSE	SF_PMA, SF_PLA
FMT_MSA.3/CIPURSE	none
FDP_ACF.1/CIPURSE	SF_PMA, SF_PLA
FDP_ACC.1/CIPURSE	SF_PMA, SF_PLA
FIA_UID.2	SF_PS, SF_CS (RNG)
FIA_UAU.2	SF_PS, SF_CS (RNG)
FIA_UAU.3	SF_PS, SF_CS (RNG)
FIA_UAU.5	SF_PS, SF_CS (RNG)
FPT_RPL.1	none
FTP_TRP.1	SF_PS
FCS_COP.1/CIPURSE/AES	SF_PS, SF_PMA, SF_PLA
FCS_CKM.4	none
FPT_FLS.1/CIPURSE	none

The TOE relies and is dependent on all SFs from [5]. In case of SF_CS only the random numbers are used. The symmetric cryptographic operations are not used. Instead the TOE provides its own implementation of AES used for mutual authentication and secure messaging.

8.1 IP_SFR (Irrelevant Platform SFRs) and RP_SFR (Relevant Platform SFRs) of [5]

RP_SFR: FRU_FLT.2, FPT_FLS.1, FMT_LIM.1. FMT_LIM.2, FAU_SAS.1, FAU_SAS.1, FPT_PHP.3, FDP_ITT.1, FPT_ITT.1, FDP_IFC.1, FPT_TST.2, FDP_ACC.1, FDP_ACF.1, FMT_MSA.1, FMT_MSA.3, FMT_SMF.1, FDP_SDI.1, FDP_SDI.2, FCS_RNG.1 => all except FCS_COP.1

IP_SFR: FCS_COP.1

Following table shows the assumptions of [5] rated according to ASE_COMP.1.2C (IrPA, CfPA or SgPA):

Table 11 Rating of assumptions

assumption	rating	comment
A.Process-Sec-IC	CfPA	Covered by lifecycle assurance
A.Plat-Appl	CfPA	Product follows user guidance of platform
A.Resp-Appl	CfPA	Product defines its assets

This means, that all platform assumptions are automatically fulfilled by this TOE.

The objectives of this TOE and its environment do not contradict any objectives of the platform TOE and its environment. There are no significant assumptions, which have to be included into this ST.

9 References

[1] Security IC Platform Protection Profile, Version 1.0, 15.06.2007, BSI-PP-0035

[2] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and General Model; Version 3.1 Revision 4 September 2012, CCMB-2012-09-001

[3] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements; Version 3.1 Revision 4 September 2012, CCMB-2012-09-002

[4] Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements; Version 3.1 Revision 4 September 2012, CCMB-2012-09-003

[5] Security Target Lite M7791 B12

[6] M7791 Controller Family for Payment Application Family Hardware Reference Manual

[7] Joint Interpretation Library, Application of Attack Potential to Smartcards, Version 2.9, January 2013

[8] M7791 Errata Sheet

[9] SLE 70 Family Programmer's Reference User's Manual

[10] M7791 Security Guidelines User's manual

[11] SLx 70 Family Production and Personalization User's Manual

Note that the versions of these documents are listed in the certification report.

[12] SLS 32TLC00xS(M) Cipurse™4move Data Book.

[14] CIPURSE™V2 Operation and Interface Specification and CIPURSE™V2 Operation and Interface Specification R2.0 Errata and Precision List.

[15] CIPURSE™V2 CIPURSE™ S Profile Specification.

[16] The CIPURSE™V2 Specification Cryptographic Protocol and CIPURSE™V2 Cryptographic Protocol R1.0 Errata and Precision List.

Note that the versions of these documents are listed in Chapter 1.4.2.2.

[17] Certification Report BSI-DSZ-CC-0963-2015 for Infineon smartcard IC (Security Controller) M7791 B12 with optional SCL library version 1.01.009 and with specific IC-dedicated firmware from Infineon Technologies AG

[ISO/IEC 7816-4] ISO/IEC 7816 International Standard: Identification cards - Integrated circuit cards; Part 4: Organization, security and commands for interchange. Edition 2005

[ISO/IEC 7816-9] ISO/IEC InternationalStandard: Identification cards - Integrated circuit(s) cards with contacts; Part 9: Commands for card management Edition 2004

[ISO/IEC 9798-2] ISO/IEC 9798 Information technology - Securitytechniques - Entity authentication; Part 2: Mechanisms using symmetric encipherment algorithms. Second edition, 1999-07-15, ISO/IEC 9798-2:1999(E) and Technical Corrigendum 1, 2004-02-01, ISO/IEC 9798-2:1999/Cor.1:2004(E)

[ISO/IEC 14443-3] ISO/IEC International Standard: Identification cards - Contactless integrated circuit(s) cards - Proximity cards; Part3: Initialization and anticollision Edition 2011

[ISO/IEC 14443-4] ISO/IEC International Standard: Identification cards - Contactless integrated circuit(s) cards - Proximity cards; Part4: Transmission protocols Edition 2008

[FIPS-197] U.S. Department of Commerce, National Institute of Standards and Technology, Information Technology Laboratory (ITL), Advanced Encryption Standard (AES), FIPS PUB 197, 2001-11-26

10 List of Abbreviations

AES	Advanced Encryption Standard
ACG	Access Group
ART	Access Rights Table
CC	Common Criteria
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
DF	Dedicated File
DFA	Differential Fault Analysis
DPA	Differential Power Analysis
EF	Elementary File
EMA	Electro Magnetic Analysis
HW	Hardware
IC	Integrated Circuit
IMM	Interface Management Module
I/O	Input/Output
ITSEC	Information Technology Security Evaluation Criteria
MAC	Message Authentication Code
MF	Master File
OS	Operating system
PCD	Proximity Coupling Device (i.e. CIPURSE™V2-compliant terminal)
PICC	Proximity Integrated Circuit Card (i.e. CIPURSE™V2-compliant card or any other object which hosts a CIPURSE™V2-compliant card application implementation)
SCL	Symmetric Crypto Library
SMG	Secure Messaging Group
SMR	Secure Messaging Rules
TSF	TOE Security Functionality

11 Glossary

Chip	Integrated Circuit
Controller	IC with integrated memory, CPU and peripheral devices
Firmware	Part of the software implemented as hardware
Hardware	Physically present part of a functional system (item)
Integrated Circuit	Component comprising several electronic circuits implemented in a highly miniaturized device using semiconductor technology
Mechanism	Logic or algorithm which implements a specific security function in hardware or software
Memory	Hardware part containing digital information (binary data)
Microprocessor	CPU with peripherals
Object	Physical or non-physical part of a system which contains information and is acted upon by subjects
Operating System	Software which implements the basic TOE actions necessary for operation
Random Access Memory	Volatile memory which permits write and read operations
Random Number Generator	Hardware part for generating random numbers
Security Function	Part(s) of the TOE used to implement part(s) of the security objectives
Security Target	Description of the intended state for countering threats
SmartCard	Plastic card in credit card format with built-in chip
Software	Information (non-physical part of the system) which is required to implement functionality in conjunction with the hardware (program code)
Subject	Entity, the TOE communicates with, e.g. in the form of a terminal, which performs actions
Target of Evaluation	Product or system which is being subjected to an evaluation
Threat	Action or event that might prejudice security

w w w . i n f i n e o n . c o m

Published by Infineon Technologies AG