Security Target Lite

for

Kapsch SAM 5000

CONTENT

DOCUMENT HISTORY

Version	Issue date	Revision description	Edited by
A	2017-10-24	This is a Lite version of 8633 902-149 G	Stefan Grännö
B	2018-02-08	Appendix B - Referenced Documents: Update of reference to new Crypto Library Chapter 1.2 PBL reference replaced by table of actual TOE references	Stefan Grännö
C	2018-03-02	Appendix B Ref 5 corrected	Stefan Grännö
D	2018-03-21	Updates based on Evaluator feedback	Stefan Grännö

1 ST Introduction

1.1 ST Reference

Title:	Security Target Lite SAM 5000
Version:	D
Date:	2018-03-21
Editor:	Anders Staaf, Combitech AB

1.2 TOE Reference

Target of Evaluation:	SAM 5000
Developer:	Kapsch TrafficCom AB

Version:

Part No.	Name	Product Version
8633 005-601	SAM 5000 M Smart Card	B
8633 005-602	SAM 5000 CS Smart Card	B
8633 005-603	SAM 5000 CS VQFN	B
8633 005-604	SAM 5000 CP Smart Card	B
8633 005-605	SAM 5000 CP VQFN	B
8633 005-606	SAM 5000 TR VQFN	B
8633 005-608	SAM 5000 P Smart Card	B

1.3 Document Overview

This is the Security Target for a high performance low cost Secure Application Module, SAM.

The TOE SW together with its certified platform are below called the TOE as shown in Figure 1. When TOE is used in referenced document, the part marked as TOE SW in Figure 1 including dependencies to the certified platform is referred.

Chapter 1 gives a description of the ST and the TOE. This description serves as an aid to understand the security requirements and the security functions.

Chapter 2 states the conformance claims made.

In chapter 3, the security problem definition of the TOE is described. This includes assumptions about the environment of the TOE, threats against the TOE, TOE environment and organizational security policies that are to be employed to ensure the security of the TOE.

The Security Objectives stated in chapter 4 describes the intent of the Security Functions. The Security Objectives are divided into two groups of security objects, for the TOE and for the TOE environment.

No extended components are defined so chapter 5 is empty.

In chapter 6 the IT security functional and assurance requirements are stated for the TOE. These requirements are a selected subset of the requirements of part 2 and 3 of the Common Criteria standard.

A brief description of how the security functional requirements are implemented in the TOE is described in chapter 7.

1.4 TOE Overview

1.4.1 TOE Type and Usage

The TOE is the Secure Application Module, SAM 5000, a module offering cryptographic functions and a secure storage of keys. SAM 5000 is designed to be used in several different devices in a road tolling system.

1.4.2 Major Security Features

Through its command API interface the TOE provides functionality such as:

- User authentication.
- PIN management
- Key management
- File management
- Encryption, decryption of data
- MAC calculation and verification
- Digital signature calculation and verification
- Status and information functionality

1.4.3 Required non-TOE Software / Hardware / Firmware

The TOE SW depends on the certified platform Infineon Technologies Smart Card IC (Security Controller) M9900 design step A22 and G11 of the SLE97 family on a smart card or the SLI97 family in a VQFN chip package and its operating system and cryptographic library for correct operation, firmware version BOS-V1.

1.5 TOE Description

1.5.1 System Overview

The TOE is to be used for encryption support and secure storage of cryptographic keys in both stationary and on-board deployments. The TOE exists in 5 different versions with different functionality ranging from the Communication Point SAM which has basic cryptographic support to the Master SAM which has extended cryptographic functionality.

1.5.2 Physical Scope

The TOE SW is a software application executing on the Infineon Technologies Smart Card IC (Security Controller) M9900 design step A22 and G11 of the SLE97 family on a smart card or the SLI97 family in a VQFN chip package. The BOS-V1 firmware version is used.

The Infineon device is Common Criteria certified EAL5, augmented by AVA_VAN.5 and ALC_DVS.2, ref.[5], compliant to the Smartcard IC Platform Protection Profile, BSI-PP-035, ref. [8].

The TOE is designed to comply with FIPS 140-2 level 3, ref. [4], requirements.

1.5.3 Logical Scope

The TOE SW executes between a calling application requesting the TOE services through a programmatic command interface, External API, and the operating system of the underlying processor. The operating system provides its functionality through the Internal API, consisting of basic functionality (called Application Note) and a Cryptographic Library.

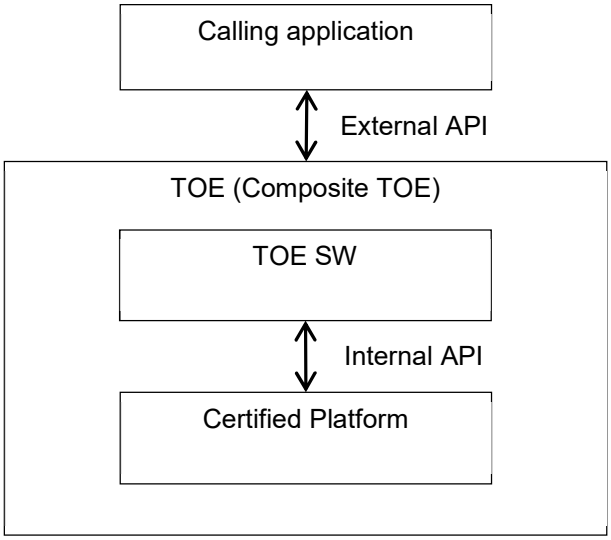

Figure 1, TOE definition

The Certified Platform consists of

- CryptoLib
- Hardware Abstraction Layer
- HW

The Certification Report for the Certified Platform can be found in [5]

1.5.3.1 Interfaces

The TOE communicates using the T=1 protocol over UART according to ISO7816-3 interface or over SPI. The commands and responses over the External API are specified in ref. [6].

The TOE SW interfaces the Infineon's IC chip operating system and cryptographic library through the Internal API according to ref. [10] and [11].

1.5.3.2 TOE Commands

The TOE provides functionality through its command interface, below this functionality is summarised. In ref. [6] all commands are listed and their availability in each TOE deployment is indicated.

- Authentication: Support for PIN based authentication and mutual authentication by challenge response schemes.
- PIN management: Change, block, and unblock PINs.
- Key management: Functionality to generate, load, export, import, delete, etc. keys.
- File management: Functionality to create, delete, read, update, etc. files.
- Encryption, decryption: Symmetric and asymmetric encryption and decryption of data.
- MAC: Calculate and verify MAC codes.
- Digital signature: Calculate and verify digital signatures.
- Additional commands for the Trusted Recorder: Get information from the Trusted Recorder.
- TOE handling: Get current status, set counters, reset, and delete all keys and files.

1.5.3.3 Not Included Functionality

The TOE will utilize cryptographic support implemented in the IC chip hardware and provided by the operating system. The following cryptographic primitives provided by the certified platform will be used:

- Data Encryption Standard (DES),
- Triple Data Encryption Standard (3DES),
- Rivest-Shamir-Adleman Cryptography (RSA),
- Advanced Encryption Standard (AES),
- Secure Hash Algorithm (SHA-1, SHA-256) as part of signature calculation/verification,
- Random Number Generator (RNG), and
- Elliptic Curve Cryptography (ECC).

The interface to the cryptographic primitives is defined in ref. [10].

1.5.3.4 File System

The file system consists several files of which Master File, MF, and Elementary Files are fixed and created at production. Additional Elementary Files can be created and deleted dynamically. The file systems for each TOE deployment are described in ref. [6] chapter 4.

The Access Conditions for each file varies between the different TOE deployments, see ref. [6] for a description. The device operating system has pre-allocated files for the chip serial number, counters, PIN, etc.

1.5.4 Configuration and Modes

The TOE can be configured by specifying access restrictions to specific objects, rules for re-authentication, and commands only to be available in a certain mode. Configuration of static objects is done during initialization (the Personalization phase according to the TOE life-cycle definition described in section 1.5.7), configuration of dynamically created objects is done at creation time (which may also include the Operational Usage phase). The configuration options are described below.

1.5.4.1 Global Access Conditions

Access conditions can be defined for commands accessing files and individual keys. The access conditions are statically set for the Master File and the static Elementary Files and keys. The access conditions are set at creation time for dynamically created files and keys. Access conditions can be combined using AND and OR constructors.

The following access conditions exist. The commands referred in the descriptions are defined in ref. [6]:

ALW - The command is always permitted.

PwdGx - Global Password: VERIFY command with x=PIN1 or PIN2 is required.

AutGSx - Authentication with Global Symmetric key: EXTERNAL AUTHENTICATE command using global symmetric key with index x is required.

AutDHx - Authentication with Diffie-Hellman session key: INTERNAL AUTHENTICATE or EXTERNAL AUTHENTICATE command using a session key created by GENERATE ADMIN TRANSFER KEYS is required. x is stating if the nonce shall be sent or received by the TOE.

ProGSx - MAC Protection by Global Symmetric key: A MAC calculated over the message fields using the symmetric key with index x is required (only used for the SET USAGE COUNTER command).

NEV - The command is never permitted.

1.5.4.2 Re-authentication

There are two counters, Start-up Usage Counter and Security Critical Commands Usage Counter, which may be used for re-authentication. The counters may be used in one out of four configuration options:

- No counters used (default)
- Start-up Usage Counter enabled
- Security Critical Commands Usage Counter enabled
- Both Start-up Usage Counter and Security Critical Commands Usage Counter enabled

The Start-up Usage Counter, if enabled, is decremented at each TOE start-up. When the counter reaches zero re-authentication to fulfill the AutGS1 access condition is needed.

The Security Critical Commands Usage Counter, if enabled, is decremented at each execution of a security critical command. The security critical commands are pre-defined and specified in ref. [6]. When the counter reaches zero authentication is mandatory for executing any of the security critical commands.

If both counters are enabled, decrementing the Start-up Usage Counter will reset the Security Critical Commands Usage Counter to its initial value if not Start-up Usage Counter has reached zero. The pre-set initial values of both counters can be changed by a TOE command.

1.5.4.3 Modes

It is possible to configure the TOE commands to only be allowed to be executed in Host Authenticated Mode. The TOE is in Host Authenticated Mode when

- user authentication has been successful,
- usage counters has not reached zero, and
- applicable command access conditions have been fulfilled.

1.5.5 Chain of Trust

The Kapsch Key Management System, KMS, is the root certificate authority, CA for handling of Admin Keys. An intermediate CA, KMS Issuing CA, is used for flexibility reasons. Certificates are not handled by the TOE but the KMS Root CA's public key is pre-installed in the TOE. The KMS Issuing CA's public key is imported into the TOE in a key container signed using the KMS Root CA's private key. The security domain has an asymmetric key pair used for generation of authentication and encryption session keys. The SD public key is stored in a key container signed using the KMS Issuing CA's private key. The following proprietary format is used for the key container.

- Public Key Container ID
- Public Key algorithm ID
- Public Key additional information
- Public Key Value
- Issuing Public Key Container ID, containing the public key used for signing
- Issuing Public Key algorithm ID
- Public Key Signature calculated over the previous fields

The Public Key Signature shall be a NIST-521 bit ECC DSA signature calculated over a SHA256 Hash.

The SD private key is stored in a key file in the file system.

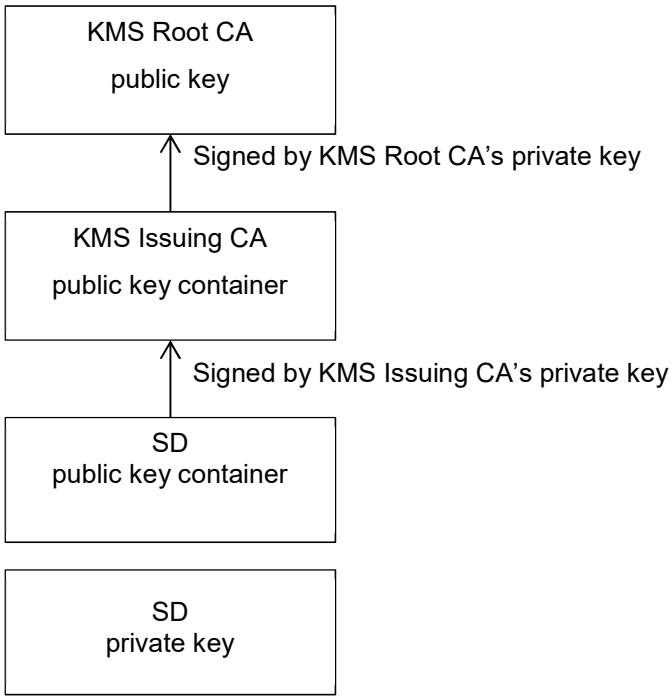

Figure 2, Chain of trust

A pre-installed symmetric Factory Authentication Key is used for authentication of the TOE at assignment to Security domain, i.e. import of the key containers and at generation of the SD asymmetric key pair.

The SD specific asymmetric keys described above are dedicated for derivation of keys for import/export of Admin Keys.

1.5.6 Cryptographic Operations and Keys

The TOE uses cryptographic primitives according to Table 1 for the specified cryptographic operations. See section 6.3.1 for a specification of the cryptographic standards used for each primitive and mode.

Cryptographic operation	Primitive/Protocol/ Scheme	Key length	Mode/HASH/ Curve
Symmetrical encryption and decryption	AES	128/256	CBC, ECB
	DES	64/128*	CBC, ECB
Key derivation	DES	64/128*	CBC
	AES	128/256	CBC
Key encryption and decryption	AES	128/256	CBC
Diffie-Hellman key exchange	EC DH	128/256	SHA-256, P-256, P512/521
MAC calculation and verification	DES MAC	64/128*	CBC
	AES MAC	128/256	CBC, EMAC, CMAC
Asymmetrical encryption and decryption	RSAES-OAEP	2048	NA
	RSAES-PKCS1-v1_5	2048	NA
Digital signature calculation and verification	RSASSA-PSS	1024/2048/ 4096	SHA-256
	RSASSA-PKCS1-v1_5	1024/2048/ 4096	SHA-1/ SHA-256
	EC-DSA		NIST P-256, NIST P-521 (only verification)BrainpoolP256r1
Random number generation	According to ref. [11].		

Table 1, Used cryptographic primitives, protocols and schemes. *) Effective 56/112 bits

The DES and Triple-DES primitives are required by the following standards for road tolling systems:

- EN 15509
- CEN ISO/TS 12813
- CEN ISO/TS 13141
- EN 16312

The SHA-1 primitive is specified in an agreement between tolling operators in US. The algorithm is referred to in document ref. [7].

1.5.6.1 Asymmetric Keys

The TOE can store the following asymmetric keys:

Key	Key type	Imported/ generated in phase [1)]	Description
KMS Root CA public key	RSA 2048	Personalisation	Used for verification of digital signatures of other keys
KMS Issuing CA public key	RSA 2048	Personalisation	Used for verification of digital signatures of other keys
SD key pair	RSA 2048	Personalisation	Generation of session keys
	ECC 521	Personalisation	ECDH encryption key creation
RSA keys pairs	RSA 1024, RSA 2048, RSA 4096	Operational Usage	End-customer usage
ECC key pairs	ECC 256, ECC 521	Operational Usage	End-customer usage

1) Phases according to section 1.5.7

Table 2 Asymmetric keys

The attributes associated to each asymmetric key pairs are:

- Key identifier (record number in key file)
- Algorithm and key length identifier
- Key access conditions

Since the cryptographic support implemented in the certified platform only can handle RSA keys in the CRT format (Chinese Remainder Theorem) the private part of the RSA keys is stored in a proprietary format holding the CRT parameters.

1.5.6.2 Symmetric Keys

The TOE can store the following symmetric keys:

Key	Key type	Imported/ generated in phase [1)]	Description
Factory Authentication Key	128 AES	Personalisation	This is categorized as an Admin key. It is used when importing public key containers and generation of SD key pair.
Other Admin Keys	-	Personalisation	TOE usage
Non-Admin Keys	-	Operational Usage	End-customer usage

1) Phases according to section 1.5.7

Table 3, Symmetric keys (not all symmetric keys are identified with name in the table)

The attributes associated to each symmetric key are:

- Key identifier (record number in key file)
- Algorithm identifier
- Key access conditions
- Usage counter for key derivation (only used in P-SAM)
- Key length
- Key Verification Code given by a truncated encrypted 0-vector

1.5.7 TOE Life Cycle

The TOE life-cycle can be separated into several distinct phases as shown in Figure 3.

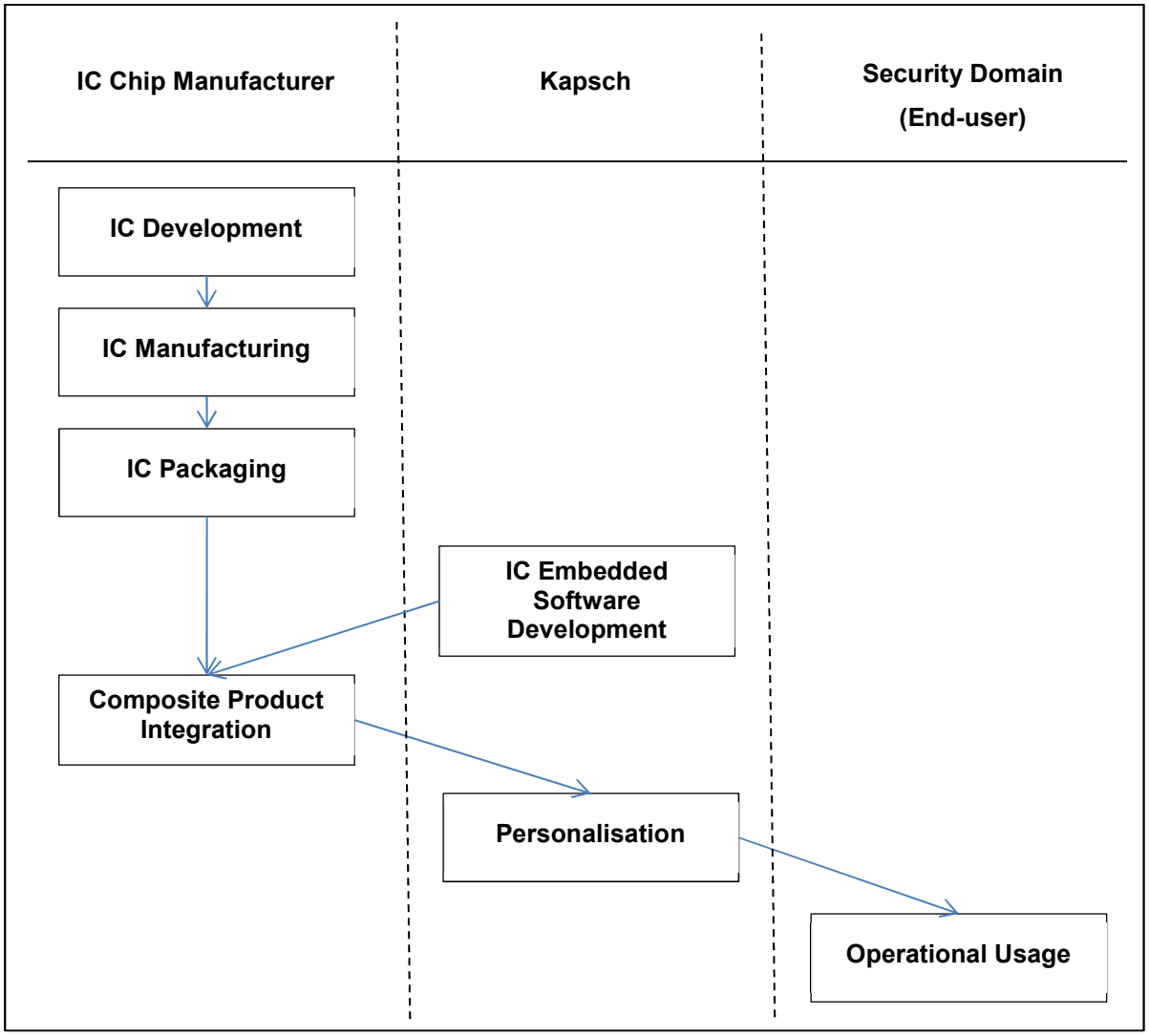

Figure 3, Composite product life cycle

The IC Development, IC Manufacturing, and IC Packaging phases take place at the IC chip manufacturer and are common for this kind of chip. i.e. not aware of the TOE SW.

At the Composite Production Integration phase, the TOE specific software is integrated into the chip.

In the Personalisation phase the backup key and the file system are initialised. Further the KMS Root CA public key and the Factory Authentication Key will be included. At this stage the IC chip including the TOE is delivered to the vendor, Kapsch.

Kapsch will in the Personalisation phase generate and load all Admin Keys for a specific Security Domain, SD.

The End-user customer will in the Operational Usage phase include all Non-admin Keys needed for the SD, e.g. keys for the Dedicated Short Range Communication, DSRC, between the OBU and the ES.

1.5.8 Roles

No roles are defined for the TOE. The TOE user is required to authenticate according to the access conditions defined for the object that is accessed. The TOE user is an IT product and no human user interface is provided.

2 Conformance Claims

2.1 CC Conformance Claim

This Security Target is CC Part 2 conformant and CC Part 3 conformant to Common Criteria version 3.1, revision 4

- Part 1: Security Functional Components, September 2012, Version 3.1, Revision 4, CCMB-2012-09-001
- Part 2: Security Functional Components, September 2012, Version 3.1, Revision 4, CCMB-2012-09-002
- Part 3: Security Assurance Components, September 2012, Version 3.1, Revision 4, CCMB-2012-09-003

The guidance from ISO/IEC 15446, *Information technology - Security techniques - Guide for the production of protection profiles and security targets*, Second edition 2009-03-01, has been used when developing this Security Target.

2.2 PP Conformance Claims

This Security Target does not claim strict or demonstrable conformance to any Protection Profile.

The TOE SW is dependent on security functionality in its operational environment, i.e. the certified platform defined in Infineon Security Target, ref. [9], and the Security IC Platform Protection Profile, BSI-PP-0035, ref. [8]. Those documents are referenced in this Security Target to get the complete picture of the security problem.

2.3 Package Conformance Claims

This Security Target claims conformance to assurance requirement package EAL5.

3 Security Problem Definition

3.1 Introduction

The security problem definition described below includes threats, organizational security policies and security usage assumptions.

3.2 Threats

Threats are described by an adverse action performed by defined threat agents on the assets that the TOE has to protect. The assets and their protection needed, the threat agents and their attack potential, and the threat adverse actions are described below.

3.2.1 Assets

Asset	TOE deployment
KMS Issuing CA container	All
SD container	All
SD key pair	All
Admin Keys	All
Non-admin Keys	All
Trusted recorder master key, derived TR key, or internally calculated MAC	TR-SAM
Derived keys not explicitly derived for external export	All
User data	All
PINs	All

Table 4 Assets to be protected

3.2.2 Threat Agents

The threat agents that are identified for the different deployments of the TOE are described below. The description includes the attack potential that is assumed for each threat agent in terms of:

Knowledge: The threat agent's competence within the technology area and knowledge about the TOE specific design and construction.

Opportunity: The opportunity for the threat agent to try to mount an attack against the TOE.

Equipment: The tools and equipment that the threat agent has access to.

Motivation: The values that might be gained for the threat agent at a successful attack.

3.2.2.1 M-SAM

The M-SAM is assumed to be physically protected, during operation and when stored. No attackers with malicious intents are identified but an Authorized admin may make mistakes.

Authorized admin	
The Authorized Admin, who is defining and deploying the TOE configuration, makes mistakes that override or bypass security features or enable opportunities for others to do so.	
Knowledge:	Deep knowledge about the technology area and the TOE system
Opportunity:	Low, the configuration is reviewed by a second Authorized admin.
Equipment:	None
Motivation:	None, has no malicious intent, is trained and follows the guidance but is capable of making errors.

Table 5 Threat agent: Authorized admin

3.2.2.2 CS-SAM and P-SAM

The CS-SAM is assumed to be installed in a server in a server room, physically protected from unauthorized persons. The P-SAM is also assumed to be used in a physically protected production environment. The threat agents: Logical remote attacker, Unauthorized user, and Authorized admin (Table 5) are identified.

Logical remote attacker	
Has no physical access, may try to remotely attack the TOE logical interface through the server's network interface through the network protection, such as firewalls, etc.	
Knowledge:	Public knowledge about the technology area and the TOE system
Opportunity:	Unlimited in time since remote access to the network
Equipment:	Specialized with a value less than the gain from an a successful attack
Motivation:	High motivation since large values could be at stake, e.g. for transportation companies

Table 6 Threat agent: Logical remote attacker

Unauthorized user	
Has authorized physical access to the server room but is not authorized to use the TOE functionality.	
Knowledge:	Public knowledge about the technology area and the TOE system
Opportunity:	Very limited, max 30 min undetected, e.g. during a lunch break
Equipment:	Specialized that can be brought to the location by hand
Motivation:	Moderate, since the risk to be revealed is considered high

Table 7 Threat agent: Unauthorized user

3.2.2.3 CP-SAM

The CP-SAM is installed in a manner that hinders unauthorized physical access. The threat agents: Physical attacker, Logical local attacker, and Authorized service personnel are identified.

Physical attacker	
Is physically attacking the RSS to reach the CP-SAM. May try to steal the TOE or attack the TOE physically.	
Knowledge:	Public knowledge about the technology area and the TOE system
Opportunity:	Limited, max 1 hour until detected by alarm system and stopped.
Equipment:	Specialized that can be brought to the CP-SAM in the RSS and with a value less than the gain from an a successful attack
Motivation:	High motivation since large values could be at stake, e.g. for transportation companies

Table 8 Threat agent: Physical attacker

Logical local attacker	
Is placed nearby the RSS and has no physical access to the TOE. May try to attack the TOE logical interface through the RSS network.	
Knowledge:	Public knowledge about the technology area and the TOE system
Opportunity:	Limited, max 1 day undetected
Equipment:	Specialized that can be brought to the place and with a value less than the gain from an a successful attack
Motivation:	High motivation since large values could be at stake, e.g. for transportation companies

Table 9 Threat agent: Logical local attacker

Authorized service personnel	
Service personnel, etc, who is performing service on the TOE deployed device, makes mistakes that override or bypass security features or enable opportunities for others to do so.	
Knowledge:	Moderate knowledge about the technology area and the TOE system
Opportunity:	Low since faulty deployment of the TOE will be detected by the system in the TOE environment
Equipment:	None
Motivation:	None, has no malicious intent, is trained and follows the guidance but is capable of making errors.

Table 10 Threat agent: Authorized service personnel

3.2.2.4 TR-SAM

The TR-SAM is installed in an OBU. The OBU is equipped with tamper protection. The threat agents: Physical OBU attacker and Logical OBU attacker are identified.

Physical OBU attacker

Has access to an OBU. Is physically attacking the OBU to reach the TR-SAM for a physical attack, including manipulation, probing, environmental stress, etc.	
Knowledge:	Public knowledge about the technology area and the TOE system
Opportunity:	Moderate since the OBU is equipped with tamper protection.
Equipment:	Specialized with a value less than the gain from an a successful attack
Motivation:	High motivation since large values could be at stake, e.g. for transportation companies

Table 11 Threat agent: Physical OBU attacker

Logical OBU attacker	
Has access to an OBU. May try to attack the TOE logical interface through the DSRC interface.	
Knowledge:	Public knowledge about the technology area and the TOE system
Opportunity:	Unlimited
Equipment:	Specialized with a value less than the gain from an a successful attack
Motivation:	High motivation since large values could be at stake, e.g. for transportation companies

Table 12 Threat agent: Logical OBU attacker

3.2.3 Threats

The threats against the TOE according to Table 13 are identified.

Name	Threat against the TOE	Threat agent
T.Logical_Leak	Logical Information Leakage A threat agent may logically attack the TOE in order to reveal sensitive assets. The modification may be achieved through deficiencies in the TOE external communication protocols or in the TOE internal asset handling.	Logical remote attacker Logical local attacker Logical OBU attacker Unauthorized user
T.Logical_Manipulation	Logical Manipulation A threat agent may logically attack the TOE in order to modify or remove sensitive assets. The attack may be achieved through deficiencies in the TOE external communication protocols or in the TOE internal assets handling.	Logical remote attacker Logical local attacker Logical OBU attacker Unauthorized user
T.Eavesdropping	Eavesdropping A threat agent may listen to and successfully interpret sensitive assets sent or received over the TOE external interface.	Logical remote attacker Logical local attacker Logical OBU attacker Unauthorized user
T.Spoofing	Spoofing	Logical remote attacker Logical local attacker

Name	Threat against the TOE	Threat agent
	A threat agent may try to disguise as an authorised user to disclose, manipulate or remove sensitive assets.	Logical OBU attacker Unauthorized user
T.Replay	Replay A threat agent may gain access to sensitive information by replaying TOE external communication.	Logical remote attacker Logical local attacker Logical OBU attacker Unauthorized user
T.Unint_Corruption	Unintentional Corruption An authorised user may by mistake override or bypass security features of the TOE or enable opportunities for others to do so.	Authorized admin Authorized service personnel

Table 13, Threats against the TOE

Table 14 lists threats against the TOE certified platform. These threats, that are included to get a complete coverage of threat agents and threats, are all identified in BSI-PP-035, ref. [8], resp. ST Infineon, ref. [9], and are all mitigated by security objectives defined in those documents. The threats against the platform and the TOE SW complement and do not contradict each other. Together they form the total amount of threats against the TOE.

Name	Threat against the TOE certified platform	Threat agent
T.Phys-Manipulation	Physical Manipulation BSI-PP-035, ref. [8], section 3.2	Unauthorized user Physical attacker Physical OBU attacker
T.Phys-Probing	Physical Probing BSI-PP-035, ref. [8], section 3.2	Unauthorized user Physical attacker Physical OBU attacker
T.Malfunction	Malfunction due to Environmental Stress BSI-PP-035, ref. [8], section 3.2	Unauthorized user Physical attacker Physical OBU attacker Logical OBU attacker
T.Leak-Inherent	Inherent Information Leakage BSI-PP-035, ref. [8], section 3.2	Unauthorized user Physical attacker Physical OBU attacker
T.Leak-Forced	Forced Information Leakage BSI-PP-035, ref. [8], section 3.2	Unauthorized user Physical attacker Physical OBU attacker Logical OBU attacker
T.Abuse-Func	Abuse of Functionality BSI-PP-035, ref. [8], section 3.2	Logical remote attacker Unauthorized user Authorized admin Logical local attacker Authorized service personnel
T.RND	Deficiency of Random Numbers BSI-PP-035, ref. [8], section 3.2	Logical remote attacker Unauthorized user Logical local attacker

Name	Threat against the TOE certified platform	Threat agent
T.Mem-Access	Memory Access Violation ST Infineon, ref. [9], section 4.1.1	Any

Table 14, Threats against the TOE certified platform

3.3 Organisational Security Policies

Organisational security policies, OSPs, for the TOE are stated according to Table 15.

Name	OSP
P.Crypto	Cryptographic Mechanisms The TOE shall provide cryptographic mechanisms according to ref. [6]. This includes mechanisms to: - encrypt and decrypt user data, - calculate and verify message authentication codes over user data, - calculate and verify digital signatures over user data, - derive keys, encrypt and decrypt keys, and - generate random data for key and challenge generation.
P.Keys	Key Mechanisms The TOE shall provide secure key mechanisms according to ref. [6]. This includes mechanisms to: - generate, - derive, - import, - export, and - backup keys. The TOE (P-SAM) shall increment a derivation counter monotonically every time a key is derived. The derivation counter shall start on zero and shall not be possible to reset after SAM production until the key is deleted.
P.Memory_Test	Memory Test The TOE shall detect memory deficiencies in the operational environment at initial start-up.

Table 15, Organizational Security Policies for the TOE

Table 16 below, lists OSP's for the TOE the certified platform. They are included to get a complete coverage of environmental policies. They are identified in BSI-PP-035, ref. [8], resp. ST Infineon, ref. [9], and are all met by security objectives defined in those documents. These OSP's and those for the TOE SW complement and do not contradict each other. Together they form the total amount of OSPs for the TOE.

Name	OSP
P.Process-TOE	Protection during TOE Development and Production BSI-PP-035, ref. [8], section 3.3
P.Add-Functions	Additional Specific Security Functionality

Name	OSP
	ST Infineon, ref. [9], section 4.2 In the ST Infineon, ref. [9], there is a O.Add-Functions defined. It is fulfilled by the TOE.

Table 16, Organizational Security Policies for the certified platform

3.4 Assumptions

Assumptions on the TOE operational environment are made according to Table 17.

Name	Assumptions on the TOE operational environment
A.Deployment	Deployment The TOE operational environment is assumed to react on faulty deployment performed by the Authorized service personnel.
A.OBU_Protection	OBU Tamper Protection The operational environment of the TOE when deployed as TR-SAM in an OBU is assumed to be equipped with tamper protection.
A.No_Evil	No Evil Authorized Administrators Authorized admins and service personnel are assumed to be security screened to be non-hostile, sufficiently trained, and willing to follow their instructions, before authorized to interact with the TOE.
A.Counter	Security Critical Commands Usage Counter The TOE operational environment is assumed to use the Security Critical Commands Usage Counter to request a new authentication before e.g. 20000 Triple-Des or AES operations have been performed.

Table 17, Assumptions on the TOE environment

4 Security Objectives

4.1 Introduction

The statement of security objectives defines the security objectives for the TOE and its environment. The security objectives intend to address all security environment aspects identified. The security objectives reflect the stated intent and are suitable to counter all identified threats and cover all identified organisational security policies and assumptions. The following categories of objectives are identified:

- The security objectives for the TOE shall be clearly stated and traced back to aspects of identified threats to be countered by the TOE and/or organisational security policies to be met by the TOE.
- The security objectives for the environment shall be clearly stated and traced back to aspects of identified threats countered by the TOE environment, organisational security policies or assumptions.
- The security objectives for the IC chip and OS parts of the platform are defined in chapter 4, ref. [8], and chapter 5, ref. [9].

4.2 Security Objectives for the TOE

The following security objectives for the TOE are defined.

Security Objective	Description
O.Authentication	The TOE shall provide measures against unauthorised access to sensitive assets.
O.Confidentiality	The TOE shall provide measures against disclosure of Admin Keys and Non-admin Keys at import and export.
O.Crypto	The TOE shall provide cryptographic mechanisms according to ref. [6]. This includes mechanisms to: - encrypt and decrypt user data, - calculate and verify message authentication codes over user data, - calculate and verify digital signatures over user data, - derive keys, - encrypt and decrypt keys, and - generate random data for key and challenge generation.
O.Keys	Key Mechanisms The TOE shall provide secure key mechanisms according to ref. [6]. This includes mechanisms to: - generate, - derive, - import, - export, and - backup keys. The TOE (P-SAM) shall increment a derivation counter monotonically every time a key is derived. The derivation counter shall start on zero and shall not be possible to reset after SAM production until the key is deleted.

Security Objective	Description
O.Integrity	The TOE shall provide measures to ensure integrity and authenticity of Admin Keys and Non-admin Keys at import and export. The TOE shall provide measures ensure integrity and authenticity of KMS Issuing CA container and SD container at import.
O.Replay_Detection	The TOE shall detect attempts to replay the following TOE commands defined in ref. [6]: - Export of Admin Keys, - Export of Non-admin Keys, - Export of asymmetric keys, - Import of Non-admin Keys, - Import of Admin Keys, - Reading encrypted binary file content, and - Update encrypted binary file content.
O.Memory_Test	The TOE shall detect memory deficiencies in the operational environment at start-up.

Table 18, Security objectives for the TOE

4.3 Security Objectives for the Operational Environment

The security objectives for the operational environment identified in Table 19.

Security Objective	Description
OE.Config_Review	Configuration Review The configuration performed by an Authorised admin must be reviewed by a second Authorised admin to minimise unintentional corruption before applied the TOE.
OE.Deployment	Deployment The TOE operational environment must react on faulty deployment performed by the Authorised service personnel.
OE.OBU_Protection	OBU Protection The OBU must be equipped with tamper protection.
OE.No_Evil	No Evil Authorised Administrators Authorised admins and service personnel must be security screened to be non-hostile, sufficiently trained, and willing to follow their instructions, before authorised to interact with the TOE.
OE.SecurityCounter	The TOE operational environment will use the Security Critical Commands Usage Counter to request a new authentication before e.g. 20000 Triple-Des or AES operations have been performed.

Table 19, Security objectives for the TOE operational environment

4.4 Security Objectives Rationale

4.4.1 Security Objectives Coverage

This section provides tracings of the security objectives for the TOE to threats, OSPs, and assumptions.

	T.Logical_Leak	T.Logical_Manipulation	T.Eavesdropping	T.Spoofing	T.Replay	T.Unint_Corruption	P.Crypto	P.Keys	P.Memory_Test	A.Deployment	A.OBU_Protection	A.No_Evil
O.Authentication	X	X		X								
O.Confidentiality	X		X									
O.Crypto	X	X	X	X			X					
O.Integrity		X										
O.Keys	X	X	X	X				X				
O.Replay_Detection					X							
O.Memory_Test									X			
OE.Config_Review						X						
OE.Deployment										X		
OE.OBU_Protection											X	
OE.No_Evil												X

Table 20, Security objectives coverage

4.4.2 Security Objectives Sufficiency

The following rationale provides justification that the security objectives for the environment are suitable to cover each individual assumption or threat to the environment, that each security objective for the environment that traces back to a threat or an assumption about the environment of use.

Threat/OSP/Assumption	Objective	Rationale
T.Logical_Leak A threat agent may logically attack the TOE in order to reveal sensitive assets. The modification may be achieved	**O.Authentication** The TOE must provide measures against unauthorised access to sensitive assets and functionality of the TOE.	**T.Logical_Leak** is mitigated by requirements on authentication (**O.Authentication**) and confidentiality of sensitive assets in transfer (**O.Confidentiality**). The requirements shall be met by

Threat/OSP/Assumption	Objective	Rationale
through deficiencies in the TOE external communication protocols or in the TOE internal asset handling.	**O.Confidentiality** The TOE shall provide measures against disclosure of Admin Keys and Non-admin Keys at import and export.	cryptographic mechanisms (**O.Crypto**) and secure cryptographic key handling (**O.Keys**).
	O.Crypto The TOE shall provide cryptographic mechanisms according to ref. [6]. This includes mechanisms to: - encrypt and decrypt user data, - calculate and verify message authentication codes over user data, - calculate and verify digital signatures over user data, - derive keys, - encrypt and decrypt keys, and - generate random data for key and challenge generation.	
	O.Keys The TOE shall provide secure key mechanisms according to ref. [6]. This includes mechanisms to: - generate, - derive, - import, - export, and - backup keys. The TOE (P-SAM) shall increment a derivation counter monotonically every time a key is derived. The derivation counter shall start on zero and shall not be possible to reset after SAM production until the key is deleted.	
T.Logical_Manipulation A threat agent may logically attack the TOE in order to modify	**O.Authentication** The TOE must provide measures against unauthorised access to	**T.Logical_Manipulation** is mitigated by requirements on authentication

Threat/OSP/Assumption	Objective	Rationale
or remove sensitive assets. The attack may be achieved through deficiencies in the TOE external communication protocols or in the TOE internal assets handling.	sensitive assets and functionality of the TOE.	(**O.Authentication**) and integrity and authenticity measures of sensitive assets in transfer (**O.Integrity**). The requirements shall be met by cryptographic mechanisms (**O.Crypto**) and secure cryptographic key handling (**O.Keys**).
	O.Crypto The TOE shall provide cryptographic mechanisms according to ref. [6]. This includes mechanisms to: - encrypt and decrypt user data, - calculate and verify message authentication codes over user data, - calculate and verify digital signatures over user data, - derive keys, - encrypt and decrypt keys, and - generate random data for key and challenge generation.	
	O.Integrity The TOE shall provide measures to ensure integrity and authenticity of Admin Keys and Non-admin Keys at import and export. The TOE shall provide measures ensure integrity and authenticity of KMS Issuing CA container and SD container at import.	
	O.Keys The TOE shall provide secure key mechanisms according to ref. [6]. This includes mechanisms to: - generate, - derive, - import, - export, and - backup keys. The TOE (P-SAM) shall increment a derivation counter monotonically every time a key is derived. The derivation counter shall start on zero and shall not be possible to reset after SAM	

Threat/OSP/Assumption	Objective	Rationale
	production until the key is deleted.	
T.Eavesdropping A threat agent may listen to and successfully interpret sensitive assets sent or received over the TOE external interface.	**O.Confidentiality** The TOE shall provide measures against disclosure of Admin Keys and Non-admin Keys at import and export.	**T.Eavesdropping** is mitigated by requirements on confidentiality of sensitive assets in transfer (**O.Confidentiality**). The requirements shall be met by cryptographic mechanisms (**O.Crypto**) and secure cryptographic key handling (**O.Keys**).
	O.Crypto The TOE shall provide cryptographic mechanisms according to ref. [6]. This includes mechanisms to: - encrypt and decrypt user data, - calculate and verify message authentication codes over user data, - calculate and verify digital signatures over user data, - derive keys, - encrypt and decrypt keys, and - generate random data for key and challenge generation.	
	O.Keys The TOE shall provide secure key mechanisms according to ref. [6]. This includes mechanisms to: - generate, - derive, - import, - export, and - backup keys. The TOE (P-SAM) shall increment a derivation counter monotonically every time a key is derived. The derivation counter shall start on zero and shall not be possible to reset after SAM production until the key is deleted.	
T.Spoofing	**O.Authentication**	

Threat/OSP/Assumption	Objective	Rationale
A threat agent may try to disguise as an authorised user to disclose, manipulate or remove sensitive assets.	The TOE must provide measures against unauthorised access to sensitive assets and functionality of the TOE.	**T.Spoofing** is mitigated by requirements on authentication to prevent unauthorised access. The requirements shall be met by cryptographic mechanisms (**O.Crypto**) and secure cryptographi key handling (**O.Keys**).
	O.Crypto The TOE shall provide cryptographic mechanisms according to ref. [6]. This includes mechanisms to: - encrypt and decrypt user data, - calculate and verify message authentication codes over user data, - calculate and verify digital signatures over user data, - derive keys, - encrypt and decrypt keys, and - generate random data for key and challenge generation.	
	O.Keys The TOE shall provide secure key mechanisms according to ref. [6]. This includes mechanisms to: - generate, - derive, - import, - export, and - backup keys. The TOE (P-SAM) shall increment a derivation counter monotonically every time a key is derived. The derivation counter shall start on zero and shall not be possible to reset after SAM production until the key is deleted.	
T.Replay A threat agent may gain access to sensitive information by replaying TOE external communication.	**O.Replay_Detection** The TOE shall detect attempts to replay the following TOE commands defined in ref. [6]: - Export of Admin Keys,	**T.Replay** is mitigated by measured to detect replay attacks.

Threat/OSP/Assumption	Objective	Rationale
	- Export of Non-admin Keys, - Export of asymmetric keys, - Import of Non-admin Keys, - Import of Admin Keys, - Reading encrypted binary file content, and - Update encrypted binary file content.	
T.Unint_Corruption An authorised user may by mistake override or bypass security features of the TOE or enable opportunities for others to do so.	**OE.Config_Review** The configuration performed by an Authorised admin must be reviewed by a second Authorised admin to minimise unintentional corruption before applied the TOE.	**T.Unint_Corruption** is mitigated by requirements on peer review of configuration applied to the TOE.
P.Crypto The TOE shall provide cryptographic mechanisms according to ref. [6]. This includes mechanisms to: - encrypt and decrypt user data, - calculate and verify message authentication codes over user data, - calculate and verify digital signatures over user data, - derive keys, - encrypt and decrypt keys, and - generate random data for key and challenge generation.	**O.Crypto** The TOE shall provide cryptographic mechanisms according to ref. [6]. This includes mechanisms to: - encrypt and decrypt user data, - calculate and verify message authentication codes over user data, - calculate and verify digital signatures over user data, - derive keys, - encrypt and decrypt keys, and - generate random data for key and challenge generation.	The **P.Crypto** policy is directly covered by **O.Crypto.**
P.Keys The TOE shall provide secure mechanisms to generate, derive, import, export, and backup keys. The TOE (P-SAM) shall increment a derivation counter monotonically every time a key is derived. The derivation counter shall start on zero and shall not be possible to reset after SAM production until the key is deleted.	**O.Keys** The TOE shall provide secure key mechanisms according to ref. [6]. This includes mechanisms to: - generate, - derive, - import, - export, and - backup keys. The TOE (P-SAM) shall increment a derivation counter monotonically every time a key is	**P.Keys** policy is directly covered by **O.Keys.**

Threat/OSP/Assumption	Objective	Rationale
	derived. The derivation counter shall start on zero and shall not be possible to reset after SAM production until the key is deleted.	
P.Memory_Test The TOE shall detect memory deficiencies in the operational environment at initial start-up.	**O.Memory_Test** The TOE shall detect memory deficiencies in the operational environment at start-up.	**P.Memory_Test** policy is directly covered by **O.Memory_Test.**
A.Deployment The TOE operational environment is assumed to react on faulty deployment performed by the Authorised service personnel.	**OE.Deployment** The TOE operational environment must react on faulty deployment performed by the Authorised service personnel.	**A.Deployment** assumption is directly covered by **OE.Deployment.**
A.OBU_Protection The TOE operational environment is assumed to be equipped with tamper protection.	**OE.OBU_Protection** The OBU must be equipped with tamper protection.	**A.OBU_Protection** assumption is directly covered by **OE.OBU_Protection.**
A.No_Evil Authorised admins and service personnel are assumed to be security screened to be non-hostile, sufficiently trained, and willing to follow their instructions, before authorised to interact with the TOE.	**OE.No_Evil** Authorised admins and service personnel must be security screened to be non-hostile, sufficiently trained, and willing to follow their instructions, before authorised to interact with the TOE.	**A.No_Evil** assumption is directly covered by **OE.No_Evil.**
A.Counter The TOE operational environment is assumed to use the Security Critical Commands Usage Counter to request a new authentication before e.g. 20000 Triple-Des or AES operations have been performed	**OE.SecurityCounter** The TOE operational environment will use the Security Critical Commands Usage Counter to request a new authentication before e.g. 20000 Triple-Des or AES operations have been performed.	**A.Counter** assumption is directly covered by **OE.SecurityCounter**.

Table 21, Security objectives sufficiency

5 Extended Components Definition

No extended components are defined.

6 Security Requirements

6.1 TOE Security Functionality

The commands allowed by the TOE in its different deployments are defined in ref. [6].

6.2 Security Functional Policies

Access rules for Users operating the TOE by commands defined in ref. [6] are stated in the Access Condition Policy, defined below by the FDP_ACC.1, FDP_ACF.1, and FMT_MSA.3 requirements.

Information flow control is restricted by the rules stated in the Import/Export Key Policy defined below by the FDP_IFC.1, FDP_IFF.1, FDP_ETC.2, and FDP_ITC.2.1 requirements.

6.3 Security Functional Requirements

6.3.1 Cryptographic Support – FCS

6.3.1.1 Cryptographic key generation – FCS_CKM.1a (AES)

FCS_CKM.1.1a The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **AES** and specified cryptographic key sizes **128 and 256 bits** that meet the following: **Ref. [11].**

6.3.1.2 Cryptographic key generation – FCS_CKM.1b (DES)

FCS_CKM.1.1b The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **DES** and specified cryptographic key sizes **64 and 128 bits** that meet the following: **Ref. [11].**

6.3.1.3 Cryptographic key generation – FCS_CKM.1c (RSA)

FCS_CKM.1.1c The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **RSA** and specified cryptographic key sizes **1024, 2048, and 4096 bits** that meet the following: **Ref. [27].**

6.3.1.4 Cryptographic key generation – FCS_CKM.1d (ECC)

FCS_CKM.1.1d The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **ECC** and specified cryptographic key sizes **256 and 521 bits** that meet the following: **Ref. [22].**

Application note: Only valid for: TR-SAM

6.3.1.5 Cryptographic key generation – FCS_CKM.1e (EC DH)

FCS_CKM.1.1e The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **EC DH, SHA-256** and specified cryptographic key sizes **128 and 256 bits based on ECC P-256 and ECC P-512/521** that meet the following: **EC DH: Ref. [26], SHA-256: Ref. [21].**

6.3.1.6 Cryptographic key access – FCS_CKM.3

FCS_CKM.3.1 The TSF shall perform **backup of keys** in accordance with a specified cryptographic key access method **encrypting the keys with a 256 bits AES key used only for backup** that meets the following: **AES: Ref. [20]**.

6.3.1.7 Cryptographic key destruction – FCS_CKM.4

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **overwriting with zeroes** that meets the following: **None**.

6.3.1.8 Cryptographic operation – FCS_COP.1a (AES encrypt/decrypt)

FCS_COP.1.1a The TSF shall perform **encryption and decryption** in accordance with a specified cryptographic algorithm **AES used in CBC or ECB modes** and cryptographic key sizes **128 or 256 bits** that meet the following: **AES: Ref. [20]; CBC, ECB: Ref. [24]**.

6.3.1.9 Cryptographic operation – FCS_COP.1b (DES encrypt/decrypt)

FCS_COP.1.1b The TSF shall perform **encryption and decryption** in accordance with a specified cryptographic algorithm **DES used in CBC or ECB modes** and cryptographic key sizes **64 or 128 bits** that meet the following: **DES: Ref. [19]; CBC, ECB: Ref. [24]**.

Application note: DES encryption in CBC mode with 64 or 128 bits key length used for calculation of access credentials is only valid for: CS-SAM, CP-SAM, and P-SAM. Other use of DES encryption/decryption is valid for: M-SAM, CS-SAM, CP-SAM, and P-SAM. It is a requirement given by the system design and protocols that the SAM must support DES also in the 64 bits mode [13].

6.3.1.10 Cryptographic operation – FCS_COP.1c (AES key derivation)

FCS_COP.1.1c The TSF shall perform **key derivation** in accordance with a specified cryptographic algorithm **AES in CBC mode** and cryptographic key sizes **128 or 256 bits** that meet the following: **Scheme: Ref. [13] 9.8, 9.9, 10.9, 10.10; AES: Ref. [20]; CBC: Ref. [24]**.

6.3.1.11 Cryptographic operation – FCS_COP.1d (DES key derivation)

FCS_COP.1.1d The TSF shall perform **key derivation** in accordance with a specified cryptographic algorithm **DES in CBC mode** and cryptographic key sizes **64 or 128 bits** that meet the following: **Scheme: Ref. [13] 9.10, 10.7, 10.8; DES: Ref. [19]; CBC: Ref. [24]**.

Application note: Derivation of 64 or 128 bits DES keys is used for calculation of access credentials. Only valid for: CS-SAM, CP-SAM, and P-SAM.

6.3.1.12 Cryptographic operation – FCS_COP.1e (Key encrypt/decrypt)

FCS_COP.1.1e The TSF shall perform **encryption and decryption** in accordance with a specified cryptographic algorithm **AES in CBC mode** and cryptographic key sizes **AES: 128 or 256 bits** that meet the following: **AES: Ref. [20]; CBC: Ref. [24]**.

6.3.1.13 Cryptographic operation – FCS_COP.1f (RSA encrypt/decrypt)

FCS_COP.1.1f The TSF shall perform **encryption and decryption** in accordance with a specified cryptographic algorithm **RSAES-OAEP or RSAES-PKCS1-v1_5** and cryptographic key sizes **2048** that meet the following: **Ref. [27].**

Application note: RSA encryption using 2048 bits key length is only valid for M-SAM. RSA decryption is valid for all SAM deployments.

6.3.1.14 Cryptographic operation – FCS_COP.1g (AES MAC)

FCS_COP.1.1g The TSF shall perform **calculation and verification of message authentication codes** in accordance with a specified cryptographic algorithm**s AES MAC in CBC and EMAC or CMAC mode** and cryptographic key sizes **128 or 256 bits** that meet the following: **AES: Ref. [20]; CBC Ref. [24]; EMAC: Ref. [23]; CMAC: Ref. [25]. TR-SAM: Ref. [14] clause 7.1.2.**

Application note: EMAC and CMAC are only valid for: CS-SAM, CP-SAM, TR-SAM and P-SAM.

6.3.1.15 Cryptographic operation – FCS_COP.1h (DES MAC)

FCS_COP.1.1h The TSF shall perform **calculation and verification of message authentication codes** in accordance with a specified cryptographic algorithm **DES MAC in CBC mode** and cryptographic key sizes **64 or128 bits** that meet the following: **Ref. [18].**

Application note: DES MAC calculation with 64 or 128 bits key length is used for calculation of access credentials. Only valid for: CS-SAM, CP-SAM, and P-SAM.

6.3.1.16 Cryptographic operation – FCS_COP.1i (SHA)

FCS_COP.1.1i The TSF shall perform **calculation of a message digest** in accordance with a specified cryptographic algorithm **SHA-1, SHA-256** and cryptographic key sizes **NA** that meet the following: **Ref. [21].**

Application note: Only used for digital signature calculations and verifications. When calculating signatures the host calculates the hash, not the TOE. The TOE does hash calculations as part of digital signatures but it is not an observable output. Only valid for: CS-SAM and CP-SAM. It is a requirement given by the system design and protocols that the SAM also must support SHA-1 [13]

6.3.1.17 Cryptographic operation – FCS_COP.1j (RSA digital signatures)

FCS_COP.1.1j The TSF shall perform **calculation and verification of digital signatures** in accordance with a specified cryptographic algorithm**s RSASSA-PSS SHA-1, RSASSA-PKCS1-v1-5 SHA-1/SHA-256** and cryptographic key sizes **1024/2048/4096** that meet the following: **RSASSA-PSS, RSASSA-PKCS1-v1-5: Ref. [27]; SHA-1/SHA-256: Ref. [21].**

Application note: Only valid for: M-SAM, CS-SAM, CP-SAM, and P-SAM.

6.3.1.18 Cryptographic operation – FCS_COP.1k (ECC digital signatures)

FCS_COP.1.1k The TSF shall perform **calculation and verification of digital signatures** in accordance with a specified cryptographic algorithm **EC-DSA** and cryptographic key sizes **NIST P-256, NIST P-521 (only verification) and BrainpoolP256r1, SHA-1/SHA-256** that meet the following: **Ref. [22], Ref. [16], and [15]. TR-SAM: Ref. [14] clause 7.1.3; SHA-1/SHA-256: Ref. [21].**

Application note: Verification is not valid for P-SAM. It is a requirement given by the system design and protocols that the SAM also must support SHA-1 [13]

6.3.1.19 Cryptographic operation – FCS_COP.1l (RNG)

FCS_COP.1.1l The TSF shall perform **true random number generation** in accordance with a specified cryptographic algorithm **None** and cryptographic key sizes **NA** that meet the following: **For TR-SAM 1/2: [12].**

Application note: The random number generator is provided by the TOE operational environment.

6.3.2 User Data Protection - FDP

6.3.2.1 Subset access control – FDP_ACC.1

FDP_ACC.1.1 The TSF shall enforce the **Access Condition Policy** on

Subject:	**User**
Objects:	**Master file,** **Elementary files, and** **Individual keys stored in a file**
Operations:	**TOE Commands covered by access conditions according to ref. [6].**

6.3.2.2 Security attribute based access control – FDP_ACF.1

FDP_ACF.1.1 The TSF shall enforce the **Access Condition Policy** to objects based on the following **subjects, objects and resp. attributes:**

		Attributes:
Subjects:	**Users**	**PINs, Challenge, Nonce, MAC, Start-up usage counter, Security critical commands usage counter, Host Authenticated Mode indicator**
Objects:	**Master file**	**File identifier, Access conditions: ALW, PwdGx, AutGSx, AutDHx, ProGSx, NEV**
	Elementary files	**File identifier, Access conditions: ALW, PwdGx, AutGSx, AutDHx, ProGSx, NEV**
	Individual keys	**Key identifier (record number in file), Access conditions: ALW, PwdGx, AutGSx, AutDHx, ProGSx, NEV**

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

a) Users may access objects which have the PwdGx access condition defined only if the user has been authenticated by the PIN x before the access. (Only valid for: M-SAM, CS-SAM and P-SAM)

b) Users may access objects which have the AutGSx access condition defined only if the user has been authenticated using challenge response and the administrative symmetric key with index x before the access. (Only valid for: CS-SAM, CP-SAM, TR-SAM and P-SAM)

c) Users may access objects which have the AutDHx access condition defined only if the user has been authenticated using a challenge response and a symmetric session key as the result of a Diffie-Hellman key agreement scheme. If x=0 a Nonce will be sent by the TOE, if x=1 a Nonce will be received by the TOE.

d) Users may access objects which have the ProGSx access condition defined only if a MAC is calculated over the whole data field of the command using the administrative symmetric key with identifier x. (Only valid for: CS-SAM, CP-SAM and P-SAM)

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules:

a) Users may always access objects which have the ALW access condition defined using TOE commands.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

a) Users shall be denied access to objects which have the NEV access condition defined.

b) Users shall be denied access to objects if the usage counters requests re-authentication (i.e. is/are configured to be used and has/have reached zero). (Only valid for: CS-SAM, CP-SAM and P-SAM)

c) Users shall be denied to load the SD Issuing CA container more than once (overwrite).

d) Users shall be denied to load the SD public key container more than once (overwrite).

e) Users shall be denied to generate SD asymmetric key pair more than once (overwrite).

f) Access to Factory Authentication key shall be denied for all other commands than: Load SD Issuing CA Container, Load SD Target CA Container, Generate SD Key Pair, and Generate Admin Transfer Key(commands according to ref. [6]).

g) If a command is not explicitly allowed for a key, it shall be denied.

h) Data authentication requests to the TOE (TR-SAM) shall be denied when the value of the referenced Toll Domain Counter has reached its maximum. (Only valid for TR-SAM 1/2)

Application note: A Toll Domain Counter in the TR-SAM configuration 1 and 2 is incremented at each authentication request from a Toll Domain. See ref. [14] for more information.

6.3.2.3 Subset information flow control – FDP_IFC.1

FDP_IFC.1.1 The TSF shall enforce the **Import/Export Key Policy** on

Subject:	**Users**
Information:	**Admin Keys and Non-admin Keys.**
Operations:	**Import and export**

6.3.2.4 Simple security attributes – FDP_IFF.1

FDP_IFF.1.1 The TSF shall enforce the **Import/Export Key Policy** based on the following types of subject and information security attributes:

		Attributes:
Subjects:	**Users**	**PINs, Challenge, Nonce**
Information:	**Admin Keys**	**Key identifier**
	Non-admin Keys	**Key identifier**

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

a) The user and the TOE shall be mutually authenticated by a Diffie-Hellman key exchange scheme before importing Admin Keys.

b) The user and the TOE shall be mutually authenticated using a challenge response and a symmetric session key as the result of a Diffie-Hellman key agreement scheme before exporting Admin Keys. (Only valid for M-SAM, CS-SAM, and P-SAM)

c) The user and the TOE shall be mutually authenticated by challenge-response schemes based on Admin Keys before importing Non-admin Keys.

d) The user and the TOE shall be mutually authenticated by challenge-response schemes based on Admin Keys before exporting Non-admin Keys. (Only valid for M-SAM, CS-SAM, and P-SAM)

e) The user shall be authenticated by a PIN before importing Non-admin Keys. (Only valid for CS-SAM)

f) The user shall be authenticated by a PIN before exporting Non-admin Keys. (Only valid for M-SAM, CS-SAM, and P-SAM)

FDP_IFF.1.3 The TSF shall enforce the **additional information flow control SFP rules: None.**

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: **None.**

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules:

a) It shall not be possible to export derived keys other than explicitly derived for the DERIVE KEY External Export command. (Only valid for CS-SAM and P-SAM)

b) A Trusted Recorder master key, derived TR key, or internally calculated MAC shall not be possible to export. (Only valid for TR-SAM)

6.3.2.5 Export of user data with security attributes – FDP_ETC.2

FDP_ETC.2.1 The TSF shall enforce the **Import/Export Key Policy** when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.2.2 The TSF shall export the user data with the user data's associated security attributes.

FDP_ETC.2.3 The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.

FDP_ETC.2.4 The TSF shall enforce the following rules when user data is exported from the TOE:

a) Export of Admin Keys:
Admin Keys shall be encrypted using AES-CBC and a 256 bits key encryption key, Admin Transfer encryption key. An CMAC using a 256 bits key authentication key, Admin Transfer authentication key, shall be applied. (Only valid for M-SAM, CS-SAM, and P-SAM)

b) Export of Non-admin Keys using symmetric methods:
Non-admin Keys shall be decrypted using AES-CBC and a 256 bits key encryption key. (Only valid for M-SAM, CS-SAM, and P-SAM)

c) Export of Non-admin Keys using asymmetric methods:
Non-admin Keys shall be encrypted using RSA 2048 bits key. A RSA digital signature shall be applied using 2048 bits key. (Only valid for M-SAM)

d) Derived AES 128/256 bits key and derived DES 64 bits keys shall be possible to export in plain text in a physically secure environment. (Only valid for CS-SAM and P-SAM)

6.3.2.6 Import of user data with security attributes – FDP_ITC.2

FDP_ITC.2.1 The TSF shall enforce the **Import/Export Key Policy** when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.2.2 The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3 The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

FDP_ITC.2.4 The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.5 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE:

a) **Import of Admin Keys:**
Admin Keys shall be decrypted using AES-CBC and a 256 bits key encryption key, Admin Transfer encryption key. An AES MAC using CBC and a 256 bits key authentication key, Admin Transfer authentication key, shall be verified. The Admin Transfer keys shall only be used for import and export of Admin keys. (Only valid for CS-SAM, CP-SAM, TR-SAM, and P-SAM)

b) **Import of Non-admin Keys using symmetric methods:**
Non-admin Keys shall be decrypted using AES-CBC and a 256 bits key encryption key. (Only valid for CS-SAM, CP-SAM, TR-SAM, and P-SAM)

c) **Import of Non-admin Keys using asymmetric methods:**
Non-admin Keys shall be decrypted using RSA 2048 bits key.

d) **Import of KMS Issuing CA container:**
The integrity and authenticity of the KMS Issuing CA container shall be verified using a digital signature verified against the pre-loaded KMS Root CA public key.

e) **Import of SD container:**
The integrity and authenticity of the SD container shall be verified using a digital signature verified against the loaded KMS Issuing CA public key.

6.3.3 Identification and Authentication – FIA

6.3.3.1 Authentication failure handling – FIA_AFL.1a (PIN)

FIA_AFL.1.1a The TSF shall detect when **three** unsuccessful authentication attempts occur related to **authentication using PIN**.

FIA_AFL.1.2a When the defined number of unsuccessful authentication attempts has been **met** the TSF shall

- **block/disable commands secured by PwdGx,**
- **allow unblocking the TOE using a dedicated unblocking PIN**.

Application note: There are two PINs defined each with a dedicated unblocking PIN. Which of the two PIN's, if any, the user shall supply for authentication is set by access conditions. Only valid for M-SAM, CS-SAM, and P-SAM.

6.3.3.2 Authentication failure handling – FIA_AFL.1b (Unblocking)

FIA_AFL.1.1b The TSF shall detect when **seven** unsuccessful authentication attempts occur related to **unblocking the TOE**.

FIA_AFL.1.2b When the defined number of unsuccessful authentication attempts has been **met** the TSF shall

- **block/disable commands secured by PwdGx,**

- **disallow unblocking the TOE using the dedicated unblocking PIN.**

Application note: There are two PINs defined, each with a dedicated unblocking PIN. Which of the two PIN's, if any, the user shall supply for authentication is set by access conditions. Only valid for M-SAM, CS-SAM, and P-SAM.

6.3.3.3 Verification of secrets – FIA_SOS.1

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that **PINs** meet **the length of eight bytes, each byte with possible values of 0x00 – 0xFF**.

Application note: Only valid for M-SAM, CS-SAM, and P-SAM.

6.3.3.4 Timing of authentication – FIA_UAU.1

FIA_UAU.1.1 The TSF shall allow **commands that does not have the PwdGx, AutGSx, AutDHx or ProGSx access conditions defined** 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.

Application note: The PwdGX authentication method is only valid for M-SAM, CS-SAM, and P-SAM), the AutGSx is only valid for CS-SAM, CP-SAM, TR-SAM, and P-SAM, the ProGSx is only valid for CS-SAM, CP-SAM, and P-SAM).

6.3.3.5 Multiple authentication mechanisms – FIA_UAU.5

FIA_UAU.5.1 The TSF shall provide **the following mechanisms:**

- **Verification of a user supplied PIN, PwdGx (M-SAM, CS-SAM, P-SAM)**
- **Verification using challenge – response, AutGSx (CS-SAM, CP-SAM, TR-SAM, and P-SAM)**
- **Verification using a Diffie-Hellman key exchange scheme, AutDHx**
- **Verification using a calculated MAC, ProGSx (CS-SAM, CP-SAM, and P-SAM)**

to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the **access conditions defined for the object accessed by the requested TOE command.**

Application note: There are two PINs defined. Which of the two PIN's the user shall supply for authentication is set by access conditions. The PIN values can be changed by a management function command. The authentication mechanisms are defined in ref. [13].

6.3.3.6 Re-authenticating – FIA_UAU.6

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

- **The TOE is configured to use the Start-up Usage Counter and it has reached zero: Authentication to fulfill the AutGS1 access condition is required.**
- **The TOE is configured to use the Security Critical Commands Usage Counter and it has reached zero: Authentication is required before executing any of the security critical commands:**
  - **CALCULATE ACCESS CREDENTIALS,**
  - **CALCULATE AES MAC,**
  - **CALCULATE DES MAC,**
  - **DECRYPT DATA**
  - **DERIVE KEY EXTERNAL EXPORT,**
  - **ENCRYPT DATA**
  - **OBU KEY PERSONALISATION,**
  - **VERIFY AES MAC,**
  - **VERIFY DES MAC,**
  - **DECRYPT DATA ASYM, or**
  - **SIGN DATA.**
- **If the TOE is configured to use both the Start-up Usage Counter and the Security Critical Commands Usage Counter, the Security Critical Commands Usage Counter will be reset to its preconfigured initial value when the Start-up Usage Counter is decremented and has not reached zero**.

Application note: Only valid for CS-SAM, CP-SAM, and P-SAM. Please see ref. [6] for descriptions of the security critical commands.

6.3.4 Security Management – FMT

6.3.4.1 Static attribute initialisation – FMT_MSA.3

FMT_MSA.3.1 The TSF shall enforce the **Access Condition Policy** to provide **the NEV access condition as** default values for **access conditions of dynamically created objects** that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow **none** to specify alternative initial values to override the default values when an object or information is created.

6.3.4.2 Specification of Management Functions – FMT_SMF.1

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

a) It shall be possible to read out the unique chip serial number of the TOE.

b) The TOE shall support changing and unblocking of PINs. (Only valid for M-SAM, CS-SAM, and P-SAM)

c) It shall possible to reset both Usage Counters to their pre-configured value before they have reached zero without blocking other communication. (Only valid for CS-SAM, CP-SAM and P-SAM)

d) It shall be possible to delete keys, after authentication using an Admin Key (only valid for CS-SAM, CP-SAM, TR-SAM, and P-SAM) or after authentication using PIN verification (only valid for M-SAM, CS-SAM, and P-SAM), accordingly:

- **a. All keys, except the Factory Authentication Key and the SD Key Pair, individually.**
- **b. All symmetric keys, except the Admin Keys (Only valid for CS-SAM, CP-SAM, TR-SAM and P-SAM).**
- **c. All keys, except the Factory Authentication Key and the KMS Root CA public key container. Note: This will bring the TOE to factory settings. Also PINs and counters will be reset to factory default values. (Only valid for CS-SAM, CP-SAM, TR-SAM and P-SAM)**
- **d. A Kill command shall unconditionally erase ALL keys including the Factory Authentication Key and the KMS Root CA public key container. (Only valid for CS-SAM, CP-SAM, TR-SAM and P-SAM)**

e) It shall be possible to obtain the following information about a key:

- **a. The key unique identifier**
- **b. The Key Verification Code, KVC (for symmetric keys)**
- **c. The key derivation counter (Only valid for P-SAM)**

f) At key generation is shall be possible to define a set of commands allowed for the key. The set of commands shall be possible to change after generation.

g) It shall be possible to modify and delete the access conditions of dynamically created objects.

Application note: The key derivation counter is only used in the P-SAM and is monotonically incremented every time a key is derived from the key. The derivation counter shall start on zero and not be possible to reset until the key is deleted. The derivation counter shall stop when reaching its maximum value and reject further derivations to be performed.

6.3.5 Protection of the TSF – FPT

6.3.5.1 Replay Detection – FPT_RPL.1

FPT_RPL.1.1 The TSF shall detect replay for the following entities:

At commands:

- **Export of Admin Keys (Only valid for M-SAM, CS-SAM, and P-SAM)**
- **Export of Non-admin Keys (Only valid for M-SAM, CS-SAM, and P-SAM)**
- **Import of Non-admin Keys (Only valid for CS-SAM, CP-SAM, TR-SAM, and P-SAM)**
- **Import of Admin Keys (Only valid for CS-SAM, CP-SAM, TR-SAM, and P-SAM)**
- **Reading encrypted binary file content**
- **Update encrypted binary file content**

The replay shall be detected by using a random number, received from a previously issued get challenge command, as initialisation vector, IV, for the encryption/decryption of the data.

If the Backup-key is used for the encryption the IV will be set to zero and no replay detection will be possible.

FPT_RPL.1.2 The TSF shall **discard the command** when replay is detected.

6.3.5.2 Testing of External Entities – FPT_TEE.1

FPT_TEE.1.1 The TSF shall run a suite of tests **during initial start-up** to check the fulfilment of **the integrity of the Memory Protection Unit's, MPU, configuration and the Non-Volatile Memory, NVM.**

FPT_TEE.1.2 If the test fails, the TSF shall **be possible to be informed about the test results.**

6.4 Security Assurance Requirements

The security assurance requirements according to Table 22 have been chosen. The comprise EAL5.

Assurance Class	Assurance Component Name	Component
ADV: Development	Security architecture description	ADV_ARC.1
	Complete semi-functional specification with additional error information	ADV_FSP.5
	Implementation representation of the TSF	ADV_IMP.1
	Well-structured internals	ADV_INT.2
	Semiformal modular design	ADV_TDS.4
AGD: Guidance documents	Operational user guidance	AGD_OPE.1
	Preparative procedures	AGD_PRE.1
ALC: Life-cycle support	Production support, acceptance procedures and automation	ALC_CMC.4
	Development tools CM coverage	ALC_CMS.5
	Delivery procedures	ALC_DEL.1
	Identification of security measures	ALC_DVS.1
	Developer defined life-cycle model	ALC_LCD.1
	Compliance with implementation standards	ALC_TAT.2
ASE: Security Target evaluation	Conformance claims	ASE_CCL.1
	Extended components definition	ASE_ECD.1
	ST introduction	ASE_INT.1
	Security objectives	ASE_OBJ.2
	Derived security requirements	ASE_REQ.2
	Security problem definition	ASE_SPD.1
	TOE summary specification	ASE_TSS.1
ATE: Tests	Analysis of coverage	ATE_COV.2
	Testing: modular design	ATE_DPT.3
	Functional testing	ATE_FUN.1
	Independent testing – sample	ATE_IND.2
AVA: Vulnerability assessment	Methodical vulnerability analysis	AVA_VAN.4

Table 22, Security Assurance Requirements

6.5 Security Requirements Rationale

6.5.1 Security Functional Requirements Dependencies

Requirement	Direct explicit dependencies	Dependencies met by	Comment
FCS_CKM.1a	[FCS_CKM.2 or FCS_COP.1] and FCS_CKM.4	FCS_COP.1a, FCS_COP.1g, FCS_COP.1e and FCS_CKM.4	
FCS_CKM.1b	[FCS_CKM.2 or FCS_COP.1] and FCS_CKM.4	FCS_COP.1b, FCS_COP.1h and FCS_CKM.4	
FCS_CKM.1c	[FCS_CKM.2 or FCS_COP.1] and FCS_CKM.4	FCS_COP.1f, FCS_COP.1j and FCS_CKM.4	
FCS_CKM.1d	[FCS_CKM.2 or FCS_COP.1] and FCS_CKM.4	FCS_COP.1k and FCS_CKM.4	
FCS_CKM.1e	[FCS_CKM.2 or FCS_COP.1] and FCS_CKM.4	FCS_COP.1a and FCS_CKM.4	
FCS_CKM.3	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] and FCS_CKM.4	--- FCS_CKM.4	The backup key is pre-loaded in TOE at the Personalization phase.
FCS_CKM.4	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	FDP_ITC.2 and FCS_CKM.1a - e	Both generated and imported keys are deleted.
FCS_COP.1a	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] and FCS_CKM.4	FCS_CKM.1a, FCS_CKM.1e, FDP_ITC.2 and FCS_CKM.4	Both generated and imported keys are used for AES encryption/decryption.
FCS_COP.1b	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] and FCS_CKM.4	FCS_CKM.1b, FDP_ITC.2 and FCS_CKM.4	Both generated and imported keys are used for DES encryption/decryption.
FCS_COP.1c	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] and FCS_CKM.4	FCS_CKM.1a, FCS_CKM.1e, FDP_ITC.2 and FCS_CKM.4	Both generated and imported keys are used for AES key derivation.

Requirement	Direct explicit dependencies	Dependencies met by	Comment
FCS_COP.1d	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] and FCS_CKM.4	FCS_CKM.1b, FDP_ITC.2 and FCS_CKM.4	Both generated and imported keys are used for DES key derivation.
FCS_COP.1e	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] and FCS_CKM.4	FCS_CKM.1a, FCS_CKM.1e, FDP_ITC.2 and FCS_CKM.4	Both generated and imported keys are used for AES key encryption.
FCS_COP.1f	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] and FCS_CKM.4	FCS_CKM.1c, FDP_ITC.2, and FCS_CKM.4	Both generated and imported keys are used for RSA encryption/decryption
FCS_COP.1g	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] and FCS_CKM.4	FCS_CKM.1a, FCS_CKM.1e, FDP_ITC.2 and FCS_CKM.4	Both generated and imported keys are used for AES MAC.
FCS_COP.1h	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] and FCS_CKM.4	FCS_CKM.1b, FDP_ITC.2 and FCS_CKM.4	Both generated and imported keys are used for DES MAC.
FCS_COP.1i	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] and FCS_CKM.4	--- ---	No keys are used for SHA-1 calculation.
FCS_COP.1j	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] and FCS_CKM.4	FCS_CKM.1c, and FCS_CKM.4	
FCS_COP.1k	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] and FCS_CKM.4	FCS_CKM.1d and FCS_CKM.4	
FCS_COP.1l	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] and FCS_CKM.4	FCS_COP.1a, FCS_COP.1b and FCS_CKM.4	
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1	
FDP_ACF.1	FDP_ACC.1 and FMT_MSA.3	FDP_ACC.1 FMT_MSA.3	
FDP_ETC.2	FDP_ACC.1 or FDP_IFC.1	FDP_IFC.1	

Requirement	Direct explicit dependencies	Dependencies met by	Comment
FDP_IFC.1	FDP_IFF.1	FDP_IFF.1	
FDP_IFF.1	FDP_IFC.1 and FMT_MSA.3	FDP_IFC.1	FMT_MSA.3 is not applicable since no default values exists for the security attributes.
FDP_ITC.2	[FDP_ACC.1 or FDP_IFC.1] and [FTP_ITC.1 or FTP_TRP.1] and FPT_TDC.1	FDP_IFC.1 --- ---	Imported keys are always encrypted no trusted channel is needed. Consistency with the user (the host) is assured at integration not at run-time. FPT_TDC.1 is not needed.
FIA_AFL.1a	FIA_UAU.1	FIA_UAU.1	
FIA_AFL.1b	FIA_UAU.1	FIA_UAU.1	
FIA_SOS.1	-	-	
FIA_UAU.1	FIA_UID.1	Not met	No identification is required in this single user system.
FIA_UAU.5	-	-	
FIA_UAU.6	-	-	
FMT_MSA.3	FMT_MSA.1 and FMT_SMR.1	- -	Restrictions to access security attributes are controlled by access conditions. The TOE is not aware of roles.
FMT_SMF.1	-	-	
FPT_RPL.1	-	-	
FPT_TEE.1	-	-	

Table 23, SFR dependencies

6.5.2 Security Assurance Dependencies Analysis

The chosen evaluation assurance level is EAL5 and all dependencies are met internally by the EAL package.

6.5.3 Security Functional Requirements Coverage

	O.Authentication	O.Confidentiality	O.Crypto	O.Keys	O.Integrity	O.Replay-Detection	O.Memory_Test
FCS_CKM.1a				X			
FCS_CKM.1b	X			X			
FCS_CKM.1c				X			
FCS_CKM.1d	X			X			
FCS_CKM.1e				X			
FCS_CKM.3				X			
FCS_CKM.4				X			
FCS_COP.1a			X				
FCS_COP.1b			X				
FCS_COP.1c			X				
FCS_COP.1d			X				
FCS_COP.1e		X	X				
FCS_COP.1f		X	X				
FCS_COP.1g			X		X		
FCS_COP.1h			X				
FCS_COP.1i			X		X		
FCS_COP.1j			X		X		
FCS_COP.1k			X		X		
FCS_COP.1l	X		X	X			
FDP_ACC.1	X						
FDP_ACF.1	X						
FDP_ETC.2		X			X		
FDP_IFC.1	X						
FDP_IFF.1	X						
FDP_ITC.2		X			X		
FIA_AFL.1a	X						
FIA_AFL.1b	X						
FIA_SOS.1	X						
FIA_UAU.1	X						
FIA_UAU.5	X						
FIA_UAU.6	X						
FMT_MSA.3	X						

	O.Authentication	O.Confidentiality	O.Crypto	O.Keys	O.Integrity	O.Replay-Detection	O.Memory_Test
FMT_SMF.1	X			X			
FPT_RPL.1						X	
FPT_TEE.1							X

Table 24, Security Functional Requirements Coverage

6.5.4 Security Functional Requirements Sufficiency

Objective	SFR	Rationale
O.Authentication The TOE must provide measures against unauthorised access to sensitive assets and functionality of the TOE.	**FCS_COP.1l** **FCS_COP.1b** **FCS_COP.1d** **FDP_ACC.1** **FDP_ACF.1** **FDP_IFC.1** **FDP_IFF.1** **FIA_AFL.1a** **FIA_AFL.1b** **FIA_SOS.1** **FIA_UAU.1** **FIA_UAU.5** **FIA_UAU.6** **FMT_MSA.3** **FMT_SMF.1**	Authentication (**FIA_UAU.1**) is required for operations on objects according to access conditions (**FDP_IFC.1, FDP_IFF.1, FDP_ACC.1, FDP_ACF.1**) using the NEV access condition as default on dynamically created objects (**FMT_MSA.3**). Authentication shall be obtained either by PIN or challenge-response (**FIA_UAU.5**) and re-authentication shall be performed with intervals according defined counters (**FIA_UAU.6**). PINs shall be of a certain length (**FIA_SOS.1**) and shall be blocked after unsuccessful authentication attempts (**FIA_AFL.1a**) but possible to be unblocked (**FIA_AFL.1b, FMT_SMF.1**). Challenges shall be random (**FCS_COP.1l**). Access credentials shall be created by DES using 64/128 bits keys (**FCS_COP.1b, FCS_COP.1d)**.
O.Confidentiality The TOE shall provide measures against disclosure of Admin Keys and Non-admin Keys at import and export.	**FCS_COP.1e** **FCS_COP.1f** **FDP_ETC.2** **FDP_ITC.2**	AES-CBC 256 bits keys shall be used for encryption/decryption (**FCS_COP.1e**) of Admin Keys and Non-Admin Keys at export (**FDP_ETC.2**) and import (**FDP_ITC.1**). RSA with 2048 bits keys shall be used for encryption/decryption (**FCS_COP.1f**) of Non-admin Keys at export (**FDP_ETC.2**) and import (**FDP_ITC.2**).
O.Crypto The TOE shall provide cryptographic mechanisms to encrypt and decrypt user data.	**FCS_COP.1a** **FCS_COP.1b** **FCS_COP.1c** **FCS_COP.1d** **FCS_COP.1e**	AES and DES encryption/decryption shall be provided for user data (**FCS_COP.1a, FCS_COP.1b**). AES MAC and DES MAC shall be provided for message authentication

Objective	SFR	Rationale
The TOE shall provide cryptographic mechanisms to calculate and verify message authentication codes over user data. The TOE shall provide cryptographic mechanisms to calculate and verify digital signatures over user data. The TOE shall provide cryptographic mechanisms to derive keys. The TOE shall provide cryptographic mechanisms to encrypt and decrypt keys. The TOE shall provide cryptographic mechanisms to generate random data for key and challenge generation.	**FCS_COP.1f** **FCS_COP.1g** **FCS_COP.1h** **FCS_COP.1i** **FCS_COP.1j** **FCS_COP.1k** **FCS_COP.1l**	calculations and verifications over user data (**FCS_COP.1g, FSC_COP.1h**). RSA and ECC digital signatures shall be provided for user data (**FCS_COP.1i, FCS_COP.1j, FCS_COP.1k**). AES and DES algorithms shall be provided for key derivation (**FCS_COP.1c, FCS_COP.1d**). AES and DES algorithms shall be provided for key encryption and decryption (**FCS_COP.1e, FCS_COP.1f**). Random data generation shall be provided using AES and TDES (**FCS_COP.1l**).
O.Keys The TOE shall provide secure mechanisms to generate, derive, import, export, and backup keys. The TOE shall increment a derivation counter monotonically every time a key is derived. The derivation counter shall start on zero and shall not be possible to reset after SAM production until the key is deleted.	**FCS_CKM.1a** **FCS_CKM.1b** **FCS_CKM.1c** **FCS_CKM.1d** **FCS_CKM.1e** **FCS_CKM.3** **FCS_CKM.4**	Generation of AES 128/256, DES 64/128, RSA 1024/2048/4096, ECC 256/521 bits key shall be provided (**FCS_CKM.1a, FCS_CKM.1b, FCS_CKM.1c, FCS_CKM.1d**). Generation of symmetric keys using EC DH and SHA-256 shall be provided (**FCS_CKM.1e**). Encrypted backu of keys shall be performed (**FCS_CKM.3**). Keys shall be deleted using overwriting (**FCS_CKM.4**).
O.Integrity The TOE shall provide measures to ensure integrity and authenticity of Admin Keys and Non-admin Keys at import and export. The TOE shall provide measures ensure integrity and authenticity of KMS Issuing CA container and SD container at import.	**FCS_COP.1g** **FCS_COP.1i** **FCS_COP.1j** **FCS_COP.1k** **FDP_ETC.2** **FDP_ITC.2**	Both AES MAC, DES MAC, RSA digital signatures, and ECC digital signatures shall be used to ensure integrity of assets (**FCS_COP.1g, FCS_COP.1i, FCS_COP.1j, FCS_COP.1k, FDP_ETC.2, FDP_ITC.2**).
O.Replay_Detection The TOE must detect attempts to replay TOE commands.	**FPT_RPL.1**	Replay attempts on import/export of keys and reading/updating of binary file contents shall be detected (**FPT_RPL.1**).
O.Memory_Test The TOE shall detect memory deficiencies in the operational environment at initial start-up.	**FPT_TEE.1**	Memory tests shall be done at initial start-up (**FPT_TEE.1**).

Table 25, Security Functional Requirements Sufficiency

6.5.5 Justification of the Chosen Evaluation Assurance Level

The assurance level EAL5 has been chosen as appropriate for a Secure Application Module since it provides a moderate level of assured security, and a thorough investigation of the TOE.

It is assumed that the TOE is operated in an environment where attackers have public or moderate expertise of the involved systems (e.g., general and publicly available knowledge about the technology area), resources and motivation are assumed to be high because of possible high-value assets protected by the TOE and the opportunity for an attack is varies between the deployment scenarios. The overall attack potential is assumed to be moderate, which means that EAL5 and AVA_VAN.4 is considered an appropriate assurance level.

The assurance requirements are not reproduced in this protection profile as they are chosen from Common Criteria Part 3, without any alterations done to the SARs.

7 TOE Summary Specification

This section presents information to how the TOE meets the functional requirements described in previous sections of this ST.

7.1 TOE Security Functions

Each of the security requirements and the associated descriptions correspond to security functions. Hence, each function is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functions and rationalize that the security functions satisfy the necessary requirements. Table 26 lists the security functions and their associated SFRs.

TOE Security Function	SFR	Description
Cryptographic Support	FCS_CKM.1a	Cryptographic key generation – AES
	FCS_CKM.1b	Cryptographic key generation – DES
	FCS_CKM.1c	Cryptographic key generation – RSA
	FCS_CKM.1d	Cryptographic key generation – ECC
	FCS_CKM.1e	Cryptographic key generation – EC DH
	FCS_CKM.3	Cryptographic key access - Backup
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1a	Cryptographic operation – AES encrypt/decrypt
	FCS_COP.1b	Cryptographic operation – DES encrypt/decrypt
	FCS_COP.1c	Cryptographic operation – AES key derivation
	FCS_COP.1d	Cryptographic operation – DES key derivation
	FCS_COP.1e	Cryptographic operation – AES key encrypt
	FCS_COP.1f	Cryptographic operation – RSA encrypt/decrypt
	FCS_COP.1g	Cryptographic operation – AES MAC
	FCS_COP.1h	Cryptographic operation – DES MAC
	FCS_COP.1i	Cryptographic operation – SHA-1
	FCS_COP.1j	Cryptographic operation – RSA digital signature
	FCS_COP.1k	Cryptographic operation – ECC digital signature
	FCS_COP.1l	Cryptographic operation - RNG
User Data Protection	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute access control

TOE Security Function	SFR	Description
	FDP_ETC.2	Export of user data with security attributes
	FDP_IFC.1	Subset information flow control
	FDP_IFF.1	Simple security attributes
	FDP_ITC.2	Import of user data with security attributes
Identification and Authentication	FIA_AFL.1a	Authentication failure handling - PIN
	FIA_AFL.1b	Authentication failure handling – Challenge-response
	FIA_SOS.1	Verification of secrets
	FIA_UAU.1	Timing of authentication
	FIA_UAU.5	Multiple authentication mechanisms
	FIA_UAU.6	Re-authenticating
Security Management	FMT_MSA.3	Static attribute initialisation
	FMT_SMF.1	Specification of Management Functions
Protection of the TSF	FPT_RPL.1	Replay Detection
	FPT_TEE.1	Testing of External Entities

Table 26, TOE Security Functions

7.2 Cryptographic Support

The TOE provides cryptographic support to the user and for the protection of the TSF. The cryptographic support includes encryption and decryption of data and keys using AES, DES, RSA and ECC algorithms. Authentication of data is provided as AES and DES MAC calculation and verification as well as digital signatures using RSA or ECC algorithms. (FCS_COP.1a – l)

Cryptographic keys are generated for AES, DES, RSA, and ECC as well as using an EC DH scheme. (FCS_CKM.1a – e)

Backup is taken of cryptographic keys and keys are destroyed in a secure way. (FCS_CKM.3, FCS_CKM.4)

7.3 User Data Protection

Access control to sensitive assets is restricted by an access control policy, Access Condition Policy (FDP_ACC.1) that requires authentication according to configurable access conditions (FDP_ACF.1).

Import and export of sensitive assets are restricted by an information flow control policy, Import/Export Key Policy (FDP_IFC.1), that requires authentication before import or export can take place (FDP_IFF.1) and ensures that the assets are confidentiality, integrity, and authentication protected (FDP_ETC.2, FDP_ITC.2).

7.4 Identification and Authentication

Authentication (FIA_UAU.1) is required according to access conditions set for each asset. The authentication can be performed either by PIN, a challenge-response scheme, a Diffie-Hellman key exchange scheme, or a calculated MAC authentication code (FIA_UAU.5). Re-authentication is required according to configurable conditions (FIA_UAU.6). The PIN secrets shall be of a certain length

(FIA_SOS.1) and unsuccessful authentication attempts shall block the PIN (FIA_AFL.1a). Unsuccessful attempts to unblock the PIN shall block the unblocking function (FIA_AFL.1b).

7.5 Security Management

Certain management functions can be performed (FMT_SMF.1) and the access condition security attributes shall have restricted default values (FMT_MSA.3).

7.6 Protection of the TSF

Measures are applied to detect replay attempts at export and import of keys as well as for reading and updating binary file contents within the TOE (FPT_RPL.1).

Memory provided by the operational environment is functionally tested at start-up (FPT_TEE.1) and the result can be read by the user.

8 Statement of Compatibility

8.1 TSF

The platform SFRs from Security IC Platform Protection Profile, BSI-PP-0035, ref. [8], and Security Target Lite, M9900, M9905, M9906 including optional Software Libraries RSA - EC – Toolbox – FTL, Infineon Technologies AG, ref. [9], have been separated into Irrelevant Platform-SFRs, IP, not being used by the TOE, and Relevant Platform-SFRs, RP, being used by the TOE. The separation is presented in Table 27.

SFR	SFR Name	Ref.	IP	RP
FRU_FLT.2	Limited fault tolerance	[8]		X
FPT_FLS.1	Failure with preservation of secure state	[8]		X
FMT_LIM.1	Limited capabilities	[8]		X
FMT_LIM.2	Limited availability	[8]		X
FAU_SAS.1	Audit storage	[8]		X
FPT_PHP.3	Resistance to physical attack	[8]		X
FDP_ITT.1	Basic internal transfer protection	[8]		X
FPT_ITT.1	Basic internal TSF data transfer protection	[8]		X
FDP_IFC.1	Subset information flow control	[8]		X
FPT_TST.2	Subset TOE security testing	[9]		X
FDP_ACC.1	Subset access control	[9]		X
FDP_ACF.1	Security attribute based access control	[9]		X
FMT_MSA.1	Management of security attributes	[9]		X
FMT_MSA.3	Static attribute initialization	[9]		X
FMT_SMF.1	Specification of Management functions	[9]		X
FCS_COP.1/DES-112[1]	Cryptographic support	[9]		X
FCS_COP.1/DES-168[1]	Cryptographic support	[9]		X
FCS_COP.1/AES-128[1]	Cryptographic support	[9]		X
FCS_COP.1/AES-192[1]	Cryptographic support	[9]	X	
FCS_COP.1/AES-256[1]	Cryptographic support	[9]		X
FCS_COP.1/RSA RSAEP/RSADP 1024	Cryptographic support	[9]	X	
FCS_COP.1/RSA RSAEP/RSADP 2048	Cryptographic support	[9]		X
FCS_COP.1/RSA RSAEP/RSADP 4096	Cryptographic support	[9]	X	

[1] Hardware interface is used in ECB and CBC modes

SFR	SFR Name	Ref.	IP	RP
FCS_CKM.1/RSA-1024	Cryptographic key generation	[9]	X	
FCS_CKM.1/RSA-2048	Cryptographic key generation	[9]		X
FCS_CKM.1/RSA-4096	Cryptographic key generation	[9]	X	
FCS_COP.1/ECDSA-P-{256, 521}, Brainpool P256r1	Cryptographic support	[9]		X
FCS_COP.1/ECDSA-P-{192, 224, 384}, K-{163, 233, 409}, B-{233, 283, 409}, Brainpool P{160, 192, 224, 320, 384, 512} r1, Brainpool P{160, 192, 224, 256, 320, 384, 512} t1	Cryptographic support	[9]	X	
FCS_CKM.1/EC-P-{256, 521}	Cryptographic support	[9]		X
FCS_CKM.1/EC-P-{192, 224, 384}, K-{163, 233, 409}, B-{233, 283, 409}, Brainpool P{160, 192, 224, 256, 320, 384, 512} r1, Brainpool P{160, 192, 224, 256, 320, 384, 512} t1	Cryptographic support	[9]	X	
FCS_COP.1/ECDH-P-{256, 521}	Cryptographic support	[9]		X
FCS_COP.1/ECDH-P-{192, 224, 384}, K-{163, 233, 409}, B-{233, 283, 409}, Brainpool P{160, 192, 224, 256, 320, 384, 512} r1, Brainpool P{160, 192, 224, 256, 320, 384, 512} t1	Cryptographic support	[9]	X	
FDP_SDI.1	Stored data integrity monitoring	[9]		X
FDP_SDI.2	Stored data integrity monitoring and action	[9]		X
FCS_RNG.1	Quality metric for random numbers	[9]		X

Table 27, Irrelevant and relevant platform-SFRs

From Table 27 can be deduced that the platform-TSF is complete and consistent. All operations on the relevant platform-SFRs, including refinements, are also appropriate for the TOE.

8.2 Security Assurance Requirements

The platform security assurance requirements, SARs, defined in the IC chip Protection Profile, BSI-PP-0035, ref. [8], and Infineon Security Target, ref. [9], have been compiled together with the SARs from this ST in Table 28.

Security Assurance Requirements	PP [8]	ST [9]	TOE ST
Class ADV: Development			
Architectural design	ADV_ARC.1	ADV_ARC.1	ADV_ARC.1
Functional specification	ADV_FSP.4	ADV_FSP.5	ADV_FSP.5
Implementation representation	ADV_IMP.1	ADV_IMP.1	ADV_IMP.1
TSF Internals		ADV_INT.2	ADV_INT.2
TOE design	ADV_TDS.3	ADV_TDS.4	ADV_TDS.4
Class AGD: Guidance documents			
Operational user guidance	AGD_OPE.1	AGD_OPE.1	AGD_OPE.1
Preparative user guidance	AGD_PRE.1	AGD_PRE.1	AGD_PRE.1
Class ALC: Life-cycle support			
CM capabilities	ALC_CMC.4	ALC_CMC.4	ALC_CMC.4
CM scope	ALC_CMS.4	ALC_CMS.5	ALC_CMS.5
Delivery	ALC_DEL.1	ALC_DEL.1	ALC_DEL.1
Development security	ALC_DVS.2	ALC_DVS.2	ALC_DVS.1
Life-cycle definition	ALC_LCD.1	ALC_LCD.1	ALC_LCD.1
Tools and techniques	ALC_TAT.1	ALC_TAT.2	ALC_TAT.2
Class ASE: Security Target evaluation			
Conformance claims	ASE_CCL.1	ASE_CCL.1	ASE_CCL.1
Extended components definition	ASE_ECD.1	ASE_ECD.1	ASE_ECD.1
ST introduction	ASE_INT.1	ASE_INT.1	ASE_INT.1
Security objectives	ASE_OBJ.2	ASE_OBJ.2	ASE_OBJ.2
Derived security requirements	ASE_REQ.2	ASE_REQ.2	ASE_REQ.2
Security problem definition	ASE_SPD.1	ASE_SPD.1	ASE_SPD.1
TOE summary specification	ASE_TSS.1	ASE_TSS.1	ASE_TSS.1
Class ATE: Tests			
Coverage	ATE_COV.2	ATE_COV.2	ATE_COV.2
Depth	ATE_DPT.2	ATE_DPT.3	ATE_DPT.3
Functional tests	ATE_FUN.1	ATE_FUN.1	ATE_FUN.1
Independent testing	ATE_IND.2	ATE_IND.2	ATE_IND.2

Security Assurance Requirements	PP [8]	ST [9]	TOE ST
Class AVA: Vulnerability assessment			
Vulnerability analysis	AVA_VAN.5	AVA_VAN.5	AVA_VAN.4

Table 28, Security Assurance Requirements

From Table 28 it is evident that the SARs stated for the TOE is a subset of the platform SARs and do not exceed those.

8.3 Security Objectives

8.3.1 Security Objectives for the TOE

The relevant security objectives for the certified platform have been reproduced below for the reader's convenience.

Platform Security Objectives	Ref.
O.Leak-Inherent Protection against Inherent Information Leakage 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 O.Phys-Probing is about direct measurements on elements on the chip surface. Details correspond to an analysis of attack scenarios which is not given here.	[8]
O.Phys-Probing Protection against Physical Probing The TOE must provide protection against disclosure of User Data, against the disclosure/reconstruction of the Security IC Embedded Software or against the disclosure of other critical information about the operation of the TOE. 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.	[8]
O.Malfunction Protection against Malfunctions 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.	[8]
O.Phys-Manipulation Protection against Physical Manipulation The TOE must provide protection against manipulation of the TOE (including its software and Data), the Security IC Embedded Software and the User Data. This includes protection against - reverse-engineering (understanding the design and its properties and functions), - manipulation of the hardware and any data, as well as - controlled manipulation of memory contents (Application Data).	[8]

Platform Security Objectives	Ref.
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.	
O.Leak-Forced Protection against Forced Information Leakage The Security IC must be protected against disclosure of confidential data processed in the Security IC (using methods as described under O.Leak-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 (O.Malfunction)” and/or - by a physical manipulation (refer to “Protection against Physical Manipulation (O.Phys-Manipulation)”. If this is not the case, signals which normally do not contain significant information about secrets could become an information channel for a leakage attack.	[8]
O.Abuse-Func Protection against Abuse of Functionality The TOE must prevent that functions of the TOE which may not be used after TOE Delivery can be abused in order to (i) disclose critical User Data, (ii) manipulate critical User Data of the Security IC Embedded Software, (iii) manipulate Soft-coded Security IC Embedded Software or (iv) 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.	[8]
O.Identification TOE Identification The TOE must provide means to store Initialisation Data and Pre-personalisation Data in its non-volatile memory. The Initialisation Data (or parts of them) are used for TOE identification.	[8]
O.RND Random Numbers The TOE will ensure the cryptographic quality of random number generation. For instance random numbers shall not be predictable and shall have a 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.	[8]
O.Add-Functions Additional Specific Security Functionality The TOE must optionally provide the following specific security functionality to the Smartcard Embedded Software: - Advanced Encryption Standard (AES) - Triple Data Encryption Standard (3DES) - Rivest-Shamir-Adleman (RSA) - Elliptic Curve Cryptography (EC)	[9]
O.Mem-Access Area based Memory Access Control The TOE must provide the Smartcard Embedded Software with the capability to define restricted access memory areas. The TOE must then enforce the partitioning of such memory	[9]

Platform Security Objectives	Ref.
areas so that access of software to memory areas and privilege levels is controlled as required, for example, in a multi-application environment.	

Table 29, Platform security objectives

The platform security objectives are complementing the TOE security objectives by

- Protection from confidential data disclosure on a physical hardware level (O.Leak-Inherent, O.Phys-Probing, O.Leak-Forced)
- Protection from platform malfunction or manipulation (O.Malfunction, O.Phys-Manipulation, O.Abuse-Func, O.Mem-Access)
- Offering means for identification and cryptographic operations (O.Identification, O.RND, O.Add-Functions)

No contradiction between the certified platform and the TOE security objectives has been identified.

8.3.2 Security Objectives for the Environment

The security objectives for the certified platform environment have been reproduced below for the reader's convenience.

Platform Security Objectives for the Environment	Ref.	Met by the TOE
OE.Plat-Appl Usage of Hardware Platform To ensure that the TOE is used in a secure manner the Security IC Embedded Software shall be designed so that the requirements from the following documents are met: (i) hardware data sheet for the TOE, (ii) data sheet of the IC Dedicated Software of the TOE, (iii) TOE application notes, other guidance documents, and (iv) findings of the TOE evaluation reports relevant for the Security IC Embedded Software as referenced in the certification report.	[8]	ADV_ARC ADV_FSP ADV_INT ADV_TDS
OE.Resp-Appl Treatment of User Data Security relevant User Data (especially cryptographic keys) are treated by the Security IC Embedded Software as required by the security needs of the specific application context.	[8]	O.Authentication O.Confidentiality O.Crypto O.Keys O.Integrity O.Replay_Detection O.Memory_Test
OE.Process-Sec-IC Protection during composite product manufacturing Security procedures shall be used after TOE Delivery up to delivery to the end-consumer to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorised use). This means that Phases after TOE Delivery up to the end of Phase 6 (refer to Section 1.2.3) must be protected appropriately. For a preliminary list of assets to be protected refer to paragraph 140H 92 (page 141H 30).	[8]	ALC_CMC ALC_CMS ALC_DEL ALC_DVS ALC_LCD ALC_TAT

Table 30, Platform security objectives for the environment

The platform security objectives for the environment are all met by the requirements in this ST according to the Table 30. No contradictions between the security objectives stated for the platform environment and for the TOE (section 4.3) exist.

8.4 Security Problem Definition

8.4.1 Threats

See section 3.2 for a description of the threats against the TOE and the certified platform.

8.4.2 Organizational Security Policies

See section 3.3 for a description of the OSPs for the TOE and the certified platform.

8.4.3 Assumptions on the Environment

The assumptions for the platform environment have been reproduced below for the reader's convenience. The corresponding objectives are all met by the TOE according to section 8.3.2.

Platform Assumptions on the Environment	Met by objective	Ref.
A.Process-Sec-IC Protection during Packaging, Finishing and Personalisation It is assumed that security procedures are used after delivery of the TOE by the TOE Manufacturer up to delivery to the end-consumer to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorised use). This means that the Phases after TOE Delivery (refer to Sections 119H 1.2.2 and 120H 7.1) are assumed to be protected appropriately. For a preliminary list of assets to be protected refer to paragraph 121H 92 (page 122H 30).	OE.Process-Sec-IC	[8]
A.Plat-Appl Usage of Hardware Platform The Security IC Embedded Software is designed so that the requirements from the following documents are met: (i) TOE guidance documents (refer to the Common Criteria assurance class AGD) such as the hardware data sheet, and the hardware application notes, and (ii) findings of the TOE evaluation reports relevant for the Security IC Embedded Software as documented in the certification report.	OE.Plat-Appl	[8]
A.Resp-Appl Treatment of User Data	OE.Resp-Appl	[8]

Platform Assumptions on the Environment	Met by objective	Ref.
All User Data are owned by Security IC Embedded Software. Therefore, it must be assumed that security relevant User Data (especially cryptographic keys) are treated by the Security IC Embedded Software as defined for its specific application context.		
A.Key-Function Usage of Key-dependent Functions Key-dependent functions (if any) shall be implemented in the Smartcard Embedded Software in a way that they are not susceptible to leakage attacks (as described under T.Leak-Inherent and T.Leak-Forced).	OE.Plat-Appl OE.Resp-Appl	[9]

Table 31, Platform assumptions on the environment

Appendix A – Abbreviations and Acronyms

Acronym or Abbr.	Explanation
Admin Key	Admin Keys are symmetric AES keys used to protect a security domain
AES	Advanced Encryption Standard
CA	Certification Authority
CMAC	Cipher-based MAC
CP-SAM	Communication Point SAM
CS-SAM	Central Services SAM
DES	Data Encryption Standard
DSRC	Dedicated Short Range Communication. Denotes the interface between the OBU and the ES.
FIPS	Federal Information Processing Standards
Host	The host is an actor with its own SAM. Typically this is a central system with an attached CSM.
KMS	Key Management System
KVC	Key Verification Code
MAC	Message Authentication Code
M-SAM	Master SAM
NIST	National Institute of Standards and Technology
Non-Admin Keys	Non-Admin keys are symmetric keys used in operation.
OBU	On Board Unit
OSP	Organisational Security Policy
P-SAM	OBU Personalisation SAM
PIN	Personal Identification Number
RSAES-OAEP	RSA encoding mechanism identical to REM 1 according to ISO/IEC 18033-2:2006 §11.3.2 .
RSAES-PKCS1-v1_5	RSA encoding mechanism identical to REM 1 according to ISO/IEC 18033-2:2006 §11.3.2 .
SAM	Secure Application Module
SD	Security Domain. Within one SD devices have trust in each other. Technically they have the same of Administrative Master keys. One project has one SD.
SHA	Secure Hash Algorithm
SMD	Surface-Mount Device
TOE	Target Of Evaluation
Toll domain	An area or part of a road network where a toll regime is applied
TR	Trusted Recorder

Acronym or Abbr.	Explanation
TSF	TOE Security Functionality

Table 32, Abbreviations and acronyms

Appendix B - Referenced Documents[2]

[1] Common Criteria for Information Technology Security Systems, Part 1: Introduction and general model, Version 3.1, Revision 4, CCMB-2012-09-001, September 2012

[2] Common Criteria for Information Technology Security Systems, Part 2: Security functional requirements, Version 3.1, Revision 4, CCMB-2012-09-002, September 2012

[3] Common Criteria for Information Technology Security Systems, Part 3: Security assurance requirements, Version 3.1, Revision 4, CCMB-2012-09-003, September 2012

[4] SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES, FIPS 140-2, National Institute of Standards and Technology

[5] BSI-DSZ-CC-0827-V6-2017 for Infineon Technologies Smart Card IC (SecurityController) M9900 A22/G11/C22/D22, M9905 A11,M9906 A11 with optional RSAv1.03.006/v2.05.005/v2.07.003, ECv1.03.006/v2.05.005/v2.07.003, Toolboxv1.03.006/v2.05.005/v2.07.003, Flash TranslationLayer V1.01.0008, SCL v2.01.011/v2.02.010 andPSL v4.00.09 libraries with specific IC dedicated software from Infineon Technologies AG

[6] Interface Specification for Kapsch SAM 5000, 8633 803-311, Kapsch TrafficCom AB [1]

[7] https://partners-global.kapschtraffic.com/rfid/Security/Standards/ACQ20121128RFI_TollTechnology.pdf

[8] Security IC Platform Protection Profile, Version 1.0, 15.06.2007, BSI-PP-0035, European Smart Card Industry Association

[9] Security Target Lite, M9900, M9905, M9906 including optional Software Libraries RSA - EC - SCL- PSL, Version 2.8.0, Date 2017-08-18, Infineon Technologies AG

[10] CI97_2-07-003_RSA4k-ECC521_Embedding

[11] IFX Application Notes SLE97 version 2.5.0

[12] NIST-Recommended Random Number Generator Based on ANSI X9.31, Appendix A.2.4, Using the 3-Key Triple DES and AES Algorithms, January 31, 2005, NIST

[13] Device Requirement Specification for Kapsch SAM 5000, 8633 803-253, Kapsch TrafficCom AB [1]

[14] Electronic fee collection — Secure monitoring for autonomous toll systems — Part 2: Trusted recorder, March 2015, CEN/TS 16702-2

[15] RFC 5639, Elliptic Curve Cryptography (ECC) Brainpool Standard, Curves and Curve Generation

[16] ISO/IEC 14888-3:2006, Information technology -- Security techniques -- Digital signatures with appendix -- Part 3: Discrete logarithm based mechanisms

[2] When referenced version is not provided the current version of the applicable document applies. The current version can be found in the SAM 5000 Product Baseline 8633 803-576

[17] ISO/IEC 7816-3:2006, Identification cards -- Integrated circuit cards -- Part 3: Cards with contacts -- Electrical interface and transmission protocols

[18] ISO 16609:2012, Financial services, Requirements for message authentication using symmetric techniques

[19] ISO/IEC 18033-3:2007, Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers

[20] ISO/IEC 18033-3:2005, Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers

[21] FIPS PUB 180-4. Secure Hash Standard (SHS)

[22] FIPS PUB 186-2, Digital Signature Standard (DSS)

[23] ISO/IEC 9797-1:2011, Information technology -- Security techniques – Message Authentication Codes (MACs) -- Part 1: Mechanisms using a block cipher

[24] ISO/IEC 10116:2006, Information technology -- Security techniques -- Modes of operation for an n-bit block cipher

[25] NIST Special Publication 800-38B, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication

[26] NIST Special Publication 800-56A, rev 2, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography

[27] PKCS #1 V2.1, PKCS #1 V2.1: RSA CRYPTOGRAPHY STANDARD (June 14, 2002) from RSA Laboratories

[28] Implementing a NIST SP800-90A Random Bit Generator (DRBG), TRNG post-processing for PTG.3, DRG.4 and FIPS compliance, Application Note, Rev.1.1 2014-09-30