TÜBİTAK BİLGEM UEKAE

NATIONAL RESEARCH INSTITUTE OF ELECTRONICS AND CRYPTOLOGY

eID Applications Unit

AKİS v2.2.8I

SECURITY TARGET LITE

Revision no	01
Revision date	17.12.2014
Document code	AKİS-228I-STLite-01
Prepared by	eID Applications Unit
Approved by	AKİS Project Manager

REVISION HISTORY

Revision#	Revision Reason	Date
1.	First publish for the public version of the ST	17.12.2014

CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 ST INTRODUCTION

1.1 ST REFERENCE

Title: Security Target Lite of AKİS v2.2.8I

Document Version: 01

CC Version: 3.1 (Revision 4)

Assurance Level: EAL4 + AVA_VAN.5 and ALC_DVS.2

1.2 TOE REFERENCE

The current Security Target refers to the product AKİS v2.2.8I

1.3 TOE OVERVIEW

1.3.1 TOE TYPE

AKİS v2.2.8I contact based smartcard is a composite product consisting of embedded operating system and the security IC. The TOE consists of

- AKİS v2.2.8Iembedded operating system,
- IC dedicated software (test and support software including libraries),
- security IC,
- guidance documentation,
- activation data.

1.3.2 MAJORSECURITY PROPERTIES OF THE TOE

The TOE provides the following services to the application:

- Protection against modification, probing, environmental stress and emanation attacks mainly by platform specification and embedded operating system support as detailed in Section 8.
- Access control to services and data by using role attribute, PIN-knowledge attribute, activation agent authentication status, personalization agent authentication status, initialization agent authentication status and device authentication status.
- The following identification and authentication services:

- activation agent identification& authentication by asymmetric cryptographic verification,
- initialization and personalization agent identification& authentication by symmetric decryption,
- terminal and chip identification & authentication by certificate authentication,
- role identification & authentication by certificate authentication,
- user identification & authentication by PIN verification.

- The following cryptographic services:[1]
    - SHA-256 Operation,
    - AES Operation2,
    - CMAC Operation,
    - TDES Operation3,
    - signature generation PKCS#1 v1.5,
    - signature generation PKCS#1 v2.1,
    - signature generation ISO/IEC 9796-2 Scheme 1,
    - signature verification ISO/IEC 9796-2 Scheme 14,
    - asymmetric decryption PKCS#1 v1.5,
    - asymmetric decryption PKCS#1 v2.1,
    - asymmetric encryption/decryption RAW RSA5,
    - random number generation.
- Security management, for services and data by supporting activation agent, initialization agent and personalization agent roles, and any other roles defined by the application.
- Secure messaging services between TOE and the terminal.

1TOE also has capabilityfor SHA-1 operation. But it is not in thescope of evaluationbecause of securityconsideration.
2No interface for AES and CMAC operation is present. The services start during secure messaging automatically.
3No interface for TDES operation is present. TDES decryption operation is provided during initialization and personalization authentication automatically.
4No interface for ISO/IEC 9796-2 Scheme 1 signature generation and verification is present. The services start during secure messaging automatically.
5No interface for RAW RSA encryption/decryption is present. The service starts during secure messaging automatically.

1.3.3 THE USAGE OF THE TOE

The TOE is designed and developed to be as a platform for smart card applications. It supports the life cycle requirements of the smart card applications and provides security services to the smart card applications.

AKİSv2.2.8Isupports two different configurations to the application owner:

- chip configuration ,
- SAM configuration.

Chip configuration is developed to act as user card application like eIDs. The SAM configuration is developed to act on behalf of the terminal as a secure access module.

TOE has security features as detailed in Section 1.3.2, for both configurations. But, there is a slight difference between two configurations in their secure messaging properties.

In chip configuration, two secure messaging types are performed.

The first one is mutual authentication between card (chip) and the terminal by certificate exchange. In this method, both the terminal and the card possess a public key certificate and the corresponding private key. They share their trusted public keys with each other by certificate exchange procedure. Next, they agree on secure messaging keys by key agreement procedure. Finally secure messaging starts. This secure messaging starts in each mutual authentication automatically.

In the second method, a random data is generated by the terminal and sent to TOE confidentially. Next, using this random data, card and the terminal agree on the secure messaging keys by key agreement procedure. Finally, TOE starts secure messaging. Public key cryptography is used in each step of the key agreement process to ensure confidentiality. No certificate is needed in this method.

In SAM configuration, only the second method is performed.

The other difference between the two configurations is in the terminal authentication method. Chip configuration provides terminal authentication by internal and external authentication with certificate exchange. But in SAM configuration, it is provided by PIN authentication. By this way, “authenticated terminal" means PIN authenticated terminal for SAM configuration.

1.4 REQUIRED NON-TOE HW/ SW/ FIRMWARE AVAILABLE TO THE TOE

None.

1.5 TOE DESCRIPTION

1.5.1 LOGICAL VIEW

The logical view of the TOE is given in Figure 1. Logicaly, TOE consists of the communication subsystem, command subsystem, security subsystem, memory and file

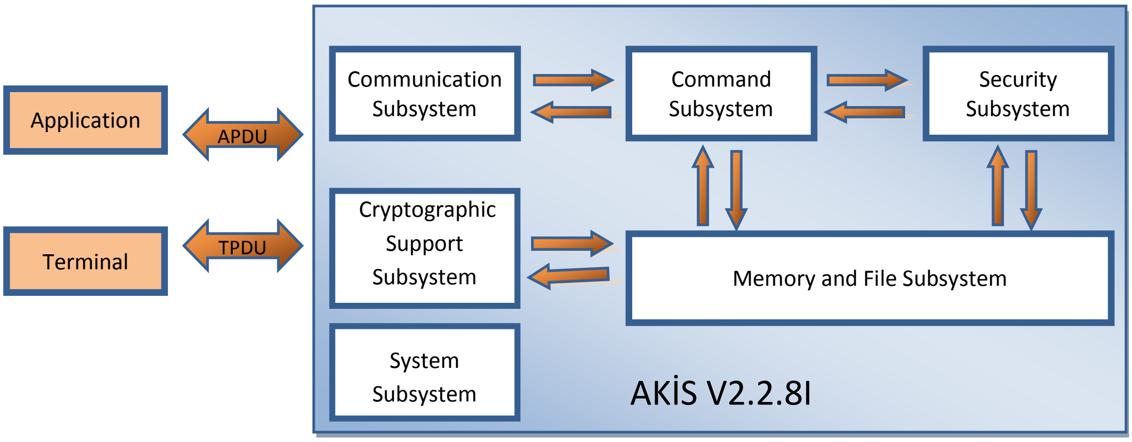


Figure 1. AKİS v2.2.8I Logical View

Communication Subsystem:

Communication subsystem manages the communication between the AKİS v2.2.8Iand the external world. Two layered communication takes place between the outer world and the AKİS v2.2.8I, for the transmission purposes T=1 protocol is implemented, for the application purposes APDU packets are used[8].

Command Subsystem:

Command subsystem processes the commands received from communication subsystem. It performs the commands via help of the Security Subsystem, Memory and File System Subsystem.

Cryptographic Support Subsystem:

All cryptographic functions like encryption, decryption, signature generation, signature verification, random number generation, hash calculation are performed within this subsystem.

Security Subsystem:

Access control conditions and lifecycle management operations are performed within this subsystem. Whenever a security control is to be done via command subsystem, it asks to the security subsystem if the action is allowed or not.

Memory and File System:

Memory and file system manages the non-volatile memory of the security IC. Memory and file system gives services to both of the command subsystem and the security subsystem.

System Subsystem:

System Subsystem includes the functions related to the whole system such as security controls of the system.

1.5.2 PHYSICAL VIEW

Physical view of the TOE is given in the platform information.

1.5.3 INTERFACES

For the electrical I/O:

- ISO 1177 - Information Processing Character Structure For Start/Stop And Synchronous Character Oriented Transmission [7] .

For the transmission:

- ISO 7816-3 Information Technology – Identification Cards – Integrated Circuits with Contacts Part 3: Electronic Signals and Transmission Protocols - T=1 Protocol[8].

For the application:

- ISO 7816-4 Information Technology – Identification Cards – Integrated Circuits with Contacts Part 4: Organization, security and commands for interchange[9].
- ISO 7816-8 Information Technology – Identification Cards – Integrated Circuits with Contacts Part 8: Commands for security operations [9].
- ISO 7816-9 Information Technology – Identification Cards – Integrated Circuits with Contacts Part 9: Commands for card management [11].

1.5.4 LIFE CYCLE

AKİS v2.2.28I is a composite product of Security IC and embedded operating system. Being a smart card application, TOE has a similar life cycle as defined IC PP[1].
There are slight differences for composite TOE. The first one, delivery of composite TOE is performed after phase 5. Also, additional sub phases are defined for composite TOE.
A brief overview is given below for common phases which are detailed in IC PP[1]. Although TOE delivery refers to "after Phase-5", due to configuration needs after TOE delivery, Phase-6 is divided into sub phases that are described in section 1.5.4.1.

Life Cycle Phases:

Phase-1:

- Security IC embedded software, or, embedded operating system, development.

Phase-2:

- IC development:
  - IC design,
  - IC dedicated software development.

Phase-3:

- IC manufacturing:
  - integration and photo mask fabrication,
  - IC production,
  - IC testing.

Phase-4:

- IC Packaging.
- Security IC packaging (and testing).

Phase-5:

- Composite product integration.
- Loading security IC embedded software.

Phase-6:

- Personalization:
  - the composite product personalization and testing stage where the user data is isolated into the security IC's memory.

Phase-7:

- Operational phase:
  - the composite product usage by its issuers and consumers which may include loading and other management of applications.

1.5.4.1 SUB PHASES OF PHASE 6 AND ADDITIONAL PHASE DEFINED FOR EMBEDDED OPERATING SYSTEM

Phase-6 is separated into three following subphases by embedded operating system:

- activation subphase,
- initialization subphase,
- personalization subphase,

Additionally, “death phase” is added.

Activation Subphase:

TOE, AKİS v2.2.8I, is activated in this phase. Initialization key and personalization key are also loaded in this phase. TOE accepts only activation command and some commands that provide very limited information about TOE in this phase. The phase is ended by activation operation. It is managed by activation agent. A 2048 bit cryptogram is sent to TOE by “exchange challenge "command. If the signature of sent cryptogram is verified successfully, activation is completed and composite TOE (card) becomes ready for initialization.

Initialization Subphase:

This phase starts by successful authentication of initialization key. Another successful authentication is needed to complete this phase. File architecture is created by initialization agent. Application data also might be written and access rules might be defined in this phase. Listed commands in Table1can be used by initialization agent. Initialization agent can perform any operation by using these commands. Application specific restrictions cannot be implemented in initialization subphase.
Initialization operations must be performed in a secure environment.

Table1. Commands used in the initialization and personalization phases

#	Commands
1.	KART TEST
2.	EXCHANGE CHALLENGE
3.	INITIALIZATION[6]
4.	PERSONALIZATION[7]

6Applicapleonly in theinitializationphase
7Applicapleonly in thepersonalizationphase

5.	CHANGE KEY
6.	FORMAT
7.	ERASE BINARY
8.	DIR
9.	DELETE SDO
10.	GET DATA
11.	PUT DATA
12.	GET RESPONSE
13.	GET CHALLENGE
14.	SELECT FILE
15.	CREATE FILE
16.	DELETE FILE
17.	UPDATE BINARY
18.	READ BINARY
19.	APPEND RECORD
20.	UPDATE RECORD
21.	READ RECORD
22.	GENERATE ASYMMETRIC KEY PAIR
23.	TERMINATE CARD USAGE

Personalization Subphase:

This phase starts by successful authentication of personalization key. Another successful authentication is needed to complete this phase. Personal information data are written and access rules are defined in this phase. Listed commands in Table1can be used by personalization agent. Personalization agent can perform any operation by using these commands. Application specific restrictions cannot be implemented in personalization subphase.

Personalization operations must be performed in a secure environment.

Death Phase:

Death phase is defined by embedded operating system. TOE becomes out of order and can't be used as a legitimate one. TOE enters this phase because of unsuccessful authentication attempts during activation, initialization and personalization. In addition, some critical integrity errors in operational stage cause death phase. In this phase, TOE doesn’t accept any command, but the ones that provide limited information about TOE.

2 PLATFORM INFORMATION

2.1 PLATFORM IDENTIFICATION

Platform:

- Infineon Technologies, SLE78CFX2400P

Platform ST:

- Security Target Including Optional Software Libraries RSA – EC – SHA2 – Toolbox; Common Criteria CCv3.1 EAL6 Augmented (EAL6+, AVA_VAN.5, ALC_DVS.2) Resistance to Attackers with High Attack Potential Version 1.4, 2013-08-26, [0782b.pdf can be found on commoncriteriaportal.org]

Platform PP Conformance:

- Security IC Platform Protection Profile, Version 1.0, 15 June 2007, BSI-CC-PP-0035-2007

Platform Assurance Level:

- EAL6 + ALC_FLR.1

Platform Certification Report:

- BSI-DSZ-CC-0782-2012, 11.09.2012 [0782a.pdf can be on commoncriteriaportal.org]

Common Criteria Version:

- CC v3.1 Revision 3

Platform Features:

- 24-bit linear addressing,
- up to 16 MByte of addressable memory,
- register based architecture,
- 2-stage instruction pipeline,
- extensive set of powerful instructions, including 16 and 32-bit arithmetic and logic instructions,
- CACHE with single-cycle access searching,

- 16-bit ALU.

Configuration of AKİS v2.2.8IPlatform:

- contact based communication ISO7816-3,
- flash loader unlocked: EOS is loaded to the IC by Infineon but flash loader functionality is still delivered with the IC to be locked by card issuer,
- RAM: 8K,
- total flash memory: 300KB,
- FLASH memory dedicated for EOS: 128 KB,
- FLASH memory dedicated for user data: 108KB,
- with RSA 2048, RSA 4096 and SHA-2 libraries,
- without EC and toolbox libraries.

Configuration of M7892:

- software libraries RSA 2048 v1.02.013, RSA 4096 v1.02.013, SHA-2 v1.01,
- guidance documentation;
  - M7982 Controller Family for Security Applications,
  - SLX 70 Family Production and Personalization, User's Manual,
  - SLE 70 Family Programmer's Reference User's Manual,
  - SLE 70 Asymmetric Crypto Library Crypto@2304T, RSA / ECC / Toolbox, User's Interface,
  - Chip card and Security ICs, SLx70 Family Secure Hash Algorithm SHA-2,
  - Crypto@2304 T User Manual,
  - M7892 Controller Security Guidelines User Manual,
  - M7892 Controller Family for Security Applications, Errata Sheet.

2.2 PLATFORM DESCRIPTION

2.2.1 PLATFORM HARDWARE

The TOE provides a real 16-bit CPU-architecture and is compatible to the Intel 80251 architecture. The block diagram of the platform is given in Figure. The major components are stated below.

Core:

- two CPUs,

- MMU (Memory Management Unit),
- MED (Memory Encryption Decryption),
- EDU (Error Detection Unit),
- CACHE with post failure detection.

Memory:

- ROM (not user accessible),
- Infineon SOLID FLASH Memory [EEPROM],
- RAM.

Cryptographic Co-Processors:

- SCP (Symmetric co-processor) [AES, TDES – two keys and three keys],
- Crypto2304T [RSA-2048 bit, RSA-4096 bit with CRT, EC].

Bus systems:

- a memory bus,
- a peripheral bus for high speed communication with peripherals.

Peripherals:

- true random NUMBER GENERATOR (TRNG),
- deterministic random number generator (DRNG),
- timers,
- watchdog,
- universal asynchronous receiver/transmitter (UART),
- checksum module (CRC).

Control:

- dynamic power management,
- internal clock oscillator,
- interrupt and peripheral event channel controller (ITP and PEC),
- interface management module (IMM).

Security Modules:

- operation within the specified range (frequency sensor),
- alarms,
- user mode security life control (UmSLC),

- voltage regulator.

Infineon®SOLID FLASH:

The flexible memory concept consists of ROM and flash memory as part of the non volatile memory (NVM), respectively Infineon SOLID FLASH. For the Infineon SOLID FLASH memory the unified channel programming (UCP) memory technology is used.

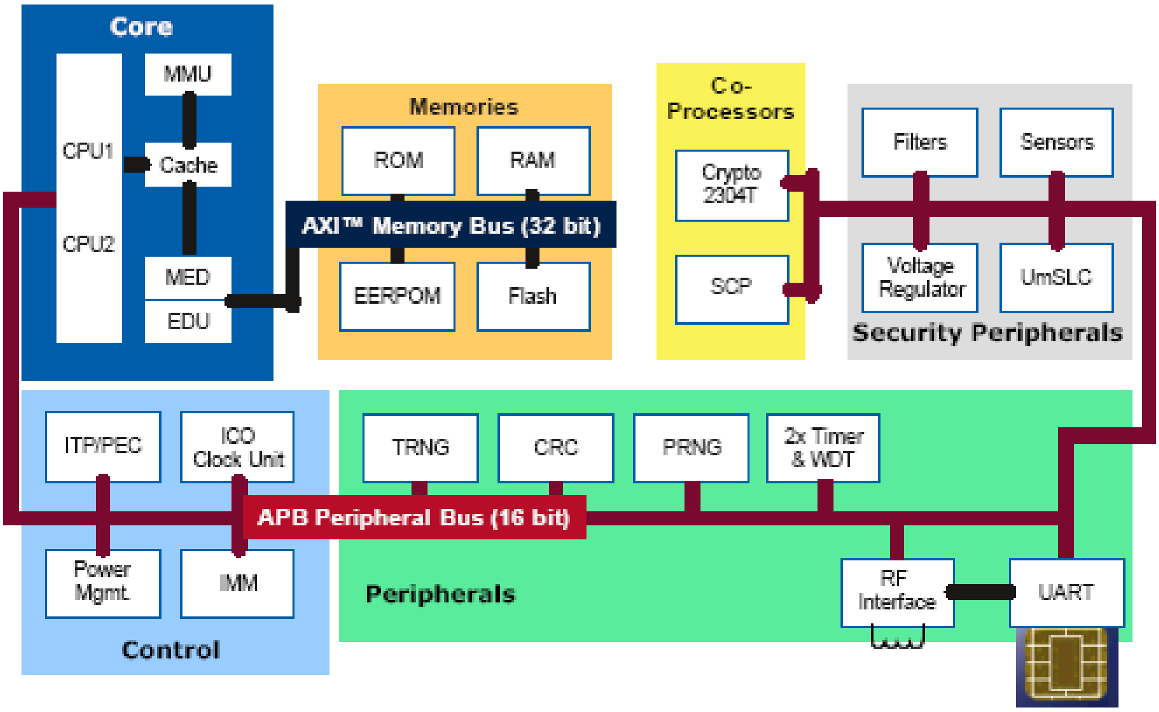


Figure 2. Platform Hardware

2.2.2 PLATFORM FIRMWARE

The firmware parts are RMS Library, the SAM, the STS and the flash loader.

RMS Library:

The RMS library provides some functionality via an API to the Smartcard Embedded Software such as Infineon® SOLID FLASH™ service routines.

STS (Self Test Software):

The STS is implemented in a separated TEST-ROM being part of the platform. The STS firmware is used for test purposes during start-up.

SAM (Service Algorithm Module):

Provides functionality for the tearing save write into the Infineon SOLID FLASH.

Flash Loader:

Flash loader allows downloading the embedded operating system to the Infineon SOLID FLASH during the manufacturing process. Infineon AG provides following possibilities for the card issuer to download their software to the IC:

- Infineon downloads the user software during the IC production phase.
- Infineon may supply the IC without the EOS, in this case EOS is not delivered to Infineon.
- Infineon downloads the parts of the EOS and Card Issuer completes the rest

AKİS v2.2.8Iis securely delivered to the Infineon. Platform certification covers the delivery process of EOS to the Infineon.

Card Issuer receives the TOE (platform + TOE) and the Activation Card with the Flash Loader on, but locked. The EOS can reactivate the Flash Loader and can flash the card with new EOS, with the activation card before initialization phase. But once card is activated and it is in initialization or in the later phases, flash loader functionality is forever locked.

2.2.3 PLATFORM SOFTWARE

Platform software consists of RSA, SHA-2 and base libraries and they are delivered as object code. They are also delivered securely to the AKİS Project Group.

RSA Library:

The RSA library is used to provide a high level interface to RSA cryptography implemented on the hardware component Crypto2304T.

RSA library has protection against SPA, DPA, DFA attacks.

SHA-2 Library:

The SHA-2 library provides the calculation of a hash value of given input. SHA-2 is intended to be used for signature generation, verification and generic data integrity checks.

BASE Library:

The base library provides the low level interface to the asymmetric cryptographic coprocessor and has no user available interface. The base library does not provide any security functionality, implements no security mechanism, and does not provide additional specific security functionality.

2.2.4 PLATFORM INTERFACES

External Interfaces:

- The physical interface of the TOE to the external environment, that is the entire surface of the IC,
- The electrical interface of the TOE to the external environment that is constituted by the pads of the chip, RES, I/O, CLK lines and supply lines VCC and GND,
- The data-oriented I/O interface to the TOE that is formed by the I/O pad,
- ISO 7816-3 Cards with contacts, electrical interface and transmission protocols.

EOS Interfaces:

- Special function registers [Interface to the firmware] which are used for general configuration purposes and chip configuration,
- The interface of the platform to the EOS which is constituted on one hand by the RMS routine calls and on the other by the instruction set of the platform,
- The interface of the platform to test routines, formed by STS test routine call,
- The interface to the RSA and SHA-2 that are defined from RSA and SHA-2 library interfaces.

2.3 PLATFORM SECURITY SPECIFICATION

2.3.1 PLATFORM SECURITY SERVICES

2.3.1.1 RANDOM NUMBER GENERATOR

Physical random number generator:

Quality metric is AIS31 PTG.2**(**Functionality Classes and Evaluation Methodology for Physical Random Number Generators – Version 2.1, 2011-12-02, Bundesamt für Sicherheit in der Informationstechnik respectively “A proposal for: Functionality classes for random number generators”, Version 2.0, 2011-09-18, Wolfgang Killmann, T-Systems GEI GmbH, Werner Schindler, Bundesamt für Sicherheit in der Informationstechnik)

Deterministic random number generator:

Out of the scope for certification.

2.3.1.2 RSA FUNCTIONALITY

RSA library:

The RSA library is used to provide a high level interface to RSA cryptography implemented on the hardware component Crypto2304T.

RSA library has protection against SPA, DPA, DFA attacks.

RSA Routines:

- RsaKeyGen (RSA key pair generation),
- RsaVerify (RSA signature verification),
- RsaSign (RSA signature generation),
- RsaModulus (RSA modulus recalculation).

2.3.1.3 DES FUNCTIONALITY

The TOE supports the encryption and decryption in accordance with the specified algorithm TDES with cryptographic key sizes of 112 bits or 168 bits.

2.3.1.4 SHA LIBRARY

The SHA-library provides the calculation of a hash value of given input. SHA-2 is intended to be used for signature generation, verification and generic data integrity checks.

2.3.2 PLATFORM SECURITY FEATURES

Integrity Guard Concept:

This new product family features a progressive security philosophy focusing on the data integrity. This new concept is based on three main principles:

- full error detection,
- full encryption,
- intelligent active shielding.

2.3.2.1 FULL ON-CHIP ENCRYPTION

The TOE provides full on-chip encryption covering the complete core, busses, memories and cryptographic co-processors leaving no plaintext on the chip.

Encrypted signals have no use for an attacker neither for manipulation nor probing (probing and emission monitoring)

2.3.2.2 ERROR DETECTION

Operation errors:

- double CPU.

Memory errors:

- SOLID FLASH EDC and ECC) (one bit and two bits respectively),
- RAM EDC,
- Cache.

2.3.2.3 INTELLIGENT ACTIVE SHIELDING

An intelligent shielding finishes the upper layers above security critical signals and wires, finally providing the so called “I^2 Shield”.

3 CC CONFORMANCE CLAIM

This security target claims conformance to

- Common Criteria for Information Technology Security Evaluation, Part 1:Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, September 2012.
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1 Revision 4, September 2012.
- Common Criteria for Information Technology Security Evaluation, Part 3:Security Assurance Components; CCMB-2012-09-003, Version 3.1 Revision 4, September 2012.

As conformance claim is as follows:

- part 2 extended,
- part 3 conformant.

3.1 PP CLAIM

This ST does not claim conformance to any PP.

3.2 PACKAGE CLAIM

The current ST is conformant to the following security requirements package: assurance package EAL4 augmented with AVA_VAN.5 and ALC_DVS.2 as defined in the CC, part 3.

4 SECURITY PROBLEM DEFINITION

The TOE is the embedded operating system (EOS) with the security IC. Hence application is not part of the TOE; it does not have user data and TSF data belonging to the application. But it provides containers for storing files, keys and PINs, and functionality to manage these entities to the application.

4.1 ASSETS

AKİS v2.2.8Iis the composite product consisting of the embedded operating system and the security IC. Since the security target of the security IC [2]claims strict conformance to the PP[1] the assets defined in section 3.1 of the protection profile apply to this Security Target.
Additional assets are defined below.

4.1.1 PRIMARY ASSETS

Primary assets represent user data in the sense of the CC. They are given in Table2.

Table2. Primary Assets of the TOE

Asset Name	Definition	Protection Need
Files (user data stored):	All files that is provided to the application to store data.	Confidentiality Integrity
User data transferred:	All data transferred between TOE and external entities.	Confidentiality Integrity

4.1.2 SECONDARY ASSETS

Secondary assets include TSF and TSF data of the TOE. They are given in Table3.

Table3. Secondary Assets of the TOE

Asset Name	Definition	Protection Need
PINs	TOE should provide PIN verification mechanism to the application but it does not have natively PINs. As part of the PIN verification mechanism, PINs are stored in the	Confidentiality Integrity

Asset Name	Definition	Protection Need
	containers that is provided by TOE and transferred by the TSF mechanisms. Therefore, confidentiality and integrity of the PINS are satisfied by both TOE and the application.	
Keys	Applications might need keys for their security functionality. TOE should provide containers to the application to store and manage them securely. Namely, confidentiality and the integrity of the keys are satisfied by TOE and the application.	Confidentiality Integrity
Access reference rules file	This is the file to be created by the application that arranges access control to the assets and to the TSF Interface. The integrity need of this file is different than the standard file (user data stored). Thus this is regarded as a different asset.	Confidentiality Integrity
Activation data	These are the data used in the activation agent authentication.	Confidentiality Integrity
Initialization and personalization data	These are the data used in authentication of initialization and personalization agents.	Confidentiality Integrity
SAM or chip PubK	SAM or Chip Public Keys (PubK) are used to verify the root CA certificates	Integrity
SAM or chip PrK	The SAM or Chip Private Keys (PrK) are used to prove the authenticity of the TOE.	Confidentiality Integrity
SAM or chip CA certificate	Root CA Certificate is the root certificate to be used to validate certificate chains.	Integrity
SAM or chip certificate	The SAM or Chip Certificates are used to prove the authenticity of SAM or Chip Public Key. They are signed by CA certificate.	Integrity
IC identification data	It is the data to uniquely identify the TOE.	Integrity

Asset Name	Definition	Protection Need
EOS code	TSF code is the EOS code that is in operation and in storage. For the proper function of TOE, integrity, confidentiality of the TSF Code must be protected. Also its correct operation must be maintained.	Integrity, confidentiality
Security services	The TOE provides security services to the application. Correct operation of the cryptographic operations is essential for the application that the TOE serves for.	Correct Operation
Files (as TSF data)	The TOE provides data containers to the application, these data containers can be used as TSF data by the application. So, TOE might include files as TSF Data in addition to other TSF data.	Confidentiality, integrity
Genuineness of TOE	Genuineness of the SC shows that it is neither copied nor cloned.	Availability

4.2 SUBJECTS AND EXTERNAL ENTITIES

This ST considers the external entities and subjects given in Table4.

Table4. Subjects and External Entities of the TOE

Entity	Subject	Definition
Activation agent	+	Activation agent is the entity who activates the card and writes the configuration data, initialization and personalization data to the TOE.
Initialization agent	+	Initialization agent is the entity who initializes the TOE.
Personalization agent	+	Personalization agent is the entity who personalizes the TOE.
Terminal	+	The entity that card communicates with.
Application defined role	+	Any agent defined by application developer. Application developer may be thought as Initialization and personalization agent.

Entity	Subject	Definition
Card holder	-	Card holder is whom the card is issued for. It is the owner of the Chip Card.
IC developer	-	The entity that designs the IC and develops the IC Dedicated Software.
EOS developer	-	The entity that designs and develops the EOS.
Application developer	-	The entity that designs and develops the application.
IC manufacturer	-	The entity who performs following activities: • production of the Integrated circuit, • testing the Integrated circuit, • EOS is loaded to the NVM of the IC. Flash loader mechanism is not disabled by the IC manufacturer, • writes the configuration data and IC serial number.
Card Issuer	-	The entity holding the authority to issue the cards. Card issuer employs the application developer to develop the application that fulfils its needs. After the application is developed and the TOE is received, card issuer may separate its authority to the following roles: activation agent, initialization agent and personalization agent and delegate these roles to other entities or perform them by itself.
Certificate authorities (Root CA, chip CA, terminal CA, role CA)	-	Certificate authorities are the entities which issue the certificates. Chip CA and terminal CA (valid for chip configuration) certificates are signed by the root CA.
Attacker	-	A threat agent trying to violate the system security policy. Attacker may have at most high attack potential.

4.3 THREATS

4.3.1 HARDWARE RELATED THREATS

Threats related to hardware are given in this section.

T.Physical_Probing

An attacker may perform physical probing of the TOE in order to disclose user data or other critical information, to disclose/reconstruct the TOE's embedded operating system about the operation of the TOE. Physical probing requires direct interaction with the TOE's internals. Techniques commonly employed in IC failure analysis and IC reverse engineering efforts may be used after determination of software design including treatment of user data, hardware security mechanisms and layout characteristics need to be identified. This pertains to "measurements" using galvanic contacts or any type of charge interaction whereas manipulations are considered under the threat "Physical Manipulation (T.Physical_Manipulation)". "Inherent Information Leakage (T.Lekage_Inherent)" and "Forced Information Leakage (T.Leakage_Forced)" may use physical probing with complex signal processing.

T.Physical_Manipulation

An attacker may physically modify the TOE in order to modify user data/TSF Data, or TOE's hardware and embedded operating system, modify or deactivate security services of the TOE, or modify security mechanisms of the TOE to enable attacks disclosing or manipulating the user data/TSF Data
The modification may be achieved through techniques commonly employed in IC failure analysis and IC reverse engineering efforts. The modification may result in the deactivation of a security feature. Before that hardware security mechanisms and layout characteristics need to be identified. Determination of software design including treatment of user data may also be a pre-requisite. Changes of circuitry or data can be permanent or temporary. In contrast to malfunctions (refer to T.Env_Malfunction) the attacker requires gathering significant knowledge about the TOE's internal construction.

T.Lekage_Inherent

An attacker may exploit information that is leaked from the TOE during usage of smart card to disclose confidential user data or/and TSF-data. Leakage may occur through emanations, variations in power consumption, I/O characteristics, clock frequency, or by changes in processing time requirements. This leakage may be interpreted as a covert channel transmission but is more closely related to measurement of operating parameters, which may be derived either from contact or contactless interface measurements and can then be related to the specific operation being performed. Some Examples are Differential Power Analysis (DPA) and fault injection (Differential Fault Analysis).

T.Leakage_Forced

An attacker may exploit information leaking from the TOE during its usage in order to disclose confidential User/TSF Data even if the information leakage is not inherent but caused by the attacker.

This threat pertains to attacks where methods described in “Malfunction due to Environmental Stress” (refer to T.Env_Malfunction) is used to cause leakage from signals which normally do not contain significant information about secret

T.Env_Malfunction

An attacker may cause a malfunction of TSF or TOE’s hardware and embedded operating system by applying environmental stress in order to modify security services of the TOE, or TOE’s hardware and embedded operating system or affect security mechanisms of the TOE to enable attacks disclosing or manipulating the user data or TSF Data. The modification of security services of the TOE may affect the quality of random numbers provided by the random number generator.

T.Abuse_Function

An attacker may use functions of the TOE which may not be used after TOE Delivery in order to (i) disclose or manipulate user data in the TOE, (ii) manipulate (explore, bypass, deactivate or change) security services of the TOE (iii) enable an attack disclosing or manipulating the user data or TSF Data.

T.RND

An attacker may predict or obtain information about random numbers generated by the TOE security service for instance because of a lack of entropy of the random numbers provided.

An attacker may gather information about the random numbers produced by the TOE security service. Because unpredictability is the main property of random numbers this may be a problem in case they are used to generate cryptographic keys. Here the attacker is expected to take advantage of statistical properties of the random numbers generated by the TOE. Malfunctions or premature ageing are also considered which may assist in getting information about random numbers.

4.3.2 ADDITIONAL THREAT DUE TO COMPOSITE TOE SPECIFIC FUNCTIONALITY

Terminal and communication related threats are given in this section.

T. Eavesdropping

An attacker may monitor the communication between the TOE and the terminal to get unauthorized access to the user data and/or TSF Data.

T.Session_Hijacking

An attacker may wait until the identification and authentication process is completed and session is established between the TOE and the terminal. After the session is established, attacker may take out the TOE or the terminal from the communication channel and takes over. That way attacker bypasses the identification and authentication process and accesses to services illegitimately.

T.Man_in_The_Middle

An attacker may alter the communication between the TOE and the terminal. An attacker listens and alters the connection between the TOE and the terminal in order to access the services that he or she is unauthorized to access.

T.Skimming

The terminal which obtains smart card's interactions with the world by controlling all I/O's can observe user identification data, so this terminal must be trusted not to capture the user's identification data. Concerning a variety of fake-terminal attacks become possible, in these cases the user must be able to differentiate between "real devices" that are manufactured by a trusted party and between "fake devices" that are manufactured by the attackers. The user cannot identify that the terminal has hidden features, for example the message they sign was not altered by a malicious terminal. The security has nothing to do with the smart card/ terminal exchange; it is the back-end processing system that monitors the card.

Card Cloning and Forgery Related Threats

T.Counterfeit

An attacker produces an unauthorized copy or reproduction of a genuine TOE to be used as part of a counterfeit operation. He or she may generate a new data set or extract completely or partially the data from a genuine TOE and copy them on another functionally appropriate chip to imitate this genuine TOE. This violates the genuineness of the TOE being used either for authentication of a Card presenter as the Card holder.

T.Unauthorised_Access

An attacker may access to data that he or she is not authorized to.

T.Unauthorised_Management

An attacker may illegitimately use the security management services of the TOE.

4.4 ORGANISATIONAL SECURITY POLICIES

Organizational security policies of the composite TOE is given in Table5.

Table5. Composite TOE Policies

#	Policy Name	Definition
1.	P.Identification_and_Authentication	The TOE should support • chip authentication, • terminal authentication, • PIN verification, • role holder authentication and any combination of this.
2.	P.PKI	There will be terminal authentication CA, chip authentication CA, Role CA all of which certificates are signed by Root CA. terminal certificates, chip certificates and role certificates will be signed by according CA.
3.	P.Access_Control	Role attribute, PIN knowledge attribute, device authentication attribute of the user will be used as a security attribute to determine the access control behavior and security management privileges during operational phase.
4.	P.PreOperational_Security_Management	The TOE should support • activation agent, • initialization agent, • personalization agent functions and roles
5.	P.Operational_Security_Management	The TOE should support • any management function and role defined by the application.

6.	P.Cryptographic_Operations	The TOE should support following cryptographic functions:
		• RSA key pair generation,
		• hash calculation ,
		• eSign operations;
		  ◦ PKCS #1 v2.1,
		  ◦ PKCS #1 v1.5,
		  ◦ ISO/IEC 9796-2 Scheme 1,
		• asymmetric decryption;
		  ◦ PKCS #1 v2.1 OAEP,
		  ◦ PKCS #1 v1.5,
		  ◦ Raw RSA,
		• asymmetric encryption;
		  ◦ Raw RSA,
		• TDES calculation,
		• AES operation,
		• CMAC operation.

4.5 ASSUMPTIONS

Assumptions for the operational environment of the composite TOE is given in Table6.

Table6. Composite TOE Assumptions

#	Assumption Name	Definition
1.	A.Secure_Application	Application will correctly define the access rules of the application data.
2.	A.Key_and_Certificate_Security	All keys and certificates should be produced, stored and used securely outside of TOE.
3.	A.PIN_Handling	PINS belonging to the application should be handled securely by PIN owner.
4.	A.Personnel_Security	Personnel who hold privileges over the TOE should act responsively and according to the application requirements.

#	Assumption Name	Definition
5.	A.Trusted_Parties	It is assumed that the authenticated parties that the TOE communicates act responsively.
6.	A.Pre-Operational_Environment	It is assumed that the Physical environments of initialization and personalization phases are secure.

5 SECURITY OBJECTIVES

5.1 SECURITY OBJECTIVES FOR THE TOE

The TOE is the composite product consisting of embedded operating system and the security IC. The platform (security IC) and the embedded operating system have different interfaces to the external world. The platform has the physical and electrical interfaces and the embedded operating system has the logical interfaces. Therefore the attacks done through the physical and electrical interfaces are mostly countered by the platform and the attacks performed through logical interfaces are countered by the embedded operating system.

5.1.1 PLATFORM OBJECTIVES

Platform objectives are:

- OT.Physical_Probing,
- OT.Physical_Manipulation,
- OT.Leakage_Inherent,
- OT.Leakage_Forced,
- OT.Env_Malfunction,
- OT.Abuse_Function,
- OT.RND.

OT.Physical_Probing

The TOE must provide protection against disclosure of user data and TSF Data. This includes protection against

- measuring through galvanic contacts which is direct physical probing on the chips surface except on pads being bonded (using standard tools for measuring voltage and current) or
- measuring not using galvanic contacts but other types of physical interaction between charges (using tools used in solid-state physics research and IC failure analysis).

With a prior reverse engineering to understand the design and its properties and functions. The TOE must be designed and fabricated so that it requires a high combination of complex equipment, knowledge, skill, and time to be able to derive detailed design information or other information which could be used to compromise security through such a physical attack.

OT.Physical_Manipulation

The TOE must provide protection against manipulation of the TOE (including its software and data), user data and TSF data. This includes protection against

- reverse-engineering (understanding the design and its properties and functions),
- manipulation of the hardware and any data,
- controlled manipulation of memory contents (application data).

The TOE must be designed and fabricated so that it requires a high combination of complex equipment, knowledge, skills, and time to be able to derive detailed design information or other information which could be used to compromise security through such a physical attack.

OT. Leakage_Inherent

The TOE must provide protection against disclosure of confidential data stored and/or processed in the security IC

- by measurement and analysis of the shape and amplitude of signals (for example on the power, clock, or I/O lines) and
- by measurement and analysis of the time between events found by measuring signals (for instance on the power, clock, or I/O lines).

This objective pertains to measurements with subsequent complex signal processing whereas OT.Physical_Probing is about direct measurements on elements on the chip surface.

OT. Leakage_Forced

The TOE must be protected against disclosure of confidential data processed in the TOE (using methods as described under OT.Leakage_Inherent) even if the information leakage is not inherent but caused by the attacker.

- by forcing a malfunction (refer to “Protection against Malfunction due to Environmental Stress (OT.Env_Malfunction)” and/or
- by a physical manipulation (refer to “Protection against Physical Manipulation (OT.Phys-Manipulation)”.

If this is the case, signals which normally do not contain significant information about secrets could become an information channel for a leakage attack.

OT.Env_Malfunction

The TOE must ensure its correct operation.

The TOE must indicate or prevent its operation outside the normal operating conditions where reliability and secure operation has not been proven or tested. This is to prevent malfunctions.

Examples of environmental conditions are voltage, clock frequency, temperature, or external energy fields.

Remark: A malfunction of the TOE may also be caused using a direct interaction with elements on the chip surface. This is considered as being a manipulation (refer to the objective OT.Phys-Manipulation) provided that detailed knowledge about the TOE´s internal construction is required and the attack is performed in a controlled manner.

OT.Abuse_Function

The TOE must prevent those functions of the TOE which may not be used after TOE Delivery can be abused in order to

- disclose critical user data and TSF Data,
- manipulate critical user data and TSF Data,
- bypass, deactivate, change or explore security features or security services of the TOE.

Details depend, for instance, on the capabilities of the Test Features provided by the IC Dedicated Test Software which are not specified here.

OT.RND

The TOE will ensure the cryptographic quality of random number generation. For instance random numbers shall not be predictable and shall have sufficient entropy. The TOE will ensure that no information about the produced random numbers is available to an attacker since they might be used for instance to generate cryptographic keys.

Note 1: Some of platform objectives aren't included in this ST. They are either irrelevant for composite TOE or covered by other objectives. Detailed compatibility and coverage situation are defined in Section 9.

5.1.2 EMBEDDED OPERATING SYSTEM OBJECTIVES

Objectives for the embedded operating system are:

- OT.Identification_and_Authentication,
- OT.Access_Control,
- OT.Security_Management,
- OT.Cryptographic_Operations,
- OT.Secure_Communication,
- OT.Storage_Integrity.

OT.Identification_and_Authentication

The TOE must support following authentication mechanisms: activation agent authentication, initialization agent authentication, personalization agent authentication, chip authentication, terminal authentication[8], Role certificate holder authentication and PIN verification.

OT.Access_Control

The TOE must control the access to the user data and security services according to access control rules determined by the application. Role attribute, PIN-knowledge attribute, device authentication status and authentication should be used as security attributes during the decision of access permission.

OT.Security_Management

The TOE must support following roles: activation agent, initialization agent, personalization agent, and any other roles defined by the application.

OT.Cryptographic_Operations

The TOE must perform following cryptographic operations: asymmetric key pair generation, random number generation, hash calculation, eSign operations, symmetric cryptographic operations.

OT.Secure_Communication

The TOE must support secure communication with the terminal. TOE supports encryption, integrity and authenticity protection against attacks during communication between TOE and terminal.

OT. Storage_Integrity

TOE must support storage integrity protection for critical user data and TSF data.

5.2 SECURITY OBJECTIVES FOR OPERATIONAL ENVIRONMENT

Objectives for the operational environment are:

- OE.PKI,
- OE.Secure_Application,
- OE.Key_and_Certificate_Security,
- OE.PIN_Handling,
- OE.Personnel_Security,
- OE.Responsible_Parties,

8Providedby PIN authenticationfor SAM Configuration.

- OE.Pre-Operational_Env_Sec.

OE.PKI

There must be terminal authentication CA, chip authentication CA, Role CA all of which certificates are signed by Root CA. Terminal Certificates, Chip Certificates and Role Certificates must be signed by the corresponding CA.

OE.Secure_Application

Applicationshould correctly define the access rules of the application data. Also application should fulfill the security requirements of EOS as described in [12].

OE.Key_and_Certificate_Security

Key creation and storage outside of the TOE should be handled securely.

OE.PIN_Handling

PIN Creation and usage by Card Holder should be handled securely.

OE.Personnel_Security

The personnel who have privileges (EOS developer, activation agent, initialization agent and personalization agent)should have necessary security clearances and should act responsibly.

OE.Responsible_Parties

The parties that the TOE communicates (sends or receives data; and/or receives or gives services) should act responsively. For example, terminal should protect any data against confidentiality integrity attacks after taking TOE.

OE.Pre-Operational_Env_Sec

Physical environment of initialization and personalization phases should be secure.

5.3 SECURITY OBJECTIVES RATIONALE

The justification related to the threats “Physical Probing (T.Physical_Probing)”, “Physical Manipulation (T.Physical_Manipulation)”, “Inherent Information Leakage (T.Lekage_Inherent)”, “Forced Information Leakage (T.Leakage_Forced)“, “Malfunction due to Environmental Stress (T.Env_Malfunction)”, “Abuse of Functionality (T.Abuse_Function)” and “Deficiency of Random Numbers (T.RND)” is given below.

For all threats, the corresponding objectives in Section5.1.1are stated in a way, which directly corresponds to the description of the threat in Section 4.3.1. It is clear from the description of each objective, that the corresponding threat is removed. More specifically, in every case the ability to use the attack method successfully is countered by the objective.

Removal of T.Physical_Manipulation and T.Env_Malfunction are also supported by additional objectives as detailed below:

T.Physical_Manipulation is mainly removed by OT.Physical_Manipulation. OT.Storage_Integrity also supports correspondent of the threat by detecting integrity anomalies and acting.

T.Env_Malfunction is mainly removed by OT.Env_Malfunction. OT.Storage_Integrity also supports correspondent of the threat by detecting integrity anomalies and acting.

T.Eavesdropping is countered by OT.Secure_Communication.

T.Session_Hijacking is countered by OT.Secure_Communication.

T.Man_in_The_Middle is countered by OT.Secure_Communication.

T.Skimmmingis countered by OT.Identification_and_Authentication and OT.Physical_Manipulation as they provide protection against physical manipulation of authenticity verification key.

T.Counterfitingis countered by OT.Identification_and_Authentication, OT.Physical_Probing, OT.Leakage_Inherent, OT.Leakage_Forced and OT.Abuse_Function. Against the Identification fraud, the TOE gives identification and authentication services via OT.Identification_and_Authentication. Against the attacks to these services, the TOE protects the TSF data related with identification and authentication services. OT.Physical_Probing, OT.Leakage_Inherent, OT.Leakage_Forced, OT.Abuse_Function provides protection against disclosure of secret authentication key.

T.Unauthorised_Access is countered by OT.Access_Control. It handles the unauthorized access to the user data and services.

T.Unauthorised_Managementis countered by OT.Security_Management, which put mechanisms to manage TSF data, and puts the Identification and authentication requirements for the management activities.

P.Identification_and_Authenticationis covered by OT.Identification_and_Authentication covers the support for the chip authentication, terminal authentication[9],role holder authentication, and PIN verification mechanisms which are addressed by P.Identification_and_Authentication.

P.PKI is covered byOE.PKI. Additionally OT.Identification_and_Authentication covers support for the chip authentication, terminal authentication[10] and role holder authentication mechanisms. These authentication mechanisms include the verification of PKI hierarchy dictated by P.PKI.

P.Access_Control is covered by OT.Access_Control.

P.PreOperational_Security_Management is covered by OT.Security_Management.

9Providedby PIN authenticationfor SAM Configuration.
10Providedby PIN authenticationfor SAM Configuration.

P.Operational_Security_Management is covered by OT.Security_Managemen.

P.Cryptographic_Operations is covered by OT.Cryptographic_Operations.

A.Secure_Application is covered by OE.Secure_Application.

A.Key_and_Certificate_Security is covered by OE.Key_and_Certificate_Security.

A.PIN_Handling is covered by OE.PIN_Handling.

A.Personnel_Security is covered by OE.Personnel_Security.

A.Trusted_Parties is covered by OE.Responsible_Parties.

A.Pre-Operational_Environment is covered by OE.Pre-Operational_Environment.

Table7 gives the coverage of the threats, assumptions and OSPs by the objectives.

Table7. Security Objectives versus Assumptions, Threats or OSPs

Threats/OSPs/Assumptions	**Corresponding Objectives**
T.Physical_Probing	OT.Physical_Probing
T.Physical_Manipulation	OT.Physical_Manipulation, OT.Storage_Integrity
T.Lekage_Inherent	OT.Leakage_Inherent
T.Leakage_Forced	OT.Leakage_Forced
T.Env_Malfunction	OT.Env_Malfunction, OT.Storage_Integrity
T.Abuse_Function	OT.Abuse_Function
T.RND	OT.RND
T. Eavesdropping	OT.Secure_Communication,
T.Session_Hijacking	OT.Secure_Communication,
T.Man_in_The_Middle	OT.Secure_Communication,
T.Skimming	OT.Identification_and_Authentication, OT.Physical_Manipulation
T.Counterfiting	OT.Identification_and_Authentication, OT.Physical_Probing OT.Leakage_Inherent OT.Leakage_Forced OT.Abuse_Function
T.Unauthorised_Access	OT.Access_Control
T.Unauthorised_Management	OT.Security_Management
P.Identification_and_Authentication	OT.Identification_and_Authentication
P.PKI	OT.Identification_and_Authentication, OE.PKI

Threats/OSPs/Assumptions	**Corresponding Objectives**
P.Access_Control	OT.Access_Control
P.PreOperational_Security_Management	OT.Security_Management
P.Operational_Security_Management	OT.Security_Management
P.Cryptographic_Operations	OT.Cryptographic_Operations
A.Secure_Application	OE.Secure_Application
A.Key_and_Certificate_Security	OE.Key_and_Certificate_Security
A.PIN_Handling	OE.PIN_Handling
A.Personnel_Security	OE.Personnel_Security
A.Trusted_Parties	OE.Responsible_Parties
A.Pre-Operational_Environment	OE.Pre-Operational_Env_Sec

6 EXTENDED COMPONENTS

The extended components defined and described for the TOE are:

- Family FAU_SAS (Audit Data Storage),
- Family FMT_LIM (Limited capabilities and availability),
- Family FCS_RNG(Generation of Random Numbers),
- Component FPT_TST.2,
- Family FIA_API (Application Proof of Identity),
- Family FPT_EMSEC TOE Emanation.

6.1 DEFINITION OF THE FAMILY FAU_SAS (AUDIT DATA STORAGE)

FAU_SAS family of the Class FAU (Security Audit) is defined in the platform PP document [1] and describes the functional requirements for the storage of audit data. It has a more general approach than FAU_GEN, because it does not necessarily require the data to be generated by the TOE itself and because it does not give specific details of the content of the audit records.

Family behavior

This family defines functional requirements for the storage of audit data.

Component leveling

FAU_SAS.1 Requires the TOE to provide the possibility to store audit data.

Management: FAU_SAS.1

There are no management activities foreseen.

Audit: FAU_SAS.1

There are no actions defined to be auditable.

6.1.1 FAU_SAS.1 AUDIT STORAGE

Hierarchical to: No other components.

FAU_SAS.1.1 The TSF shall provide [assignment: *list of subjects*] with the capability to store [assignment: *list of audit information*] in the [assignment: *type of persistent memory*].

Dependencies: No dependencies.

6.2 DEFINITION OF THE FAMILY FCS_RNG (GENERATION OF RANDOM NUMBERS)

FCS_RNG of the Class FCS (cryptographic support) is defined in platform ST document [1]. This family describes the functional requirements for random number generation used for cryptographic purposes according to Anwendungshinweise und Interpretationenzum Schema (AIS) —Functionality classes and evaluation methodology for physical random number generators, AIS31 [15]. This security functional component is used instead of the functional component FCS_RNG.1 defined in the platform protection profile[1].

Family behavior

This family defines quality requirements for the generation of random numbers which are intended to be used for cryptographic purposes.

Component leveling:

FCS_RNG: Generation of random numbers	1

FCS_RNG.1: Generation of random numbers requires that the random number generator implements defined security capabilities and that the random numbers meet a defined quality metric.

Management: FCS_RNG.1

There are no management activities foreseen.

Audit: FCS_RNG.1

There are no actions defined to be auditable.

6.2.1 FCS_RNG.1 RANDOM NUMBER GENERATION

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RNG.1.1: The TSF shall provide a [selection: physical, non-physical true, deterministic, hybrid] physical, hybrid deterministic] random number generator that implements: [assignment: *list of security capabilities*].

FCS_RNG.1.2: The TSF shall provide random numbers that meet [assignment: *a defined quality metric*].

6.3 DEFINITION OF THE FAMILY FMT_LIM (Limited Capabilities And Availability)

FMT_LIM of the Class FMT (Security Management) is defined as given in the IC PP [1]. This family describes the functional requirements for the test features of the TOE. The new functional requirements were defined in the class FMT because this class addresses the management of functions of the TSF. The examples of the technical mechanism used in the TOE appropriate to address the specific issues of preventing the abuse of functions by limiting the capabilities of the functions and by limiting their availability.

Family behavior

This family defines requirements that limit the capabilities and availability of functions in a combined manner. Note that FDP_ACF restricts the access to functions whereas the component Limited Capability of this family requires the functions themselves to be designed in a specific manner.

Component leveling:

FMT_LIM.1 Limited capabilities requires that the TSF is built to provide only the capabilities (perform action, gather information) necessary for its genuine purpose.

FMT_LIM.2 Limited availability requires that the TSF restrict the use of functions (refer to Limited capabilities (FMT_LIM.1)). This can be achieved, for instance, by removing or by disabling functions in a specific phase of the TOE's life-cycle.

Management: FMT_LIM.1, FMT_LIM.2

There are no management activities foreseen.

Audit: FMT_LIM.1, FMT_LIM.2

There are no actions defined to be auditable.

The TOE Functional Requirement "Limited capabilities (FMT_LIM.1)" is specified as follows.

6.3.1 FMT_LIM.1 LIMITED CAPABILITIES

Hierarchical to: No other components.

FMT_LIM.1.1 The TSF shall be designed and implemented in a manner that limits its capabilities so that in conjunction with "Limited availability (FMT_LIM.2)" the following policy is enforced [assignment: *Limited capability and availability policy*].

Dependencies: FMT_LIM.2 Limited availability.

The TOE Functional Requirement “Limited availability (FMT_LIM.2)” is specified as follows.

6.3.2 FMT_LIM.2 LIMITED AVAILABILITY

Hierarchical to: No other components.

Dependencies: FMT_LIM.1 Limited capabilities.

FMT_LIM.2.1 The TSF shall be designed in a manner that limits its availability so that in conjunction with “Limited capabilities (FMT_LIM.1)” the following policy is enforced [assignment: *Limited capability and availability policy*].

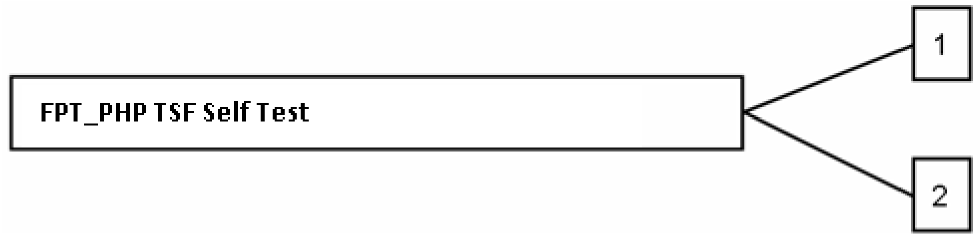
6.4 DEFINITION OF THE FAMILYFPT_TST (TSF Self Test)

FPT_TST Family is defined in Common Criteria Part2 [4]. The functional component FPT_TST.2 is defined as an extended component to this family in the IC ST[2][14].The family definition is updated with the added extended component.

Family Behavior

The Family Behavior is defined in Common criteria Part3 [3] section 15.14 (442, 443).

Component leveling:



FPT_TST.1: The component FPT_TST.1 is defined in [3] section 15.14 (444, 445, 446).

FPT_TST.2: Subset TOE security testing, provides the ability to test the correct operation of particular security functions or mechanisms. These tests may be performed at start-up, periodically, at the request of the authorized user, or when other conditions are met. It also provides the ability to verify the integrity of TSF data and executable code.

This component allows that particular parts of the security mechanisms and functions provided by the TOE can be tested after TOE delivery or are tested automatically and continuously during normal operation transparent for the user. This security functional component is used instead of the functional component FPT_TST.1 from Common Criteria Part 2. For the user it is important to know which security functions or mechanisms can be tested. The functional component FPT_TST.1 does not mandate to explicitly specify the security functions being tested. In addition, FPT_TST.1 requires verifying the integrity of TSF data and stored TSF executable code which might violate the security policy.

Management: FPT_TST.2

The following actions could be considered for the management functions in FMT:

- management of the conditions under which subset TSF self-testing occurs, such as during initial start-up, regular interval or under specified conditions,
- management of the time interval as appropriate.

Audit: FPT_TST.2

There are no auditable events foreseen.

6.4.1 FPT_TST.2 SUBSET TOE TESTING

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TST.2.1: The TSF shall run a suite of self-tests [selection: during initial start-up, periodically, during normal operation, at the request of the authorized user, and/or at the conditions [assignment: *conditions under which self-test should occur*]] to demonstrate the correct operation of [assignment: *functions and/or mechanisms*].

6.5 DEFINITION OF THE FAMILY FIA_API (APPLICATION PROOF OF IDENTITY)

FIA_API of the Class FIA (Identification Authentication) is defined as given in BSI-CC-PP-0056 PP [16].

Family Behavior

This family defines functions provided by the TOE to prove its identity and to be verified by an external entity in the TOE IT environment.

Component leveling:

FIA_API.1 Authentication Proof of Identity:

Management: FIA_API.1

The following actions could be considered for the management functions in FMT: Management of authentication information used to prove the claimed identity.

Audit: FIA_API.1

There are no actions defined to be auditable.

6.5.1 FIA_API.1 AUTHENTICATION PROOF OF IDENTITY

Hierarchical to: No other components.

Dependencies: No dependencies

FIA_API.1.1 The TSF shall provide a [assignment: *authentication mechanism*] to prove the identity of the [assignment: *authorized user or role*].

6.6 DEFINITION OF THE FAMILY FPT_EMSEC (TOE EMANATION)

FPT_EMSEC of the Class FPT (Protection of the TSF) is defined as given in BSI-CC-PP-0056 PP [16].

The TOE shall prevent attacks against TOE and other secret data where the attack is based on external observable physical phenomena of the TOE. This family describes the functional requirements for the limitation of intelligible emanations which are not directly addressed by other functional requirements defined in Common Criteria Part2.

Family behavior

This family defines requirements to mitigate intelligible emanations.

Component Leveling

FPT_EMSEC.1 TOE Emanation has two constituents:

FPT_EMSEC.1.1 Limit of emissions requires to not emit intelligible emissions enabling access to TSF data or user data.

FPT_EMSEC.1.2 Interface emanations requires to not emit interface emanation enabling access to TSF data or user data.

Management: FPT_EMSEC.1

There are no management activities foreseen.

Audit: FPT.EMSEC.1

There are no actions defined to be auditable.

6.6.1 FPT_EMSEC.1 TOE EMANATION

Hierarchical to: No other components

Dependencies: No dependencies

FPT_EMSEC.1.1 The TOE shall not emit [assignment: *types of emissions*] in excess of [assignment: *specified limits*] enabling access to [assignment: *list of types of TSF data*] and [assignment list of types of user data].

FPT_EMSEC.1.2 The TSF shall ensure [assignment: *type of users*] are unable to use the following interface [assignment*: type of connection*] to gain access to [assignment: *list of type of user data*].

7 SECURITY REQUIREMENTS

7.1 OVERVIEW

This part of the ST defines the detailed security requirements that shall be satisfied by the TOE. The statement of TOE security requirements shall define the functional and assurance security requirements that the TOE needs to satisfy in order to meet the security objectives for the TOE. The CC allows several operations to be performed on functional requirements; refinement, selection, assignment, and iteration are defined in Section 8.1 of Common Criteria Part1[3]. Each of these operations is used in this ST.

The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinements of security requirements are denoted in such a way that added words are in **bold text** and removed are ~~crossed out~~.

The **selection** operation is used to select one or more options provided by the CC instating a requirement. Selections having been made are denoted as underlined text.

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments are denoted by *italicized* text.

The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing a slash "/", and the iteration indicator after the component identifier.

7.2 SECURITY FUNCTIONAL REQUIREMENTS

TOE security functional requirements of the composite product are summarized in Table8.

Table8. List of SFRs

CLASS FAU		
1.	FAU_SAS.1	Audit Storage
CLASS FCS		
2.	FCS_CKM.1/SM	Cryptographic Key Generation - Secure Messaging Session Keys
3.	FCS_CKM.1/SM_PER-INI	Cryptographic key generation– Secure Messaging Keys for Pre-Operational Phase
4.	FCS_CKM.1/RSA_KeyPair	Cryptographic key generation- RSA KeyPair Generation

5.	FCS_CKM.2/SM	Cryptographic key distribution – Secure Messaging Keys
6.	FCS_CKM.2/SM_PER-INI	Cryptographic Key Distribution – Secure Messaging Keys For Pre-Operational Phases
7.	FCS_CKM.4	Cryptographic Key Destruction
8.	FCS_COP.1/SHA	Cryptographic Operation-SHA 256 Calculation
9.	FCS_COP.1/AES	Cryptographic Operation-AES Calculation for Secure Messaging
10.	FCS_COP.1/TDES	Cryptographic Operation- Initialization Verification with TDES
11.	FCS_COP.1/CMAC	Cryptographic Operation- CMAC Calculation for Secure Messaging
12.	FCS_COP.1/SIG-GEN_PKCS#1 V1.5	Cryptographic Operation-Signature Generation PKCS#1 v1.5
13.	FCS_COP.1/SIG-GEN_PKCS #1 V2.1	Cryptographic Operation-Signature Generation PKCS#1 v2.1
14.	FCS_COP.1/SIG-GEN_9796	Cryptographic Operation-Signature Generation ISO/IEC 9796-2 Scheme 1
15.	FCS_COP.1/SIG-VER_9796	Cryptographic Operation- Signature Verification ISO/IEC 9796-2 Scheme 1
16.	FCS_COP.1/DEC_PKCS#1 V1.5	Cryptographic Operation-Asymmetric Decryption PKCS#1 v.1.5
17.	FCS_COP.1/DEC_PKCS#1 V2.1 OAEP	Cryptographic Operation-Asymmetric Decryption PKCS#1 v2.1
18.	FCS_COP.1/RSA_RAW	Cryptographic Operation-Asymmetric Encryption/Decryption RAW RSA
19.	FCS_RNG.1	Generation of Random Numbers
CLASS FDP		
20.	FDP_ACC.1/Data	Subset Access Control-Data Access

21.	FDP_ACC.1/FUN	Subset Access Control-Function Access
22.	FDP_ACF.1/Data	Security Attribute Based Access Control-Data Access
23.	FDP_ACF.1/FUN	Security Attribute Based Access Control-Function Access
24.	FDP_UCT.1	Basic Data Exchange Confidentiality
25.	FDP_UIT.1	Data Exchange Integrity
26.	FDP_IFC.1	Subset Information Flow Control
27.	FDP_ITT.1	Basic Internal Transfer Protection
28.	FDP_SDI.1/HW	Stored Data Integrity Monitoring
29.	FDP_SDI.2/HW	Stored Data Integrity Monitoring And Action-Hw Protection
CLASS FIA		
30.	FIA_AFL.1/PIN	Authentication Failure Handling – PIN Verification
31.	FIA_AFL.1/ACT	Authentication Failure Handling – Activation
32.	FIA_AFL.1/PER	Authentication Failure Handling - Initialization
33.	FIA_AFL.1/INI	Authentication Failure Handling - Personalization
34.	FIA_API.1	Authentication Proof of Identity
35.	FIA_UAU.1	Timing of Authentication
36.	FIA_UAU.4	Single Use Authentication Mechanisms
37.	FIA_UAU.5	Multiple Authentication Mechanisms
38.	FIA_UAU.6	Re-Authenticating
39.	FIA_UID.1	Timing of Identification
CLASS FMT		

40.	FMT_LIM.1	FMT_LIM.1 Limited Capabilities
41.	FMT_LIM.2	FMT_LIM.2 Limited Availability
42.	FMT_SMF.1	Specification of Management Functions
43.	FMT_SMR.1	Security Roles
44.	FMT_MOF.1	Management of Security Functions Behavior
45.	FMT_MSA.1	Management of Security Attributes
46.	FMT_MTD.1/ INI_PER_AUTH_DATA	Management of TSF Data - Initialization and Personalization Authentication Data Write
47.	FMT_MTD.1/ INI_PER_AUTH_DATA_Change	Management of TSF data - Initialization and Personalization Authentication Data Change
48.	FMT_MTD.1/ Keys_and_AC_Rules_Write_and_Change	Management of TSF Data-Keys and Access Control Rules Write And Change
49.	FMT_MTD.1/PuK_Keys_Use	Management of TSF data-Public Key Usage
50.	FMT_MTD.1/PrK_Use	Management of TSF data Private Key Usage
51.	FMT_MTD.1/PIN_Management	Management of TSF data – PIN Management
CLASS FPT		
52.	FPT_EMSEC.1	TOE Emanation
53.	FPT_FLS.1	Failure with Preservation of Secure State
54.	FPT_ITT.1	Basic Internal TSF Data Transfer Protection
55.	FPT_PHP.3	Resistance to Physical Attack
56.	FPT_TST.1	TOE Testing

57.	FPT_TST.2	Subset TOE Testing
58.	FRU_FLT.2	Limited Fault Tolerance

Table9. SFRs provided by HW Document

#	Name	Title	Defined in	Note
1.	FDP_IFC.1 [HW]	Subset Information Flow Control	HW_PP	-
2.	FDP_ITT.1 [HW]	Basic Internal Transfer Protection	HW_PP	-
3.	FMT_LIM.1 [HW]	Limited Capabilities	HW_PP	-
4.	FMT_LIM.2 [HW]	Limited Availability	HW_PP	-
5.	FPT_FLS.1 [HW]	Failure with Preservation of Secure State	HW_PP	-
6.	FPT_ITT.1 [HW]	Basic Internal TSF Data Transfer Protection	HW_PP	-
7.	FPT_PHP.3 [HW]	Resistance to Physical Attack	HW_PP	-
8.	FRU_FLT.2 [HW]	Limited Fault Tolerance	HW_PP	-
9.	FAU_SAS.1 [HW]	Audit Storage	HW_PP	-
10.	FCS_RND.1 [HW]	Generation of Random Numbers	HW_PP	Covered by FCS_RNG.1 defined HW ST.
11.	FCS_CKM.1/RSA_KeyPair	Cryptographic Key Generation	HW_ST	
12.	FCS_COP.1/DES	Cryptographic Operation	HW_ST	
13.	FCS_COP.1/AES	Cryptographic Operation	HW_ST	
14.	FCS_COP.1/SHA	Cryptographic Operation	HW_ST	

#	Name	Title	Defined in	Note
15.	FCS_COP.1/RSA	Cryptographic Operation	HW_ST	
16.	FDP_SDI.1 [HW]	Stored Data Integrity Monitoring	HW_ST	
17.	FDP_SDI.2 [HW]	Stored Data Integrity Monitoring And Action	HW_ST	
18.	FCS_RNG.1 [HW]	Quality Metric for Random Numbers	HW_ST	
19.	FPT_TST.2 [HW]	Subset TOE Testing	HW_ST	

Application Note 1: The functional requirement FCS_RNG.1 which is defined in Platform ST [2][14]is a refinement of the FCS_RND.1 defined in the Protection Profile [1]

7.2.1 CLASS FAU: SECURITY AUDIT

FAU_SAS.1 Audit storage

Hierarchical to: No other components.

Dependencies: No dependencies.

FAU_SAS.1.1 The TSF shall provide the *IC Manufacturer*[11]with the capability to store *the IC Identification Data*[12]in the *not changeable configuration page area and non-volatile memory*[13].

7.2.2 CLASS FCS: CRYPTOGRAPHIC SUPPORT

FCS_CKM.1/SM Cryptographic Key Generation - Secure Messaging Session Keys

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] fulfilled by both FCS_CKM.2, FCS_COP.1/AES and FCS_COP.1/CMAC

[FCS_CKM.4 Cryptographic Key Destruction] fulfilled by FCS_CKM.4

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *Diffie-Hellman-Protocol Key Agreement*

11[assignment: list of subjects]
12 [assignment: list of auditinformation]
13[assignment: type of persistent memory].

Method[14] and specified cryptographic key sizes *32 bytes*[15] that meet the following *NIST 800-56A*[16].

Application Note 2: Generated keys by this SFR are used by both the TOE and the terminal. These keys are distributed to the terminal by FCS_CKM.2 and used by the FCS_COP.1/CMAC and FCS_COP.1/AES.

FCS_CKM.1/SM_PER-INI Cryptographic key generation– Secure Messaging Keys for Pre-Operational Phase

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] fulfilled by FCS.CKM.2/SM_PER-INI, FCS_COP.1/AES, FCS_COP.1/CMAC

[FCS_CKM.4 Cryptographic Key Destruction] fulfilled by FCS_CKM.4

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *Pre-Operational Secure Messaging Key Generation Algorithm for AKİS v2.2.8I*[17]and specified cryptographic key sizes *32 bytes*[18] that meet the following: *none*[19].

Application Note 3: This functionality is valid for pre-operational phases.

FCS_CKM.1/RSA_KeyPair Cryptographic Key Generation- RSA KeyPair Generation

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic Key Distribution, or FCS_COP.1 Cryptographic Operation] fulfilled by FCS_COP.1/SIG-GEN_PKCS#1 V1.5, FCS_COP.1/SIG-GEN_PKCS #1 V2.1, FCS_COP.1/SIG-GEN_9796, FCS_COP.1/DEC_PKCS#1 V1.5, FCS_COP.1/DEC_PKCS#1 V2.1 OAEP, FCS_COP.1/RSA_RAW,

[FCS_CKM.4 Cryptographic Key Destruction] is fulfilled by FCS_CKM.4

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *PKCS v2.1 RFC3447*[20] and specified cryptographic key sizes *2048 bit*[21] that meet the following: *According to section*

---

14 [assignment: cryptographickeygenerationalgorithm]
15[assignment: cryptographickeysizes]
16[assignment: list of standards]
17[assignment: cryptographickeygenerationalgorithm]
18[assignment: cryptographickeysizes]
19[assignment: list of standards]
20[assignment: cryptographickeygenerationalgorithm]
21[assignment: cryptographickeysizes]

3.2(2) in PKCS v2.1 RFC3447, for u=2, i.e., without any (r_i, d_i, t_i), i> 2. For p x q < 22048 additionally according to section3.2[22].

FCS_CKM.2/SM Cryptographic Key Distribution – Secure Messaging Keys

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of User Data without Security Attributes, orFDP_ITC.2 Import of User Data with Security Attributes, or FCS_CKM.1 Cryptographic Key Generation] fulfilled by FCS_CKM.1/SM

[FCS_CKM.4 Cryptographic Key Destruction] fulfilled by FCS_CKM.4

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method *Device Authentication-Secure Messaging*[23] that meets the following: *TCKK Projesinde Kullanılan Kriptografik Algoritmalar Tanım Dokümanı, 4 Nisan 2012, v1.3, TÜBİTAK BİLGEM UEKAE Kriptoloji Birimi*[24].

FCS_CKM.2/SM_PER-INI Cryptographic Key Distribution – Secure Messaging Keys for Pre-Operational Phases

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, orFDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] fulfilled by FCS_CKM.1/SM_PER-INI.

FCS_CKM.4 Cryptographic key destruction fulfilled by FCS_CKM.4

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method: *AKİSv2.2.8I SM_PER-INI key distribution method*[25] that meets the following: *TCKK Projesinde Kullanılan Kriptografik Algoritmalar Tanım Dokümanı, 4 Nisan 2012, v1.3, TÜBİTAK BİLGEM UEKAE Kriptoloji Birimi*[26].

FCS_CKM.4 Cryptographic Key Destruction

Hierarchical to: No other components.

22[assignment: list of standards]
23 [assignment: cryptographic key distribution method]
24 [assignment: list of standards]
25 [assignment: cryptographic key distribution method]
26 [assignment: list of standards]

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] fulfilled by FCS_CKM.1/SM and FCS_CKM.1/SM_PER-INI

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *AKİS v2.2.8I Key Destruction Method*[27] that meets the following: *none*[28].

FCS_RNG.1 Cryptographic Key Destruction

Dependencies: No dependencies

FCS_RNG.1.1 The TSF shall provide a *physical* random number generator that implements:

PTG.2.1 A total failure test detects a total failure of entropy source immediately when the RNG has started. When a total failure is detected, no random numbers will be output.

PTG.2.2 If a total failure of the entropy source occurs while the RNG is being operated, the RNG prevents the output of any internal random number that depends on some raw random numbers that have been generated after the total failure of the entropy source.

PTG.2.3 The online test shall detect non-tolerable statistical defects of the raw random number sequence (i) immediately when the RNG has started, and (ii) while the RNG is being operated. The TSF must not output any random numbers before the power-up online test has finished successfully or when a defect has been detected.

PTG.2.4 The online test procedure shall be effective to detect non-tolerable weaknesses of the random numbers soon.

PTG.2.5 The online test procedure checks the quality of the raw random number sequence. It is triggered continuously. The online test is suitable for detecting non-tolerable statistical defects of the statistical proper- ties of the raw random numbers within an acceptable period of time.

FCS_RNG.1.2 The TSF shall provide *numbers in the format 8- or 16-bit* that meet

PTG.2.6 Test procedure A, as defined in [15]does not distinguish the internal random numbers from output sequences of an ideal RNG.

27 [assignment: cryptographic key destruction method]
28 [assignment: list of standards]

PTG.2.7 The average Shannon entropy per internal random bit exceeds 0.997.

The following cryptographic functions are implemented and evaluated in the TOE:

- SHA-256 operation,
- AES operation,
- CMAC operation,
- TDES operation,
- signature generation PKCS#1 v1.5,
- signature generation PKCS#1 v2.1,
- signature generation ISO/IEC 9796-2 Scheme 1,
- signature verification ISO/IEC 9796-2 Scheme 1,
- asymmetric decryption PKCS#1 v1.5,
- asymmetric decryption PKCS#1 v2.1,
- asymmetric encryption/decryption RAW RSA,
- random number generation.

Preface Regarding Security Level related to Cryptography

The strength of the cryptographic algorithms was not rated in the course of the Product Certification. To fend off attackers with high attack potential, appropriate cryptographic algorithms with adequate key lengths must be used (references can be found in national and international documents and standards). According to these standards RSA-1024 is not recommended. Therefore, for this functions it shall be checked whether the related cryptographic operations are appropriate for the intended system.

In addition, TDES 112 bit is also not recommended. Yet AKİS v2.2.8I does not supply interface for TDES 112 bit. In addition, the functions triggering TDES operations are used in the initialization and personalization subphases which are assumed to be carried on in physically secure environment. Therefore, no cryptographic attack due to TDES functionality is foreseen.

FCS_COP.1 /SHA Cryptographic Operation-SHA 256 Calculation

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] is not fulfilled but justified.

[FCS_CKM.4 Cryptographic key destruction] is not fulfilled but justified.

FCS_COP.1.1 The TSF shall perform *hash value calculation*[29] in accordance with a specified cryptographic algorithm *SHA-256*[30] and cryptographic key sizes *none*[31] that meet the following: *U.S. Department of Commerce / National Institute of Standards and Technology, Secure Hash Standard (SHS), FIPS PUB 180-4, 2012-March, section 6.2 SHA-256*[32].

Application Note 4:TOE also has SHA-1 capability. But it is not in the scope of this certification.

FCS_COP.1 /AES Cryptographic Operation-AES Calculation for Secure Messaging

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] is fulfilled by FCS_CKM.1/SM and FCS_CKM.1/SM_PER-INI

[FCS_CKM.4 Cryptographic Key Destruction] is fulfilled by FCS_CKM.4

FCS_COP.1.1 The TSF shall perform *encryption and decryption*[33] in accordance with a specified cryptographic algorithm *AES ECB and CBC Mode*[34] and cryptographic key sizes *32 bytes*[35] that meet the following:

- *AES-256: FIPS 197 Advanced Encryption Standard, NIST, November 2001,*
- *CBC Mode: Recommendation for Block Cipher Modes of Operation, NIST SP 800-38A, December 2001*[36]

Application Note5:TOE has no interface for AES operation. It is provided automatically when secure messaging operation starts

FCS_COP.1 /TDES Cryptographic Operation-Initialization Verification with TDES

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] is not fulfilled but justified.

29 [assignment: list of cryptographicoperations]
30 [assignment: cryptographicalgorithm]
31 [assignment: cryptographickeysizes]
32 [assignment: list of standards]
33 [assignment: list of cryptographicoperations]
34 [assignment: cryptographicalgorithm]
35 [assignment: cryptographickeysizes]
36 [assignment: list of standards]

[FCS_CKM.4 Cryptographic Key Destruction] is not fulfilled but justified.

FCS_COP.1.1 The TSF shall perform *initialization verification with decryption*[37] in accordance with a specified cryptographic algorithm *Triple DES*[38] and cryptographic key sizes *112 bits*[39]that meet the following: *National Institute of Standards and Technology (NIST), Technology Administration, U.S. Department of Data Encryption Standard (DES), NIST Special Publication 800-38A, 2001 Edition2*[40]

Application Note 6: Applicable only for decryption form during initialization agent and personalization agent authentication.

FCS_COP.1 /CMAC Cryptographic operation-CMAC Calculation for Secure Messaging

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] is fulfilled but FCS_CKM.1/SM and FCS_CKM.1/SM_PER-INI

FCS_CKM.4 Cryptographic key destruction fulfilled by FCS_CKM.4

FCS_COP.1.1 The TSF shall perform *message authentication*[41] in accordance with a specified cryptographic algorithm *AES-CMAC*[42] and cryptographic key sizes *32 bytes*[43] that meet the following:

- *AES-256: FIPS 197 Advanced Encryption Standard, NIST, November 2001, NIST SP 800-38B*
- *"Recommendation For Block Cipher Modes of Operation: The CMAC Mode for Authentication" May 2005*[44]

Application Note 7:TOE has no interface for CMAC operation. It is provided automatically when secure messaging operation starts.

FCS_COP.1/SIG-GEN_PKCS#1 V1.5 Cryptographic Operation-Signature Generation PKCS#1 v1.5

Hierarchical to: No other components.

37 [assignment: list of cryptographicoperations]
38 [assignment: cryptographicalgorithm]
39 [assignment: cryptographickeysizes]
40 [assignment: list of standards]
41 [assignment: list of cryptographicoperations]
42 [assignment: cryptographicalgorithm]
43 [assignment: cryptographickeysizes]
44 [assignment: list of standards]

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] fulfilled by FCS_CKM.1/RSA_KeyPair

FCS_CKM.4 Cryptographic key destruction fulfilled by FCS_CKM.4

FCS_COP.1.1 The TSF shall perform *digital signature generation*[45] in accordance with specified cryptographic algorithm *RSASSA*[46] and cryptographic key sizes 1024/*2048 bit*[47] that meet the following: *PKCS#1 v1.5, RFC 2313, March 1998.*[48]

FCS_COP.1/SIG-GEN_PKCS #1 V2.1 Cryptographic Operation-Signature Generation PKCS#1 v2.1

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] fulfilled by FCS_CKM.1/RSA_KeyPair

FCS_CKM.4 Cryptographic key destruction fulfilled by FCS_CKM.4

FCS_COP.1.1 The TSF shall perform *digital signature generation*[49] in accordance with a specified cryptographic algorithm *RSASSA-PSS*[50] and cryptographic key sizes *1024/2048 bit*[51] that meet the following: *PKCS#1 v2.1,RFC 3447, February 2003*[52]

FCS_COP.1 /SIG-GEN_9796 Cryptographic operation-Signature Generation ISO/IEC 9796-2 Scheme 1

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] fulfilled by FCS_CKM.1/RSA_KeyPair

FCS_CKM.4 Cryptographic key destruction fulfilled by FCS_CKM.4

FCS_COP.1.1 The TSF shall perform *digital signature generation*[53] in accordance with a specified cryptographic algorithm *RSA and SHA-256*[54] and cryptographic key sizes *1024/2048 bit*[55] that meet the following: *ISO/IEC 9796-2 Scheme 1, 2010*[56]

---

45 [assignment: list of cryptographicoperations]
46 [assignment: cryptographicalgorithm]
47 [assignment: cryptographic key sizes]
48[assignment: list of standards]
49 [assignment: list of cryptographic operations]
50 [assignment: cryptographic algorithm]
51 [assignment: cryptographic key sizes]
52[assignment: list of standards]
53 [assignment: list of cryptographic operations]

FCS_COP.1 /SIG-VER_9796 Cryptographic operation- Signature Verification ISO/IEC 9796-2 Scheme 1

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]
not fulfilled but justified
[FCS_CKM.4 Cryptographic Key Destruction] not fulfilled but justified

FCS_COP.1.1 The TSF shall perform *digital signature verification*[57] in accordance with a specified cryptographic algorithm *RSA and SHA-256*[58] and cryptographic key sizes *1024/2048 bit*[59] that meet the following: *ISO/IEC 9796-2 Scheme 1, December 2010*[60].

FCS_COP.1 / DEC_PKCS#1 v1.5 Cryptographic operation-Asymmetric Decryption PKCS#1 v.1.5

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] fulfilled by FCS_CKM.1/RSA_KeyPair
[FCS_CKM.4 Cryptographic Key Destruction] fulfilled by FCS_CKM.4

FCS_COP.1.1 The TSF shall perform *asymmetric decryption*[61] in accordance with specified cryptographic algorithm *RSAES*[62] and cryptographic key sizes *1024/2048 bit*[63] that meet the following: *PKCS #1 v1.5, RFC 2313, March 1998.*

FCS_COP.1 / DEC_PKCS#1 v2.1 Cryptographic operation-Asymmetric Decryption PKCS#1 v2.1

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] fulfilled by FCS_CKM.1/RSA_KeyPair
FCS_CKM.4 Cryptographic Key Destruction] fulfilled by FCS_CKM.4

---

54 [assignment: cryptographic algorithm]
55 [assignment: cryptographic key sizes]
56[assignment: list of standards]
57 [assignment: list of cryptographic operations]
58 [assignment: cryptographic algorithm]
59 [assignment: cryptographic key sizes]
60[assignment: list of standards]
61 [assignment: list of cryptographic operations]
62 [assignment: cryptographic algorithm]
63 [assignment: cryptographic key sizes]

FCS_COP.1.1 The TSF shall perform *asymmetric decryption*[64] in accordance with a specified cryptographic algorithm *RSAES-OAEP*[65] and cryptographic key sizes *1024/2048 bit*[66] that meet the following: *PKCS #1 v2.1,RFC 3447, February 2003*[67]

FCS_COP.1 / RSA_RAW Cryptographic operation-Asymmetric Encryption/Decryption RAW RSA

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] fulfilled by FCS_CKM.1/RSA_KeyPair

[FCS_CKM.4 Cryptographic Key Destruction] fulfilled by FCS_CKM.4

FCS_COP.1.1 The TSF shall perform *asymmetric encryption/decryption*[68] in accordance with a specified cryptographic algorithm *Rivest-Shamir-Adleman (RSA-Raw)*[69] and cryptographic key sizes *1024/2048 bit*[70] that meet the following: *RSA Cryptography Standard*[71]

Application Note 8:TOE has no interface for these operations. They are performed automatically when chip and terminal authentication operations start.

7.2.3 CLASS FDP: USER DATA PROTECTION

FDP_ACC.1/Data Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control fulfilled by FDP_ACF.1

FDP_ACC.1.1: The TSF shall enforce the *Application access control SFP*[72] on

subject:

- *initialization agent,*
- *personalization agent,*

64 [assignment: list of cryptographic operations]
65 [assignment: cryptographic algorithm]
66 [assignment: cryptographic key sizes]
67[assignment: list of standards]
68 [assignment: list of cryptographic operations]
69 [assignment: cryptographic algorithm]
70 [assignment: cryptographic key sizes]
71[assignment: list of standards]
72 [assignment: access control SFP]

- *terminal,*
- *application defined and allowed role,*

objects:

- *User data stored*

operations:

- *write, create, read, delete.*[73]

FDP_ACC.1/FUN Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control fulfilled by FDP_ACF.1

FDP_ACC.1.1: The TSF shall enforce the *application access control SFP*[74] on

subjects:

- *activation agent,*
- *initialization agent,*
- *personalization agent,*
- *application defined and allowed role, and*

objects and operations as referred to in

- *defined command function for activation subphase in document [12],*
- *defined command function for initialization subphase in document [12],*
- *defined command function for personalization subphase in document [12],*
- *defined command function for operation phase in document [12],*
- *defined command function for death phase in document [12].*[75]

FDP_ACF.1/Data Security attributes based access control

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset Access Control] is fulfilled by FDP_ACC.1

[FMT_MSA.3 Static Attribute Initialization] is not fulfilled but justified

73 [assignment: list of subjects, objects, andoperationsamongsubjectsandobjectscoveredbythe SFP]
74 [assignment: accesscontrol SFP]
75[assignment: list of subjects, objects, andoperationsamongsubjectsandobjectscoveredbythe SFP]

FDP_ACF.1.1 The TSF shall enforce the a*pplication access control SFP*[76] to objects based on the following:

subjects:

- *initialization agent,*
- *personalization agent,*
- *terminal,*
- *application defined and allowed role,*

subject attributes:

- *authorization level of subjects,*

object:

- *user data Stored in TOE,*

object attribute:

- *data access control rules.*[77]

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

- *Application defined and allowed roles have read, write, change access according to rules determined by application developer.*
- *Successfully authenticated terminal*[78] *have read, write, and change access according to rules determined by application developer.*[79]

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: *authenticated initialization and personalization agents are authorized to access all application data in pre-operational phase.*[80]

76 [assignment: access control SFP]
77 [assignment: list of subjectsandobjectscontrolledundertheindicated SFP, andforeach, the SFP-relevantsecurityattributes, ornamedgroups of SFP-relevantsecurityattributes]
78 It means PIN authenticated terminal for SAM configuration.
79 [assignment: rulesgoverningaccessamongcontrolledsubjectsandcontrolledobjectsusingcontrolledoperations on controlledobjects]
80 [assignment: rules, based on securityattributesthatexplicitlyauthoriseaccess of subjectstoobjects]

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *Nobody shall be allowed to have write, create, read, and delete access user data in death phase*[81].

FDP_ACF.1/FUN Security Attributes Based Access Control

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset Access Control] is fulfilled by FDP_ACC.1

[FMT_MSA.3 Static Attribute Initialization] is not fulfilled but justified

FDP_ACF.1.1 The TSF shall enforce the a*pplication access control SFP*[82] to objects based on the following:

subjects:

- *activation agent,*
- *initialization agent,*
- *personalization agent,*
- *Application defined and allowed roles,*

objects, and their attributes as referred to in[83]

- *defined command function for activation subphase in document [12]*
- *defined command function for initialization subphase in document [12]*
- *defined command function for personalization subphase in document [12]*
- *defined command function for operation phase in document [12]*
- *defined command function for death phase in document [12].*[84]

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

- *Only activation agent access defined command function for activation Subphase in document [12]*
- *Only initialization agent access defined command function for Initialization Subphase in document [12]*

81 [assignment: rules, based on securityattributes, thatexplicitlydenyaccess of subjectstoobjects]
82 [assignment: accesscontrol SFP]
83 [assignment: list of subjectsandobjectscontrolledundertheindicated SFP, andforeach, the SFP-relevantsecurityattributes, ornamedgroups of SFP-relevantsecurityattributes]
84 [assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes]

- *Only personalization agent defined command function for personalization Subphase in document [12]*
- *Only application defined and allowed roles access defined command function for operation phase in document [12].*[85]

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: *Any user is allowed to access Defined command function for Death Phase in document [12]*[86].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *none*[87].

FDP_UCT.1 Basic Data Exchange Confidentiality

Hierarchical to: No other components.

Dependencies: [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] not fulfilled but justified

[FDP_ACC.1 Subset Access Control, or FDP_IFC.1 Subset information flow control]

Is fulfilled by FDP_ACC.1

FDP_UCT.1.1 The TSF shall enforce the Application access control SFP88to transmit, receive[89]user data in a manner protected from unauthorized disclosure.

Application Note 9: This SFR is valid for the communication between TOE and Terminal.

FDP_UIT.1 Data Exchange Integrity

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] fulfilled by FDP_ACC.1

[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] not fulfilled but justified

FDP_UIT.1.1 The TSF shall enforce the *Application access control SFP*[90]to transmit, receive[91]user data in a manner protected from modification, deletion, insertion, replay[92] errors.

85 [assignment: rulesgoverningaccessamongcontrolledsubjectsandcontrolledobjectsusingcontrolledoperations on controlledobjects]
86 [assignment: rules, based on security attributes that explicitly authorise access of subjects to objects]
87 [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]
88 [assignment: access control SFP(s) and/or information flow control SFP(s)]
89[selection: transmit, receive]
90 [assignment: access control SFP(s) and/or information flow control SFP(s)]

FDP_UIT.1.2 The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion, replay[93] has occurred.

Application Note 10: This SFR is valid for the communication between TOE and terminal.

FDP_IFC.1 Subset information flow control

Hierarchical to: No other components.

Dependencies: [FDP_IFF.1 Simple security attributes not fulfilled but justified]

FDP_IFC.1.1 The TSF shall enforce the *Platform Data Processing Policy*[94]on all confidential data when they are processed between the different parts of the TOE[95].

Refinement : Data Processing Policy : user data and TSF data shall not be accessible from the TOE except when the Security IC embedded software decides to communicate the user data via an external interface. The protection shall be applied to confidential data only but without the distinction of attributes controlled by the security IC embedded software.

FDP_ITT.1 Basic Internal Transfer Protection

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] fulfilled by FDP_IFC.1

FDP_ITT.1.1 The TSF shall enforce the *Platform Data Processing Policy*[96] to prevent the *disclosure*[97]of user data when it is transmitted between physically-separated parts of the TOE.

Refinement: The different memories, the CPU and other functional units of the TOE (e.g. a cryptographic co-processor) are seen as physically-separated parts of the TOE.

FDP_SDI.1/HW Stored Data Integrity Monitoring - HW

Hierarchical to: No other components

Dependencies: No dependencies

---

91 [selection: transmit, receive]
92[selection: modification, deletion, insertion, replay]
93[selection: modification, deletion, insertion, replay]
94[assignment: information flow control SFP]
95 [assignment: list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP]
96 [assignment: access control SFP(s) and/or information flow control SFP(s)]
97 [selection: disclosure, modification, loss of use]

FDP_SDI.1.1 The TSF shall monitor user data stored in containers controlled by the TSF for *inconsistencies between stored data and corresponding EDC*[98]on all objects, based on the following attributes: *EDC value for the RAM, ROM and Infineon® SOLID FLASH™*[99].

FDP_SDI.2/HW Stored Data Integrity Monitoring And Action - HW

Hierarchical to: FDP_SDI.1 stored data integrity monitoring

Dependencies: No dependencies

FDP_SDI.2.1 The TSF shall monitor user data stored in containers controlled by the TSF for *data integrity and one- and/or more-bit-errors*[100]on all objects, based on the following attributes: *corresponding EDC value for RAM, ROM and Infineon® SOLID FLASH™ and error correction ECC for the Infineon® SOLID FLASH™*[101].

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall *correct 1 bit errors in the Infineon® SOLID FLASH™ automatically*[102].

FDP_SDI.2/EOS Stored Data Integrity Monitoring and Action

Hierarchical to: FDP_SDI.1 stored data integrity monitoring

Dependencies: No dependencies

FDP_SDI.2.1 The TSF shall monitor user data stored in containers controlled by the TSF for *data integrity and one- and/or more-bit-errors*[103]on all objects, based on the following attributes: *corresponding EDC value for integrity critical user data in files, file headers, SKK and DBT tables, special registers*[104].

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall *inform the user by an error code*[105].

7.2.4 CLASS FIA: IDENTIFICATION AND AUTHENTICATION

FIA_AFL.1/PIN - Authentication Failure Handling – PIN Verification

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

98[assignment: integrity errors]
99[assignment: user data attributes]
100[assignment: integrity errors]
101[assignment: user data attributes]
102 [assignment:actionto be taken]
103 [assignment: integrity errors]
104 [assignment: user data attributes]
105 [assignment:actionto be taken]

FIA_AFL.1.1 The TSF shall detect when *an administrator configurable positive integer within 1 to 255*[106] unsuccessful authentication attempts occur related to *PIN authentication event*[107].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met[108], the TSF shall *block the usage of PIN*[109].

FIA_AFL.1/ACT - Authentication Failure Handling – Activation

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when *64*[110] unsuccessful authentication attempts occur related to *activation role authentication*[111].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *met*[112], the TSF shall *put the card into death phase*[113].

FIA_AFL.1/INI - Authentication Failure Handling - Initialization

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when *10*[114] unsuccessful authentication attempts occur related to *initialization agent Authentication*[115].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *met*[116], the TSF shall *put the card into death phase*[117].

FIA_AFL.1/PER - Authentication Failure Handling - Personalization

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

106 [selection: [assignment: positiveintegernumber], an administratorconfigurablepositiveintegerwithin [assignment: range of acceptablevalues]]
107 [assignment: list of authenticationevents]
108 [selection: met, surpassed]
109 [assignment: list of actions]
110 [selection: [assignment: positiveintegernumber], an administratorconfigurablepositiveintegerwithin [assignment: range of acceptablevalues]]
111 [assignment: list of authenticationevents]
112 [selection: met, surpassed]
113 [assignment: list of actions]
114 [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]
115 [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]
116 [selection: met, surpassed]
117 [assignment: list of actions].

FIA_AFL.1.1 The TSF shall detect when *10*[118] unsuccessful authentication attempts occur related to *personalization agent authentication*[119].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met[120], the TSF shall *put the card into death phase*[121].

FIA_API.1 Authentication Proof of Identity

Hierarchical to: No other components

Dependencies: No dependency

FIA.API.1.1 The TSF shall provide a *chip authentication*[122] to prove the identity of the *card itself*[123].

Application Note 11: This SFR is valid for both Chip and SAM configuration.

FIA_UAU.1 Timing of Authentication

Hierarchical to: No other components.

Dependencies: [FIA_UID.1 Timing of identification] is fulfilled by FIA_UID.1.

FIA_UAU.1.1 The TSF shall allow

- *to read chip serial number: at pre-operational, operational and death phases, and*
- *to perform any application allowed actions*[124]

on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.4 Single Use Authentication Mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to

- *terminal authentication and*
- *role holder authentication.*[125]

118[selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]
119[assignment: list of authentication events].
120[selection: met, surpassed]
121[assignment: list of actions]
122[assignment: authentication mechanism]
123[assignment: authorized user or role]
124[assignment: list of TSF mediated actions]

Application Note 12: This SFR is valid for both terminal and role authentication for chip configuration. But, terminal authentication is PIN Authentication for SAM configuration as stated before. PIN Authentication is also valid for Chip Configuration. PIN authentication data might be reused normally. But this situation does not cause a security flaw by means of secure messaging capabilities.

FIA_UAU.5 Multiple Authentication Mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1 The TSF shall provide *following authentication mechanisms to support user authentication:*

- *activation agent authentication,*
- *personalization agent authentication,*
- *initialization agent authentication,*
- *terminal authentication*[126]*,*
- *role authentication,*
- *PIN authentication.*[127]

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the following policies:

- *The TOE will accept the activation agent as authenticated if he or she passes activation agent authentication.*
- *The TOE will accept the initialization agent as authenticated if he or she passes initialization agent authentication.*
- *The TOE will accept the personalization agent as authenticated if he or she passes personalization agent authentication.*
- *The TOE will accept the terminal as rightful terminal if the terminal passes authentication.*
- *The TOE will accept the application defined and allowed role if he or she passes role or PIN authentication*[128]*.*

125[assignment: identified authentication mechanism(s)]
126It means PIN authentication for SAM configuration.
127[assignment: list of multiple authentication mechanisms]

FIA_UAU.6 Re-Authenticating

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions

- *each reset or power-up,*
- *each command sent to the TOE during secure messaging.*[129]

FIA_UID.1 Timing of identification

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1 The TSF shall allow

- *to read chip serial number: at pre-operational, operational and death phases and*
- *to perform any application allowed action*[130]

on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

7.2.5 CLASS FMT: SECURITY MANAGEMENT

FMT_LIM.1 Limited capabilities

Hierarchical to: No other components.

Dependencies: [FMT_LIM.2 Limited Availability] is fulfilled by FMT_LIM.2

FMT_LIM.1.1 The TSF shall be designed and implemented in a manner that limits its capabilities so that in conjunction with “Limited availability (FMT_LIM.2)” the following policy is enforced: *Deploying test features after TOE delivery do not allow*

- *user data and TSF data to be manipulated and disclosed,*
- *embedded operating system to be reconstructed and*
- *substantial information about construction of TSF to be gathered which may enable other attacks.*[131]

128[assignment: rules describing how the multiple authentication mechanisms provide authentication]
129[assignment: list of conditions under which re-authentication is required]
130[assignment: list of TSF-mediated actions]

FMT_LIM.2 Limited availability

Hierarchical to: No other components.

Dependencies: FMT_LIM.1 Limited capabilities fulfilled by FMT_LIM.1.

FMT_LIM.2.1 The TSF shall be designed in a manner that limits its availability so that in conjunction with "Limited capabilities (FMT_LIM.1)" the following policy is enforced: *Deploying test features after TOE delivery do not allow*

- *user data and TSF Data to be manipulated and disclosed,*
- *Embedded operating system to be reconstructed,*
- *Substantial information about construction of TSF to be gathered which may enable other attacks.*[132]

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

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

- *activation,*
- *initialization,*
- *personalization,*
- *any management function defined by application developer.*[133]

FMT_SMR.1 Security Roles

Hierarchical to: No other components.

Dependencies: [FIA_UID.1/ Timing of identification] is fulfilled by FIA_UID.1.

FMT_SMR.1.1 The TSF shall maintain the roles

- *activation agent,*
- *initialization agent,*
- *personalization agent,*
- *any management role defined by application developer.*[134]

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

131[assignment: Limited capability and availability policy]
132[assignment: Limited capabilityandavailabilitypolicy]
133 [assignment: list of management functions to be provided by the TSF]
134 [assignment: the authorised identified roles]

Application Note 13: The term “role” in this SFR is used as general Word in CC Part 2 and not about authenticated role holder.

FMT_MOF.1 Management of Security Functions Behavior

Hierarchical to: No other components.

Dependencies: [FMT_SMR.1 Security Roles] fulfilled by FMT_SMR.1

[FMT_SMF.1 Specification of Management Functions] is fulfilled by FMT_SMF.1

FMT_MOF.1.1 The TSF shall restrict the ability to disable and enable[135] the functions

- *External interface command for operational mode listed in [13]in*[136] to *application defined roles*[137].

Application Note 14: Applicable only for operational phase. Not applicable for activation, initialization and personalization.

FMT_MSA.1 Management of Security Attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] fulfilled by FDP_ACC.1

[FMT_SMR.1 Security Roles] is fulfilled by FMT_SMR.1

[FMT_SMF.1 Specification of Management Functions] is fulfilled by FMT_SMF.1

FMT_MSA.1.1 The TSF shall enforce the *Application access control Policy*[138] to restrict the ability to query, modify, delete[139] the security attributes *access control rules of keys, PINs, user data*[140] to *initialization agent, personalization agents and application defined roles*[141].

FMT_MTD.1/INI_PER_AUTH_DATA Management of TSF data - Initialization and Personalization Authentication Data Write

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles fulfilled by FMT_SMR.1

FMT_SMF.1 Specification of Management Functions fulfilled by FMT_SMF.1

FMT_MTD.1.1 The TSF shall restrict the ability to write[142]the *authentication reference data for Initialization and personalization agents*[143] to *activation agent*[144].

135[selection: determine the behaviour of, disable, enable, modify the behaviour of]
136[assignment: list of functions]
137[assignment: the authorised identified roles]
138[assignment: access control SFP(s), information flow control SFP(s)]
139 [selection: change default, query, modify, delete, [assignment: other operations]]
140[assignment: list of security attributes]
141[assignment: the authorised identified roles]

FMT_MTD.1/INI_PER_AUTH_DATA_Change Management of TSF data - Initialization and Personalization Authentication Data Change

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles fulfilled by FMT_SMR.1

FMT_SMF.1 Specification of Management Functions fulfilled by FMT_SMF.1

FMT_MTD.1.1 The TSF shall restrict the ability to change[145]*the authentication reference data for Initialization and personalization agents*[146] to *Initialization and personalization agents*[147].

FMT_MTD.1/Keys_and_AC_Rules_Write_and_Change Management of TSF data-Keys and Access Control Rules Write and Change

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles fulfilled by FMT_SMR.1

FMT_SMF.1 Specification of Management Functions fulfilled by FMT_SMF.1

FMT_MTD.1.1 The TSF shall restrict the ability to write and change[148] the *root Certificate Authority public key, chip authentication PuK and PrK and access control Rules*[149] to *initialization agent, personalization agent any application defined and allowed role*[150].

FMT_MTD.1/PuK_Keys_Use Management of TSF data-Usage Public Key Usage

Hierarchical to: No other components.

Dependencies: [FMT_SMR.1 Security Roles] fulfilled by FMT_SMR.1

[FMT_SMF.1 Specification of Management Functions] fulfilled by FMT_SMF.1

FMT_MTD.1.1 The TSF shall restrict the ability to use[151]the *Root CA PuK and chip authentication PuK*[152]to *application defined and allowed roles*[153].

FMT_MTD.1/PrK_Use Management of TSF data-Private Key Usage

Hierarchical to: No other components.

142[selection: change_default, query, modify, delete, clear, [assignment: other operations]]
143[assignment: list of TSF data]
144[assignment: the authorised identified roles]
145[selection: change_default, query, modify, delete, clear, [assignment: other operations]]
146[assignment: list of TSF data]
147[assignment: the authorised identified roles]
148[selection: change_default, query, modify, delete, clear, [assignment: other operations]]
149[assignment: list of TSF data]
150[assignment: the authorised identified roles]
151[selection: change_default, query, modify, delete, clear, [assignment: other operations]]
152[assignment: list of TSF data]
153 [assignment: the authorised identified roles]

Dependencies: [FMT_SMR.1 Security Roles] fulfilled by FMT_SMR.1

[FMT_SMF.1 Specification of Management Functions] is fulfilled by FMT_SMF.1

FMT_MTD.1.1 The TSF shall restrict the ability to use[154]the *chip authentication PrK*[155]to *application defined and allowed roles*[156].

FMT_MTD.1/PIN_Management Management of TSF data – PIN Management

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles fulfilled by FMT_SMR.1

FMT_SMF.1 Specification of Management Functions fulfilled by FMT_SMF.1

FMT_MTD.1.1 The TSF shall restrict the ability to write, change, and unblock[157] the *PIN objects*[158] to *initialization agent, personalization agents, any application defined and allowed roles*[159].

7.2.6 CLASS FPT: PROTECTION OF THE TSF

FPT_EMSEC.1 TOE Emanation

Hierarchical to: No other components

Dependencies: No dependencies

FPT_EMSEC.1.1 The TOE shall not emit*, timing variations during command execution*[160]in excess of *non-useful information*[161] enabling access to *Initialization and Personalization Keys, PINs used by the application*[162], and *none*.[163]

FPT_EMSEC.1.2 The TSF shall ensure *any users*[164]are unable to use the following interface *contact interface and physical contacts*[165] to gain access to *none*.[166]

FPT_FLS.1 Failure with Preservation of Secure State

Hierarchical to: No other components.

Dependencies: No dependencies.

154[selection: change_default, query, modify, delete, clear, [assignment: other operations]]
155[assignment: list of TSF data]
156 [assignment: the authorised identified roles]
157 [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
158 [assignment: list of TSF data]
159 [assignment: the authorised identified roles]
160[assignment: types of emissions]
161[assignment: specified limits]
162[assignment: list of types of TSF data]
163[assignment list of types of user data].
164[assignment: type of users]
165[assignment: type of connection]
166[assignment: list of type of user data].

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: *exposure to operating conditions which may not be tolerated according to the requirement Limited fault tolerance (FRU_FLT.2) and where therefore a malfunction could occur*[167].

Refinement: The term "failure" above also covers "circumstances". The TOE prevents failures for the "circumstances" defined above.

Application Note 15: Secure state called security reset for TOE.

FPT_ITT.1 Basic Internal TSF Data Transfer Protection

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_ITT.1.1 The TSF shall protect TSF data from disclosure[168] when it is transmitted between separate parts of the TOE.

Refinement: The different memories, the CPU and other functional units of the TOE (e.g. a cryptographic co-processor) are seen as separated parts of the TOE.

Application Note 16: Thisrequirement is equivalent to FDP_ITT.1 above but refers to TSF data instead of user data. Therefore, it should be understood as to refer to the same data

FPT_PHP.3 Resistance to Physical Attack

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_PHP.3.1 The TSF shall resist *physical manipulation and physical probing*[169] to the *TSF*[170] by responding automatically such that the SFRs are always enforced.

Refinement: The TSF will implement appropriate mechanisms to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TSF can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that security functional requirements are enforced. Hence, "automatic

167[assignment: list of types of failures in the TSF]
168[selection: disclosure, modification]
169[assignment: physicaltamperingscenarios]
170[assignment: list of TSF devices/elements]

response" means here (i) assuming that there might be an attack at any time and (ii) countermeasures are provided at any time.

FPT_TST.1 TSF Testing

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TST.1.1 The TSF shall run a suite of self tests during normal operation[171] to demonstrate the **integrity of TSF Data except EOS Code** and correct operation of the TSF[172].

FPT_TST.1.2 The TSF shall ~~provide authenticated users with the capability to~~ verify the integrity of TSF Data[173].

FPT_TST.1.3 The TSF shall ~~provide authenticated users with the capability to~~ verify the integrity of TSF[174].

FPT_TST.2 Subset TOE Testing

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TST.2.1 The TSF shall run a suite of self tests *during initial startup and before critical operations*[175] to demonstrate the correct operation of the *alarm lines and/or following environmental sensor mechanisms:*

- *PFD - post failure detection,*
- *CORE – CPU related alarms,*
- *SCP - symmetric cryptographic co-processor,*
- *temperature alarm,*
- *AXI – memory bus,*
- *EDC – error detection code,*
- *FSE – internal frequency sensor alarm,*
- *Light – light sensitive alarm,*
- *WDT - watch dog timer related alarms,*
- *SW – software triggered alarm,*

171[selection: during initial start-up, periodically during normal operation, at the request of the authorized user, at the conditions[assignment: conditions under which self test should occur]]
172[selection: [assignment: parts of TSF], the TSF]
173[selection: [assignment: parts of TSF data], TSF data]
174[selection: [assignment: parts of TSF], TSF]
175[selection: during initial start-up, periodically, during normal operation, at the request of the authorized user, and/or at the conditions [assignment: conditions under which self-test should occur]]

- *PTRNG –physical true random number generator or TRNG true random number generator*

7.2.7 CLASS FRU: RESOURCE UTILISATION

FRU_FLT.2 Limited Fault Tolerance

Hierarchical to: FRU_FLT.1Degraded fault tolerance

Dependencies: [FPT_FLS.1 Failure with Preservation of Secure State] is fulfilled by FPT_FLS.1

FRU_FLT.2.1 The TSF shall ensure the operation of all the TOE's capabilities when the following failures occur: *exposure to operating conditions which are not detected according to the requirement Failure with preservation of secure state (FPT_FLS.1)]*[176].

Refinement: The term “failure” above means “circumstances”. The TOE prevents failures for the “circumstances” defined above.

Application Note 17: Environmental conditions include but are not limited to power supply, clock, and other external signals (e.g. reset signal) necessary for the TOE operation.

7.3 SECURITY ASSURANCE REQUIREMENTS

The assurance requirements for the evaluation of the TOE, its development and operating environment are to choose as the predefined assurance package EAL4augmented by the following components:

- ALC_DVS.2 (Sufficiency of security measures),
- AVA_VAN.5 (Advanced methodical vulnerability analysis).

176[assignment: list of type of failures]

7.4 SECURITY REQUIREMENTS DEPENDENCIES

7.4.1 SECURITY FUNCTIONAL REQUIREMENTS DEPENDENCIES

The dependence of security functional requirements for Embedded OS the security functional requirements are defined in the following Table.

Table10. Dependency of Composite TOE SFRs

#	Security Functional Requirement	Dependencies	Fulfilled by security requirements in this PP
1	FAU_SAS.1	None	----
2	FCS_CKM.1/SM	--- FCS_CKM.2 or FCS_COP.1 --- FCS_CKM.4	---FCS.CKM.2/SM, FCS_COP.1/AES, FCS_COP.1/CMAC --- FCS_CKM.4
3	FCS_CKM.1/SM_PER-INI	--- FCS_CKM.2 or FCS_COP.1 --- FCS_CKM.4	--- FCS.CKM.2/SM_PER-INI, FCS_COP.1/AES, FCS_COP.1/CMAC --- FCS_CKM.4
4	FCS_CKM.1/RSA_KeyPair	--- FCS_CKM.2 or FCS_COP.1 --- FCS_CKM.4	--- FCS_COP.1 /SIG-VER_PKCS,FCS_COP.1 /SIG-GEN_PKCS, FCS_COP.1 /SIG-VER_9796, FCS_COP.1 /SIG-GEN_9796 ---- FCS_CKM.4
5	FCS_CKM.2/SM	--- FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 --- FCS_CKM.4	--- FCS_CKM.1/SM --- FCS_CKM.4
6	FCS_CKM.2/SM_PER-INI	--- FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 --- FCS_CKM.4	--- FCS_CKM.1/SM_PER-INI --- FCS_CKM.4
7	FCS_CKM.4	None	----
8	FCS_COP.1/SHA	--- FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	--- Not fulfilled but justified. See Explanation 1

#	Security Functional Requirement	Dependencies	Fulfilled by security requirements in this PP
		--- FCS_CKM.4	--- Not fulfilled but justified. See Explanation 1
9	FCS_COP.1/AES	--- FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 --- FCS_CKM.4	---FCS_CKM.1/SM and FCS_CKM.1/SM_PER-INI --- FCS_CKM.4
10	FCS_COP.1/TDES	--- FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 --- FCS_CKM.4	--- Not fulfilled but justified. See Explanation 2 --- Not fulfilled but justified. See Explanation 3
11	FCS_COP.1/CMAC	--- FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 --- FCS_CKM.4	---FCS_CKM.1/SM and FCS_CKM.1/SM_PER-INI --- FCS_CKM.4
12	FCS_COP.1/SIG-GEN_PKCS#1 V1.5	--- FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 --- FCS_CKM.4	--- FCS_CKM.1/RSA_KeyPair --- FCS_CKM.4
13	FCS_COP.1/SIG-GEN_PKCS #1 V2.1	--- FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 --- FCS_CKM.4	--- FCS_CKM.1/RSA_KeyPair --- FCS_CKM.4
14	FCS_COP.1/SIG-GEN_9796	--- FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 --- FCS_CKM.4	--- FCS_CKM.1/RSA_KeyPair --- FCS_CKM.4
15	FCS_COP.1/SIG-VER_9796	--- FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 --- FCS_CKM.4	--- FCS_CKM.1/RSA_KeyPair --- FCS_CKM.4
16	FCS_COP.1 / DEC_PKCS#1 v1.5	--- FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 --- FCS_CKM.4	--- FCS_CKM.1/RSA_KeyPair --- FCS_CKM.4
17	FCS_COP.1 / DEC_PKCS#1 v2.1	--- FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 --- FCS_CKM.4	--- FCS_CKM.1/RSA_KeyPair --- FCS_CKM.4
18	FCS_COP.1/ RSA_RAW	--- FDP_ITC.1 or FDP_ITC.2 or	--- FCS_CKM.1/RSA_KeyPair

#	Security Functional Requirement	Dependencies	Fulfilled by security requirements in this PP
		FCS_CKM.1 --- FCS_CKM.4	--- FCS_CKM.4
19	FCS_RNG.1	None	----
20	FDP_ACC.1/Data	--- FDP_ACF.1/Data	--- FDP_ACF.1/Data
21	FDP_ACC.1/FUN	--- FDP_ACF.1/FUN	--- FDP_ACF.1/FUN
22	FDP_ACF.1/Data	--- FDP_ACC.1/Data --- FDP_MSA.3	--- FDP_ACC.1/Data --- Not fulfilled but justified. See Explanation 4
23	FDP_ACF.1/FUN	--- FDP_ACC.1/Data --- FDP_MSA.3	--- FDP_ACC.1/Data --- Not fulfilled but justified. See Explanation 7
24	FDP_UCT.1	--- FTP_ITC.1 or FTP_TRP.1 --- FDP_ACC.1 orFDP_IFC.1	--- Not fulfilled but justified. See Explanation 5 --- FDP_ACC.1
25	FDP_UIT.1	--- FDP_ACC.1 or FDP_IFC.1 --- FTP_ITC.1 or FTP_TRP.1	--- FDP_ACC.1 --- Not fulfilled but justified. See Explanation 5
26	FDP_IFC.1	--- FDP_IFF.1	--- Not fulfilled but justified. See Explanation 6
27	FDP_ITT.1	--- FDP_IFC.1	--- FDP_IFC.1
28	FDP_SDI.1/HW	None	----
29	FDP_SDI.2/HW	None	----
30	FDP_SDI.2/EOS	None	----
31	FIA_AFL.1/PIN	--- FIA_UAU.1	--- FIA_UAU.1
32	FIA_AFL.1/ACT	--- FIA_UAU.1	--- FIA_UAU.1
33	FIA_AFL.1/PER	--- FIA_UAU.1	--- FIA_UAU.1
34	FIA_AFL.1/INI	--- FIA_UAU.1	--- FIA_UAU.1
35	FIA_API.1	None	----
36	FIA_UAU.1	--- FIA_UID.1	--- FIA_UID.1
37	FIA_UAU.4	None	----
38	FIA_UAU.5	None	----

#	Security Functional Requirement	Dependencies	Fulfilled by security requirements in this PP
39	FIA_UAU.6	None	----
41	FMT_LIM.1	--- FMT_LIM.2	--- FMT_LIM.2
42	FMT_LIM.2	--- FMT_LIM.1	--- FMT_LIM.1
43	FMT_SMF.1	None	----
44	FMT_SMR.1	--- FIA_UID.1	--- FIA_UID.1
45	FMT_MOF.1	--- FMT_SMR.1 --- FMT_SMF.1	--- FMT_SMR.1 --- FMT_SMF.1
46	FMT_MSA.1	--- FDP_ACC.1 or FDP_IFC.1 --- FMT_SMR.1 --- FMT_SMF.1	--- FDP_ACC.1 --- FMT_SMR.1 --- FMT_SMF.1
47	FMT_MTD.1/INI_PER_AUTH_DATA	--- FMT_SMR.1 --- FMT_SMF.1	--- FMT_SMR.1 --- FMT_SMF.1
48	FMT_MTD.1/INI_PER_AUTH_DATA_Change	--- FMT_SMR.1 --- FMT_SMF.1	--- FMT_SMR.1 --- FMT_SMF.1
49	FMT_MTD.1/Keys_and_AC_Rules_Write_and_Change	--- FMT_SMR.1 --- FMT_SMF.1	--- FMT_SMR.1 --- FMT_SMF.1
50	FMT_MTD.1/PuK_Keys_Use	--- FMT_SMR.1 --- FMT_SMF.1	--- FMT_SMR.1 --- FMT_SMF.1
51	FMT_MTD.1/PrK_Use	--- FMT_SMR.1 --- FMT_SMF.1	--- FMT_SMR.1 --- FMT_SMF.1
52	FMT_MTD.1/PIN_Management	--- FMT_SMR.1 --- FMT_SMF.1	--- FMT_SMR.1 --- FMT_SMF.1
53	FPT_EMSEC.1	None	----
54	FPT_TST.1	None	----
55	FPT_FLS.1	None	----
56	FPT_ITT.1	None	----
57	FPT_PHP.3	None	----
58	FRU_FLT.2	FPT_FLS.1	FPT_FLS.1

Explanation 1: A key does not exist here since a hash function does not use key(s).

Explanation 2: TDES keys are used for initialization and personalization agent authentication. They are written to the TOE during activation phase. Activation phase takes place within the secure environment. So FDP_ITC.1 or FDP_ITC.2 is justified by environmental countermeasures.

Explanation 3: TDES keys are used for initialization and personalization agent authentication. They are written during the activation subphase and destruction is not needed.

Explanation 4: The TSF denies access to the objects unless their security attributes are defined. So FMT_MSA.3 is not a required for SFR FDP_ACF.1/Data properly functioning.

Explanation 5: There is only one communication channel between the TOE and the outer world. So FDP_UIT.1 and FDP_UCT.1 does not require FTP_ITC.1 and FTP_TRC.1.

Explanation 6: Security attributes are necessary for making security related decisions. Since FDP_IFC.1 applies to all data, here neither decision nor a security attribute is required. Hence there is no need to FDP_IFF.1 for FDP_IFC.1 properly functioning.

Explanation 7: Theaccesscontrol TSF according to FDP_ACF.1 usessecurityattributeshavingbeendefinedduringthemanufacturingandfixedoverthewhole life time of the TOE. No management of these security attributes (i.e. FMT_MSA.3) is necessary here.

7.4.2 SECURITY ASSURANCE REQUIREMENTS DEPENDENCIES

Security assurance level is EAL 4+ with added components AVA_VAN.5 and ALC_DVS.2. EAL4 is itself internally consistent. The dependencies of AVA_VAN.5 and ALC_DVS.2 are given below

Table11. Composite TOE SAR Dependencies

Component	Dependencies	Fulfilled or not
AVA_VAN.5	ADV_ARC.1 ADV_FSP.4 ADV_TDS.3 ADV_IMP.1 AGP_OPE.1 AGD_PRE.1 ATE_DPT.1	All dependencies are fulfilled by EAL4.
ALC_DVS.2	None	----

7.5 SECURITY FUNCTIONAL REQUIREMENTS RATIONALE

OT.Physical_Probing:

The scenario of physical probing as described for this objective is explicitly included in the assignment chosen for the physical tampering scenarios in FPT_PHP.3.Therefore, it is clear that this security functional requirement supports the objective.

OT.Physical_Manipulation:

The scenario of physical manipulation as described for this objective is explicitly included in the assignment chosen for the physical tampering scenarios inFPT_PHP.3. Therefore, it is clear that this security functional requirement supports the objective.

The security functional requirement FPT_TST.2 will detect attempts to conduce a physical manipulation on the monitoring functions of the TOE. The objective of FPT_TST.2 is OT.Phys-Manipulation. The physical manipulation will be tried to overcome security enforcing functions.

OT.Leakage_Inherent:

The refinements of the security functional requirements FPT_ITT.1 and FDP_ITT.1 together with the FDP_IFC.1 explicitly require the prevention of disclosure of secret data (TSF data as well as user data) when transmitted between separate parts of the TOE or while being processed. This includes that attackers cannot reveal such data by measurements of emanations, power consumption or other behavior of the TOE while data are transmitted between or processed by TOE parts.

Embedded Operating System has added operations to TOE, PIN verification and CMAC operation. T.Lekage_Inherent is also valid for these operations. FPT_EMSEC.1 handles these added operations and adds refinements to protect the TSF data used by cryptographic operations.

OT.Leakage_Forced:

This objective is directed against attacks, where an attacker wants to force an information leakage, which would not occur under normal conditions. In order to achieve this, the attacker has to combine a first attack step, which modifies the behavior of the TOE (either by exposing it to extreme operating conditions or by directly manipulating it) with a second attack step measuring and analyzing some output produced by the TOE. The first step is prevented by the same mechanisms which support OT.Env_Malfunction and OT.Physical_Manipulation, respectively. The requirements covering OT.Leakage_Inherent also support OT.Leakage_Forced because they prevent the attacker from being successful if he tries the second step directly.

OT.Env_Malfunction:

The definition of this objective shows that it covers a situation, where malfunction of the TOE might be caused by the operating conditions of the TOE (while direct manipulation of the TOE is covered

OT.Physical_Manipulation). There are two possibilities in this situation: Either the operating conditions are inside the tolerated range or at least one of them is outside of this range. The second case is covered by FPT_FLS.1, because it states that a secure state is preserved in this case. The first case is covered by FRU_FLT.2 because it states that the TOE operates correctly under normal (tolerated) conditions.

OT.Abuse_Function:

This objective states that abuse of functions (especially provided by the IC Dedicated Test Software, for instance in order to read secret data) must not be possible in Phase 7 of the life-cycle. There are two possibilities to achieve this: (i) They cannot be used by an attacker (i. e. its availability is limited) or (ii) using them would not be of relevant use for an attacker (i. e. its capabilities are limited) since the functions are designed in a specific way. The first possibility is specified by FMT_LIM.2 and the second one by FMT_LIM.1. Since these requirements are combined to support the policy, which is suitable to fulfill OT.Abuse_Function both security functional requirements together are suitable to meet the objective.

OT.RND:

FCS_RNG.1 requires the TOE to provide random numbers of good quality. To specify the exact metric is left to the individual Security Target for a specific TOE. Other security functional requirements, which prevent physical manipulation and malfunction of the TOE (FDP_ITT.1, FPT_ITT.1, FDP_IFC.1, FRU_FLT.2, FPT_FLS.1, FPT_PHP.3) support this objective because they prevent attackers from manipulating or otherwise affecting the random number generator.

OT.Identification_and_Authentication:

OT.Identification_and_Authentication addresses the identification and authentication mechanisms to counter masquerade attacks and implement the identification and authentication policy. FIA_UAU.5 and FIA_API.1 require the authentication mechanisms that the TOE must have.FAU_SAS.1supports this objective by requiring the TOE to have unique and unchangeable serial number. AKİS v2.2.8I also provides an interface for the application developer to read this serial number. FIA_UAU.4 protects the role and terminal authentication mechanisms against replay attacks and iterates of FIA_AFL.1 protect against the false PIN or authentication data tries. FDP_UCT.1 and FDP_UIT.1also covers the protection of integrity and confidentiality of the data shared. FCS_RNG.1 provides random number for key generation. They provide replay protection against replay attack for PIN authentication. FIA_UAU.6 requires the TOE to re authenticate the users after each command sent and after each reset or power-up. Finally, FCS_COP.1/SIG-GEN_9796, FCS_COP.1/SIG-VER_9796 and FCS_COP.1/RSA_RAW provide cryptographic mechanism for device and role authentication.

OT.Access_Control:

OT.Access_Control addresses user data protection against unauthorized access through logical paths. Physical paths are covered by OT.Physical_Probing and OT.Physical_Manipulation objectives. FIA_UID.1 and FIA_UAU.1 protects the user data from accessing without identification and authentication. FDP_ACC.1/Data, FDP_ACC.1/FUN, FDP_ACF.1/Data and FDP_ACF.1/FUN together require the enforcement of Application access control Policy.

OT.Security_Management:

Goal of OT.Security_Management is only authorized entities who are determined by application owner can manage the TSF and TSF data. FIA_UAU.1 and FIA_UID.1 limits the actions that can be done without identification and authentication. FMT_MOF.1 and FMT_MSA.1 enables the application determined entities to change to behavior of TSF and security attributes of assets.

The SFRS; FMT_MTD.1/ INI_PER_AUTH_DATA, FMT_MTD.1/ INI_PER_AUTH_DATA_Change, FMT_MTD.1/ Keys_and_AC_Rules_Write_and_Change, FMT_MTD.1/PuK_Keys_Use, FMT_MTD.1/PrK_Use, FMT_MTD.1/PIN_Management address the mechanisms to manage the TSF Data.

FMT_SMF.1 and FMT_SMR.1 address the management functions and roles to be implemented within the TOE.

OT.Cryptographic_Operations:

Objective OT.Cryptographic_Operations covers the security services and security functions that the TOE will have. The SFRs: FCS_CKM.1/RSA_KeyPair, FCS_CKM.4, FCS_COP.1/SHA, FCS_COP.1/TDES, FCS_COP.1/SIG-GEN_PKCS#1 V1.5, FCS_COP.1/SIG-GEN_PKCS #1 V2.1, FCS_COP.1/SIG-GEN_9796, FCS_COP.1/SIG-VER_9796, FCS_COP.1/DEC_PKCS#1 V1.5, FCS_COP.1/DEC_PKCS#1 V2.1 OAEP, FCS_COP.1/RSA_RAW FCS_COP.1/AES, FCS_COP.1/CMAC, FCS_RNG.1, totally cover the OT.Cryptographic_Operations. Protection against SPA, DFA and DPA are addressed within the OT.Leakage_Inherent.

OT.Secure_Communication:

Objective OT.Secure_Communication covers the protection of communication between the TOE and the external world. To fulfill this objective TOE, generates Secure Messaging Keys with the SFRs FCS_CKM.1/SM, FCS_CKM.1/SM_PER-INI and distributes them with the SFRs FCS_CKM.2/SM, FCS_CKM.2/SM_PER-INI. FCS_COP.1/AES, FCS_COP.1/CMAC provides cryptographic functions for encryption and integrity/authenticity protection of messages. FDP_UCT.1 and FDP_UIT.1 covers the protection of integrity and confidentiality of the data shared. FCS_RNG.1 provides random number for key generation. And finally FIA_UAU.6 requires the authentication of each message sent between the TOE and the external world.

OT.Storage_Integrity:

The security functional requirement —Stored data integrity monitoring (FDP_SDI.1/HW) requires the implementation of an Error Detection (EDC) algorithm which detects integrity errors of the data stored in all memories. By this the malfunction of the TOE using corrupt data is prevented. Therefore FDP_SDI.1/HW is suitable to meet the security objective.

The security functional requirement —Stored data integrity monitoring and action (FDP_SDI.2/HW) requires the implementation of an integrity observation and correction which is implemented by the Error Detection (EDC) and Error Correction (ECC) measures. The EDC is present throughout all memories of the Security IC while the ECC is realized in the Infineon® SOLID FLASH™. Embedded OS also requires the implementation of an integrity observation mechanism which is implemented by the Error Detection (EDC) for critical user data. In case of any integrity anomalies, TOE detects and inform by an error code. Therefore FDP_SDI.2/HW is suitable to meet the security objective. Embedded OS provides the same mechanism for integrity critical TSF data. Therefore FPT_TST.1 is also suitable to meet this security objective.

Table12. Coverage of TOE Objectives by SFRs

Security Functional Requirement	OT.Physical_Probing	OT.Physical_Manipulation	OT.Leakage_Inherent	OT.Leakage_Forced	OT.Env_Malfunction	OT.Abuse_Function	OT.RND	OT.Identification_and_Authentication	OT.Access_Control	OT.Security_Management	OT.Cryptographic_Operations	OT.Secure_Communication	OT.Storage_Integrity
FAU_SAS.1								✓					
FCS_CKM.1/SM												✓	
FCS_CKM.1/SM_PER-INI												✓	
FCS_CKM.1/RSA_KeyPair											✓		
FCS_CKM.2/SM												✓	
FCS_CKM.2/SM_PER-INI												✓	
FCS_CKM.4											✓		
FCS_COP.1/SHA-1											✓		
FCS_COP.1/SHA-2											✓		
FCS_COP.1/AES											✓	✓	
FCS_COP.1/TDES											✓		
FCS_COP.1/CMAC											✓	✓	
FCS_COP.1/SIG-GEN_PKCS#1 V1.5											✓		
FCS_COP.1/SIG-GEN_PKCS #1 V2.1											✓		
FCS_COP.1/SIG-GEN_9796								✓			✓		
FCS_COP.1/SIG-VER_9796								✓			✓		
FCS_COP.1/DEC_PKCS#1 V1.5											✓		
FCS_COP.1/DEC_PKCS#1 V2.1 OAEP											✓		
FCS_COP.1/RSA_RAW								✓			✓		
FCS_RNG.1							✓				✓	✓	
FDP_ACC.1/Data									✓				
FDP_ACC.1/Function									✓				
FDP_ACF.1/Data									✓				
FDP_ACF.1/Function									✓				
FDP_UCT.1												✓	

Security Functional Requirement	OT.Physical_Probing	OT.Physical_Manipulation	OT.Leakage_Inherent	OT.Leakage_Forced	OT.Env_Malfunction	OT.Abuse_Function	OT.RND	OT.Identification_and_Authentication	OT.Access_Control	OT.Security_Management	OT.Cryptographic_Operations	OT.Secure_Communication	OT.Storage_Integrity
FDP_UIT.1							✓					✓	
FDP_IFC.1			✓	✓			✓						
FDP_ITT.1			✓	✓									
FDP_SDI.1/HW					✓								✓
FDP_SDI.2/HW					✓								✓
FDP_SDI.2/EOS					✓								✓
FIA_AFL.1/PIN								✓					
FIA_AFL.1/ACT								✓					
FIA_AFL.1/PER								✓					
FIA_AFL.1/INI								✓					
FIA_API.1								✓					
FIA_UAU.1									✓	✓			
FIA_UAU.4								✓					
FIA_UAU.5								✓					
FIA_UAU.6										✓		✓	
FIA_UID.1									✓	✓			
FMT_LIM.1						✓							
FMT_LIM.2						✓							
FMT_SMF.1										✓			
FMT_SMR.1										✓			
FMT_MOF.1										✓			
FMT_MSA.1										✓			
FMT_MTD.1/INI_PER_AUTH_DATA										✓			
FMT_MTD.1/INI_PER_AUTH_DATA_Change										✓			
FMT_MTD.1/Keys_and_AC_Rules_Write_and_Change										✓			
FMT_MTD.1/PuK_Keys_Use										✓			
FMT_MTD.1/PrK_Use										✓			
FMT_MTD.1/PIN_Manageme										✓			

Security Functional Requirement	OT.Physical_Probing	OT.Physical_Manipulation	OT.Leakage_Inherent	OT.Leakage_Forced	OT.Env_Malfunction	OT.Abuse_Function	OT.RND	OT.Identification_and_Authentication	OT.Access_Control	OT.Security_Management	OT.Cryptographic_Operations	OT.Secure_Communication	OT.Storage_Integrity
nt													
FPT_EMSEC.1			✓										
FPT_FLS.1				✓	✓		✓						
FPT_ITT.1			✓	✓			✓						
FPT_PHP.3	✓	✓		✓			✓						
FPT_TST.1													✓
FPT_TST.2		✓											
FRU_FLT.2				✓	✓		✓						

7.6 SECURITY ASSURANCE REQUIREMENTS RATIONALE

An assurance level of EAL4 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. This evaluation assurance package was selected to permit a developer to gain maximum assurance from positive security engineering based on good commercial practices. In order to provide a meaningful level of assurance that the TOE provides an adequate level of defense against such attacks, the evaluators should have access to the detailed design knowledge and source code.

8 TOE SUMMARY SPECIFICATION

AKİS v2.2.8Iis the ***composite product*** consisting of Embedded Operating System and the Security IC. Some of the security features are provided mainly by Security IC and supported Embedded Operating system. Some of the security features are provided mainly by Embedded Operating system and supported by Security IC. A brief overview will be given for all Security Features. A detailed description also will be provided for the Security Features provided by Embedded Operating system. For the detailed information about security features provided by Security IC, Security IC ST[2][14]can be checked.

Security Features Provided mainly by IC and supported Embedded OS:

- SF_PS Protection against Snooping
- SF_PMA Protection against Modification Attacks
- SF_DPM Device Phase Management

Security Features Provided mainly by Embedded OS and supported IC:

- SF_IA Identification and Authentication
- SF_SMAC Security Management and access control
- SF_SM Secure Messaging
- SF_CSUP Cryptographic Support

8.1 SF_PS: PROTECTION AGAINST SNOOPING

Protection against snooping security feature is mainly inherited to the Security IC part of composite product AKİS v2.2.8I. For the detailed information Security IC ST can be checked. Added SFR with respect to security IC is the FPT_EMSEC.1.

Covered SFRs are FPT_PHP.3, FDP_IFC.1, FPT_ITT.1, FDP_ITT.1, FPT_FLS.1, and FPT_EMSEC.1.

8.2 SF_PMA: PROTECTION AGAINST MODIFICATION ATTACKS

Protection against modification attacks security feature is inherited to the composite product AKİS v2.2.8Ifrom the Security IC. For the detailed information Security IC ST can be checked.

Covered SFRs are: FDP_IFC.1, FDP_ITT.1, FDP_SDI.2/HW, FDP_SDI.2/EOS, FPT_FLS.1, FRU_FLT.2, FPT_PHP.3, FPT_ITT, FPT_TST.2, and FPT_TST.1.

8.3 SF_DPM: DEVICE PHASE MANAGEMENT

Device phase management security feature is fulfilled by Security IC and embedded operating system.

Covered SFRs are FAU_SAS.1, FMT_LIM.1, FMT_LIM.2, FDP_ITT.1, FPT_ITT.1.

AKİS v2.2.8Icomposite product may be given to Consumer before personalization. TOE provides also phase management for the sub phases defined in 1.5.4.1. TSF restricts TOE functions according to these phase management.

Covered SFRs are FDP_ACC.1/FUN and FDP_ACF.1/FUN.

8.4 SF_CSUP:CRYPTOGRAPHIC SUPPORT

The Hardware provides many cryptographic operations as detailed in HW ST. Composite TOE adds more cryptographic operations. They are RSA Key Pair Generation, Signature Verification and Generation, TDES decryption. The keys that represent confidential information are destructed after use. Covered SFRs are FCS_CKM.1/RSA_KeyPair, , FCS_COP.1/SHA, FCS_COP.1/AES, FCS_COP.1/TDES, FCS_COP.1/CMAC, FCS_COP.1/SIG-GEN_PKCS#1 V1.5, FCS_COP.1/SIG-GEN_PKCS #1 V2.1, FCS_COP.1/SIG-GEN_9796, FCS_COP.1/SIG-VER_9796, FCS_COP.1/DEC_PKCS#1 V1.5, FCS_COP.1/DEC_PKCS#1 V2.1 OAEP, FCS_COP.1/RSA_RAW.

The hardware provides true random number generation as detailed in HW ST. EOS uses hardware function to produce random numbers. With this property FCS_RNG.1 is covered.

8.5 SF_IA: IDENTIFICATION AND AUTHENTICATION

The SF.IA includes the authentication mechanisms of activation agent authentication, initialization and personalization agent authentication, chip (terminal) authentication[177] and PIN verification mechanisms. Activation agent authentication, Initialization and personalization agent authentication and PIN verification mechanisms include authentication failure handling. Role and chip (terminal) authentication mechanisms use single user authentication and therefore protected against replay attacks. PIN authentication mechanism is protected against replay attack by secure messaging capabilities. Other authentications are performed in secure environment as assumed in section 4.5.

177Terminal authentication is providedby PIN authenticationfor SAM configuration.

Covered SFRs are FIA_AFL.1/PIN, FIA_AFL.1/ACT, FIA_AFL.1/PER, FIA_AFL.1/INI, FIA_API.1, FIA_UAU.4, FIA_UAU.5.FCS_COP.1/SIG-GEN_9796, FCS_COP.1/SIG-VER_9796, FCS_COP.1/RSA_RAW, FDP_UIT.1, FDP_UCT.1 and FCS_RNG.1.

8.6 SF_SMAC: SECURITY MANAGEMENT ANDACCESS CONTROL

SMAC is the short form of Security Management and access control. The TOE includes security mechanisms to control access to TSF data and user data and also controls access to the TSF Interface. Security access rules are configurable by the application. Even application may allow these rules to be modified during operational phase. AKİS v2.2.8Iprovides application owners a flexible access control and security management mechanism. Covered SFRs are FIA_UID.1, FIA_UAU.1, FDP_ACC.1/Data, FDP_ACF.1/Data, FMT_MTD.1/INI_PER_AUTH_DATA, FMT_MTD.1/INI_PER_AUTH_DATA_Change, FMT_MTD.1/Keys_and_AC_Rules_Write_and_Change, FMT_MTD.1/PuK_Keys_Use, FMT_MTD.1/PrK_Use, FMT_MTD.1/PIN_Management,FMT_MSA.1. These SFRs arrange the access control of the TSF Data and user data.

The other SFR covered is FMT_MOF.1 which requires the access to TSFI is also manageable by the application allowed users.

Remaining SFRs covered by SF.SMAC are FMT_SMF.1 and FMT_SMR.1 which require the management functions and management roles. Preoperational roles are activation agent, initialization agent, and personalization agents. Besides supporting these roles, AKİS v2.2.8Iallows application owner to define additional management roles that active in the operational phase.

8.7 SF_SM: SECURE MESSAGING

The TOE has SF.SM which allows the TOE communicates with the external world securely. SF.SM protects the confidentiality and authenticity of the messages going between the card and the external world. Covered SFRs are FCS_CKM.1/SM, FCS_CKM.1/SM_PER-INI, FCS_CKM.2/SM, FCS_CKM.2/SM_PER-INI, FDP_UCT.1, FDP_UIT.1, FIA_UAU.6,FCS_COP.1/AES, FCS_COP.1/CMAC, FCS_RNG.1.

8.8 SECURITY FUNCTIONS RATIONALE

Table13shows the assignment of security functional requirements to TOE's security functionality.

Table13. Coverage of SFRs by TOE Security Functions

Security Functional Requirement	SF_DPM	SF_PS	SF_PMA	SF_IA	SF_SMAC	SF_SM	SF_CSUP
FAU_SAS.1				✓			
FCS_CKM.1/SM						✓	
FCS_CKM.1/SM_PER-INI						✓	
FCS_CKM.1/RSA_KeyPair							✓
FCS_CKM.2/SM						✓	
FCS_CKM.2/SM_PER-INI						✓	
FCS_CKM.4							✓
FCS_COP.1/SHA							✓
FCS_COP.1/AES						✓	✓
FCS_COP.1/TDES							✓
FCS_COP.1/CMAC						✓	✓
FCS_COP.1/SIG-GEN_PKCS#1 V1.5							✓
FCS_COP.1/SIG-GEN_PKCS #1 V2.1							✓
FCS_COP.1/SIG-GEN_9796				✓			
FCS_COP.1/SIG-VER_9796				✓			
FCS_COP.1/DEC_PKCS#1 V1.5							✓
FCS_COP.1/DEC_PKCS#1 V2.1 OAEP							✓
FCS_COP.1/RSA_RAW				✓			
FCS_RNG.1						✓	✓
FDP_ACC.1/Data					✓		
FDP_ACC.1/FUN	✓						
FDP_ACF.1/Data					✓		
FDP_ACF.1/FUN	✓						
FDP_UCT.1						✓	
FDP_UIT.1						✓	
FDP_IFC.1		✓	✓				
FDP_ITT.1	✓	✓	✓				
FDP_SDI.1/HW			✓				
FDP_SDI.2/HW			✓				

Security Functional Requirement	SF_DPM	SF_PS	SF_PMA	SF_IA	SF_SMAC	SF_SM	SF_CSUP
FDP_SDI.2/EOS			✓				
FIA_AFL.1/PIN				✓			
FIA_AFL.1/ACT				✓			
FIA_AFL.1/PER				✓			
FIA_AFL.1/INI				✓			
FIA_API.1				✓			
FIA_UAU.1					✓		
FIA_UAU.4				✓			
FIA_UAU.5				✓			
FIA_UAU.6						✓	
FIA_UID.1					✓		
FMT_LIM.1	✓						
FMT_LIM.2	✓						
FMT_SMF.1					✓		
FMT_SMR.1					✓		
FMT_MOF.1					✓		
FMT_MSA.1					✓		
FMT_MTD.1/INI_PER_AUTH_DATA					✓		
FMT_MTD.1/INI_PER_AUTH_DATA_Change					✓		
FMT_MTD.1/Keys_and_AC_Rules_Write_and _Change					✓		
FMT_MTD.1/PuK_Keys_Use					✓		
FMT_MTD.1/PrK_Use					✓		
FMT_MTD.1/PIN_Management					✓		
FPT_EMSEC.1		✓					
FPT_FLS.1		✓	✓	✓			
FPT_ITT.1	✓	✓	✓				
FPT_PHP.3		✓	✓				
FPT_TST.1			✓				
FPT_TST.2		✓	✓				
FRU_FLT.2			✓	✓			

9 STATEMENT OF COMPATIBILITY

This is the statement of compatibility between the current Composite Security Target and the Security Target of the underlying hardware.

9.1 RELEVANCE OF HARDWARE TSF

9.1.1 RELEVANT TSF

- SF_DPM Device Phase Management
- SF_PS Protection against Snooping
- SF_PMA Protection against Modification Attacks
- SF_CS Cryptographic Support

9.1.2 NOT RELEVANT TSF

- SF_PLA Protection against Logical Attacks

9.2 COMPATIBILITY: TOE SECURITY ENVIRONMENT (ASSUMPTIONS, THREATS, OSPS, SOS)

9.2.1 ASSUMPTIONS

9.2.1.1 ASSUMPTIONS FOR THE COMPOSITE TOE

Table14. Composite TOE Assumptions - Compatibility Statement

#	Assumption Name	Rationale
1.	A.Secure_Application	no conflict
2.	A.Key_and_Certificate_Security	no conflict
3.	A.PIN_Handling	no conflict
4.	A.Personnel_Security	no conflict
5.	A.Pre-	no conflict

	Operational_Environment	

9.2.1.2 ASSUMPTIONS FOR THE SECURITY IC PP

The section below describes the validity and compensation of defined assumptions in hardware PP/ST.

A.Process-Sec-IC (Protection during Packaging, Finishing and Personalization)

This is relevant until the personalization of the hardware (TOE Initialization) the assumption A.Process-Sec-IC covers the secure handling of the SC from the delivery by the hardware manufacturer to the developer until the completion of the TOE. This assumption is regarded as being relevant, but not significant, because the content of this assumption is examined during the examination of the assurance families ALC_DEL and ALC_DVS. This assumption is no more required for Composite TOE and is therefore not included into this Composite ST.

A.Plat-Appl (Usage of Hardware Platform)

This is relevant during TOE development. The assumption A.Plat-Appl assumes that the Smartcard embedded operating system securely uses the hardware, taking into account the hardware user guidance and the hardware evaluation. This assumption is regarded as being relevant, but not significant, because the content of this assumption is examined during the examination of the assurance family ADV_COMP. That corresponds to the achievement of the security objectives e.g. OT.Malfunction, OT.Phys-Manipulationin the TOE end usage. This assumption is not required for Composite TOE and is therefore not included into this Composite-ST.

A.Resp-Appl (Treatment of user data)

This assumption is covered by the TOE's objective related to TOE's Life Cycle Phase 1 "Development". It is supported by the Security Objectives OT.Access_Control, OT.Identification_and_Authentication.

Table15. Security IC PP Assumptions - Compatibility Statement

#	Assumptions	Rationale
1	A.Process-Sec-IC	covered by ALC_DEL and ALC_DVS
2	A.Plat-Appl	covered by and ADV_COMP of composite TOE
3	A.Resp-Appl	covered by OT.Access_Control, OT.Identification_and_Authentication of the composite TOE ST

9.2.1.3 ADDITIONAL ASSUMPTIONS FOR THE SECURITY IC ST TO THE SECURITY IC PP

A.Key-Function (Usage of Key-dependent Functions)

Key-dependent functions (if any) shall be implemented in the Smartcard embedded operating system in a way that they are not susceptible to leakage attacks (as described under T.Lekage_Inherent and T.Leakage_Forced.) This assumption is covered by the TOE's objectives OT.Leakage_Inherent and OT.Leakage_Forced

Table16. Security IC ST Assumptions - Compatibility Statement

#	Assumptions	Rationale
1	A.Key-Function (Usage of Key-Dependent Functions)	covered by OT.Leakage_Inherent OT.Leakage_Forced of composite TOE

9.2.2 THREATS

9.2.2.1 THREATS FOR THE COMPOSITE TOE

Table17. Composite TOE Threats - Compatibility Statement

#	Threat Name	Rationale
1.	T.Physical_Probing	matches the threat T.Phys-Probing of the IC PP
2.	T.Physical_Manipulation	matches the threat T.Phys-Manipulation of the IC PP
3.	T.Lekage_Inherent	matches the threat T.Leak-Inherent of the IC PP
4.	T.Leakage_Forced	matches the threat T.Leak-Forced of the IC PP
5.	T.Env_Malfunction	matches the threat T.Malfunction of the IC PP
6.	T.Abuse_Function	matches the threat T.Abuse-Func of the IC PP
7.	T.RND	matches the threat T.RND of the IC PP
8.	T. Eavesdropping	no conflict

9.	T.Session_Hijacking	no conflict
10.	T.Man_in_The_Middle	no conflict
11.	T.Skimming	no conflict
12.	T.Counterfiting	no conflict
13.	T.Unauthorised_Access	no conflict
14.	T.Unauthorised_Management	no conflict

9.2.2.2 THREATS FOR THE SECURITY IC PP

Table18. Security IC PP Threats - Compatibility Statement

#	Threat Name	Rationale
1.	T.Phys-Manipulation	matches the threat of the T.Physical_Manipulation of the composite TOE
2.	T.Phys-Probing	matches the threat of the T.Physical_Probing of the composite TOE
3.	T.Malfunction	matches the threat of the T.Env_Malfunction of the composite TOE
4.	T.Leak-Inherent	matches the threat of the T.Lekage_Inherentof the composite TOE
5.	T.Leak-Forced	is covered by the threats T.Leakage_Forced of the composite TOE
6.	T.Abuse-Func	covered byte threat T.Abuse_Functionof the composite TOE
7.	T.RND	covered by the threats T.RND, T.Env_Malfunction and T.Physical_Manipulation of the composite TOE.

9.2.2.3 ADDITIONAL THREATS FOR THE SECURITY IC ST TO THE SECURITY IC PP

Table19. Security IC ST Threats - Compatibility Statement

#	Threat Name	Rationale
8.	T.Mem-Access	not relevant

Application Note 18: This threat valid for multiple applications implemented on single hardware. There is only one application (Embedded Operating System) for composite TOE.

9.2.3 OSPS

9.2.3.1 OSPS FOR THE COMPOSITE TOE

Table20. Composite TOE OSPs - Compatibility Statement

#	Policy Name	Rationale
1.	P.Identification_and_Authentication	covers P.Process-TOE and P.Add-Functions (RSA),
2.	P.PKI	no conflict
3.	P.Access_Control	no conflict
4.	P.PreOperational_Security_Management	no conflict
5.	P.Operational_Security_Management	no conflict
6.	P.Cryptographic_Operations	covers P.Add-Functions(TDES, AES, RSA, RSA KeyPair, SHA-256),

9.2.3.2 OSPS FOR THE SECURITY IC PP

Table21. Security IC PP OSPs - Compatibility Statement

#	Policy Name	Rationale
1.	P.Process-TOE	covered by P.Identification_and_Authentication

9.2.3.3 ADDITIONAL OSPS FOR THE SECURITY IC ST TO THE SECURITY IC PP

Table22. Security IC ST OSPs - Compatibility Statement

#	Policy Name	Rationale
1.	P.Add-Functions	The TOE' hardware provides the following specific security functionality to the Smartcard embedded operating system: Advanced Encryption Standard, Triple Data Encryption Standard Rivest-Shamir-Adleman Cryptography, Secure Hash Algorithm SHA-2. They covered by P.Identification_and_Authentication and P.Cryptographic_Operations, T. Eavesdropping, T.Session_Hijacking T.Man_in_The_Middle. Elliptic Curve Cryptography is not relevant for composite ST.

9.2.4 SECURITY OBJECTIVES FOR THE TOE

9.2.4.1 SECURITY OBJECTIVES FOR THE COMPOSITE TOE

Table23. Composite TOE Objectives - Compatibility Statement

#	Security Objective Name	Rationale
1.	OT.Physical_Probing	matches the O.Phys-Probing the of the IC PP
2.	OT.Physical_Manipulation	covers the O.Phys-Manipulation the of the IC PP and partially covers the O.Leak-Forced of the IC PP
3.	OT.Leakage_Inherent	covers the O.Leak- Inherent of the IC PP
4.	OT.Leakage_Forced	covers the O.Leak-Forced of the IC PP
5.	OT.Env_Malfunction	covers the O.Malfunction of the IC PP and partially covers the O.Leak-Forced of the IC PP
6.	OT.Abuse_Function	matches the O.Abuse-Func of the IC PP
7.	OT.Identification_and_Authentication	Partially covers the O.Add-Functions (RSA, Random Number Generation) and O.Identification of the IC PP

#	Security Objective Name	Rationale
8.	OT.Access_Control	no conflict
9.	OT.Security_Management	no conflict
10.	OT.Cryptographic_Operations	covers the O.Add-Functions (RSA Key Pair, TDES) of the hardware ST
11.	OT.Secure_Communication	covers the O.Add-Functions (AES) of the hardware ST
12.	OT.Storage_Integrity	partially covers the O.Malfunction of the IC PP

9.2.4.2 SECURITY OBJECTIVES FOR THE SECURITY IC PP

Table24. Security IC PP Objectives - Compatibility Statement

#	Security Objective Name	Rationale
1.	O.Phys-Manipulation	covered by the OT.Physical_Manipulation of the composite TOE
2.	O.Phys-Probing	matches the OT.Physical_Probing of the composite TOE
3.	O.Malfunction	covered by the OT.Env_Malfunction of the composite TOE
4.	O.Leak-Inherent	matches the OT.Leakage_Inherent of the composite TOE
5.	O.Leak-Forced	covered by the OT.Leakage_Forced of the composite TOE
6.	O.Abuse-Func	matches the OT.Abuse_Function of the composite TOE
7.	O.RND	covered by the OT.RND, OT.Env_Malfunction and OT.Physical_Manipulation and of the composite TOE
8.	O.Identification	covered by the OT.Identification_and_Authentication

9.2.4.3 ADDITIONAL SECURITY OBJECTIVES FOR THE SECURITY IC ST TO THE SECURITY IC PP

Table25. Security IC ST SOs - Compatibility Statement

#	Security Objective Name	Rationale
1.	O.Add-Functions	covered by the OT.Cryptographic_Operations, OT.Secure_Communication, OT.Identification_and_Authentication
2.	O.Mem-Access	not relevant

9.2.5 SECURITY OBJECTIVES FOR THE ENVIRONMENT

9.2.5.1 SECURITY OBJECTIVES FOR THE COMPOSITE TOE ENVIRONMENT

Table26. Composite TOE for the Environment - Compatibility Statement

#	Security Objective Name	Rationale
1.	OE.PKI	not relevant with platform
2.	OE.Key_and_Certificate_Security	not relevant with platform
3.	OE.PIN_Handling	not relevant with platform
4.	OE.Secure_Application:	not relevant with platform
5.	OE.Personnel_Security:	not relevant with platform
6.	OE.Responsible_Parties:	not relevant with platform

9.2.5.2 SECURITY OBJECTIVES FOR THE SECURITY IC PP ENVIRONMENT

Table27. Security IC PP Objectives for the Environment - Compatibility Statement

#	Security Objective Name	Rationale
7.	OE.Process-Sec-IC	covered by ALC_DEL and ALC_DVS of the platform
8.	OE.Plat-Appl	covered by and ADV_COMP of composite TOE
9.	OE.Resp-Appl	covered by OT.Access_Control, OT.Identification_and_Authentication of the composite TOE ST

9.2.5.3 ADDITIONAL SECURITY OBJECTIVES FOR ENVIRONMENT OF THE SECURITY IC ST TO THE SECURITY IC PP ENVIRONMENT

None

9.3 COMPATIBILITY: SECURITY REQUIREMENTS

9.3.1 SECURITY FUNCTIONAL REQUIREMENTS

9.3.1.1 SFRS OF THE COMPOSITE TOE

Table28. Composite TOE SFRs - Compatibility Statement

#	SFR	Rationale
1.	FAU_SAS.1	matches the FAU_SAS.1 of the Security IC PP.
2.	FCS_CKM.1/SM	not relevant with platform SFRs
3.	FCS_CKM.1/SM_PER-INI	not relevant with platform SFRs
4.	FCS_CKM.1/ RSA_KeyPair	matches FCS_CKM.1/RSA (2048 bit) of the Security IC ST
5.	FCS_CKM.2/SM	not relevant with platform SFRs
6.	FCS_CKM.2/SM_PER-INI	not relevant with platform SFRs

#	SFR	Rationale
7.	FCS_CKM.4	no conflicts
8.	FCS_COP.1/SHA	no conflicts
9.	FCS_COP.1/AES	matches FCS_COP.1/AES (256 bit) of the Security IC ST
10.	FCS_COP.1/TDES	matches FCS_COP.1/3DES (112 bit) of the Security IC ST
11.	FCS_COP.1/CMAC	no conflicts
12.	FCS_COP.1/SIG-GEN_PKCS#1 V1.5	no conflicts
13.	FCS_COP.1/SIG-GEN_PKCS #1 V2.1	no conflicts
14.	FCS_COP.1/SIG-GEN_9796	no conflicts
15.	FCS_COP.1/SIG-VER_9796	no conflicts
16.	FCS_COP.1/DEC_PKCS#1 V1.5	no conflicts
17.	FCS_COP.1/DEC_PKCS#1 V2.1 OAEP	no conflicts
18.	FCS_COP.1/RSA_RAW	matches FCS_COP.1/RSA of the Security IC ST
19.	FCS_RNG.1	matches FCS_RNG.1 of the Security IC ST
20.	FDP_ACC.1/Data	not relevant with platform SFRs
21.	FDP_ACC.1/FUN	not relevant with platform SFRs
22.	FDP_ACF.1/Data	not relevant with platform SFRs
23.	FDP_ACF.1/FUN	not relevant with platform SFRs
24.	FDP_IFC.1	matches the FDP_IFC.1 of the Security IC ST

#	SFR	Rationale
25.	FDP_ITT.1	matches the FDP_ITT.1 of the Security IC ST
26.	FDP_SDI.1/HW	matches the FDP_SDI.1 of the Security IC ST
27.	FDP_SDI.2/HW	matches the FDP_SDI.2 of the Security IC ST
28.	FDP_SDI.2/EOS	not relevant with platform SFRs
29.	FIA_AFL.1/PIN	not relevant with platform SFRs
30.	FIA_AFL.1/ACT	no conflicts
31.	FIA_AFL.1/PER	no conflicts
32.	FIA_AFL.1/INI	no conflicts
33.	FIA_API.1	no conflicts
34.	FIA_UAU.1	not relevant with platform SFRs
35.	FIA_UAU.4	no conflicts
36.	FIA_UAU.5	no conflicts
37.	FIA_UAU.6	no conflicts
38.	FIA_UID.1	not relevant with platform SFRs
39.	FMT_LIM.1	matches the FMT_LIM.1 of the Security IC PP
40.	FMT_LIM.2	matches the FMT_LIM.2 of the Security IC PP
41.	FMT_MOF.1	not relevant with platform SFRs
42.	FMT_MSA.1	not relevant with platform SFRs
43.	FMT_MTD.1/ INI_PER_AUTH_DATA	not relevant with platform SFRs

#	SFR	Rationale
44.	FMT_MTD.1/ INI_PER_AUTH_DATA_Change	not relevant with platform SFRs
45.	FMT_MTD.1/ Keys_and_AC_Rules_Write_and_Change	not relevant with platform SFRs
46.	FMT_MTD.1/PuK_Keys_Use	not relevant with platform SFRs
47.	FMT_MTD.1/PrK_Use	not relevant with platform SFRs
48.	FMT_MTD.1/PIN_Management	not relevant with platform SFRs
49.	FMT_SMF.1	not relevant with platform SFRs
50.	FMT_SMR.1	not relevant with platform SFRs
51.	FPT_EMSEC.1	no conflicts
52.	FPT_TST.1	not relevant with platform SFRs
53.	FPT_TST.2	no conflicts (FPT_TST.2 of the Security IC ST supports)
54.	FPT_FLS.1	matches the FPT_FLS.1 of the Security IC PP
55.	FPT_ITT.1	matches the FPT_ITT.1 of the Security IC PP
56.	FPT_PHP.3	matches the FPT_PHP.3 of the Security IC PP
57.	FRU_FLT.2	matches the FRU_FLT.2 of the Security IC PP

9.3.1.2 SFRS OF THE SECURITY IC PP

Table29. Security IC PP SFRs - Compatibility Statement

No	SFR	
1.	FPT_PHP.3	matches the FPT_PHP.3 of the composite TOE
2.	FRU_FLT.2	matches the FRU_FLT.2 of the composite TOE
3.	FPT_FLS.1	matches the FPT_FLS.1 of the composite TOE
4.	FDP_ITT.1	matches the FDP_ITT.1 of the composite TOE
5.	FPT_ITT.1	matches the FPT_ITT.1 of the composite TOE
6.	FDP_IFC.1	matches the FDP_IFC.1 of the composite TOE
7.	FMT_LIM.1	matches the FMT_LIM.1 of the composite TOE
8.	FMT_LIM.2	matches the FMT_LIM.2 of the composite TOE
9.	FCS_RND.1	matches the FCS_RNG.1 of the composite TOE
10.	FAU_SAS.1	matches the FAU.SAS.1 of the composite TOE

9.3.1.3 ADDITIONAL SFRS OF THE SECURITY IC ST TO IC PP

Table30. Security IC ST SFRs - Compatibility Statement

No	SFR	Rationale
1.	FPT_TST.2	Matches the FPT_TST.2 of the Composite TOE
2.	FDP_ACC.1	not relevant
3.	FDP_ACF.1	not relevant
4.	FMT_MSA.1	not relevant
5.	FMT_MSA.3	not relevant

6.	FMT_SMF.1	not relevant
7.	FCS_COP.1/DES	matches the FCS_COP.1/TDES of the composite TOE
8.	FCS_COP.1/AES	matches the FCS_COP.1/AES of the composite TOE
9.	FCS_COP.1/RSA	matches the FCS_COP.1/RSA_RAW of the composite TOE
10.	FCS_COP.1/ECDSA	not relevant
11.	FCS_COP.1/ECDH	not relevant
12.	FCS_COP.1/SHA	matches the FCS_SHA of the composite TOE
13.	FCS_CKM.1/RSA	matches the FCS_CKM.1/RSA_KeyPair of the Composite TOE
14.	FCS_CKM.1/EC	not relevant
15.	FDP_SDI.1	matches the FDP_SDI.1/HW of the composite TOE
16.	FDP_SDI.2	matches the FDP_SDI.2/HW of the composite TOE

9.3.2 SECURITY ASSURANCE REQUIREMENTS

The level of assurance of the TOE is EAL 4 augmented with AVA_VAN.5 and ALC_DVS.2.

The chosen level of assurance of the hardware is EAL 6 augmented with ALC_DVS.2 and AVA_VAN.5

This shows that the Assurance Requirements of the TOE matches the Assurance Requirements of the hardware.

10 ABBREVIATIONS AND DEFINITIONS

AES: Advanced Encryption Standard

AKİS: Akıllı Kart İşletim Sistemi (Smart Card Operating System)

APDU: Application Packet Data Unit

CPU: Central Processing Unit

DES: Decryption and Encryption Standard

DFA: Differential Fault Analysis

DPA: Differential Power Analysis

EAL: Evaluation Assurance Level

EOS: Embedded Operating System

IC: Integrated Circuit

PP: Protection Profile

PTG2: A class that defines the requirements for RNGs used in key generation, padding bit generation, etc. PTG.2 is defined AIS31[15]

RAM: Random Access Memory

RSA: Ron Rivest, Adi Shamir and Leonard Adleman

ROM: Read Only Memory

SAM: Secure Access Module

SHA: Secure Hash Algorithm

SPA: Simple Power Analysis

SFR: Security Functional Requirement

ST: Security Target

TPDU: Transmission Protocol Data Unit

TOE: Target of Evaluation

11 BIBLIOGRAPHY

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

[2] Security Target for Common Criteria EAL6 augmented (EAL6+) M7892 B11 including optional Software Libraries RSA – EC – SHA2 – Toolbox and comprises the Infineon Technologies Security Controller M7892 b!! with Specific IC Dedicated Software and Optional RSA v1.02.013, EC v1.02.013, SHA-2 v1.01 and Toolbox v1.02.013 libraries; Version 0.8 Date: 2012-08-28

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

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

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

[6] Common Criteria for Information Technology Security Evaluation, Evaluation Methodology; Version 3.1, Revision 4, CCMB-2012-09-004

[7] ISO 1177 Information Processing Character Structure For Start/Stop And Synchronous Character Oriented Transmission

[8] ISO 7816-3 Information Technology – Identification Cards – Integrated Circuits with Contacts Part 3: Electronic Signals and Transmission Protocols - T=1 Protocol

[9] ISO 7816-4Information Technology – Identification Cards – Integrated Circuits with Contacts Part 4: Organization, security and commands for interchange

[10] ISO 7816-8 Information Technology – Identification Cards – Integrated Circuits with Contacts Part 8: Commands For Security Operations

[11] ISO 7816-9 Information Technology – Identification Cards – Integrated Circuits with Contacts Part 9: Commands for card management

[12] AKİS 2 Serisi Yönetici Kullanıcı Kılavuzu, v14, 20.03.2014

[13] AKİS 2 Serisi Kullanıcı Kılavuzu, v14, 20.03.2014

[14] Maintenance Security Target for Common Criteria EAL6 augmented (EAL6+) M7892 B11 Including optional Software Libraries RSA – EC – SHA2 – Toolbox and comprises the Infineon Technologies Security Controller M7892 B11 with Specific IC Dedicated Software

and Optional RSA v1.02.013, EC v1.02.013, SHA-2 v1.01 and Toolbox v1.02.013 libraries; Version 1.4 Date: 2013-08-26

[15] Functionality classes and evaluation methodology for physical random number generators AIS31, Version 2.1, 2011-12-02, Bundesamt für Sicherheit in der Informationstechnik respectively —A proposal for: Functionality classes for random number generators , Version 2.0, 2011-09-18, Wolfgang Killmann, T-Systems GEI GmbH, Werner Schindler, Bundesamt für Sicherheit in der Informationstechnik

[16] Common Criteria Protection Profile Machine Readable Travel Document with ICAO Application, Extended access control, Version 1.10, 25th March. 2009.