Security Target for CSP on Upteq NFC422 v1.0 JCS platform

Common Criteria
Security Target - Public version
EAL4+

Release	Date (dd/mm/yy)	Author	Modifications
1.3p	29/06/2020	THALES	Created from evaluated ST (V1.3)

Table of content

Table of figures

Tables

1 REFERENCES AND ACRONYMS

1.1 REFERENCE DOCUMENTS

1.1.1 External References

[CC]	Common Criteria references
[CC-1]	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, CCMB-2017-04-001, Version 3.1 Revision 5, April 2017.
[CC-2]	Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, CCMB-2017-04-002, Version 3.1 Revision 5, April 2017.
[CC-3]	Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, CCMB-2017-04-003, Version 3.1 Revision 5, April 2017.
[CEM]	Common Methodology for Information Technology Security Evaluation CCMB-2017-04-004, version 3.1 rev 5, April 2017
[JIL-SECREQ]	JIL: Security requirements for post-delivery code loading, version 1.0, February 2016
[CCDB]	Common Criteria mandatory technical document – Composite product evaluation for smart cards and similar devices, Version 1.5.1, May 2018
[PP]	**Protection profiles**
[PP-IC]	Security IC Platform Protection Profile with augmentation Packages– BSI-CC-PP-0084-2014 v1.0
[PP-JCS]	Java Card System – Open Configuration Protection Profile BSI-CC-PP-0099-2017, Version 3.0.5, December 2017
[PP-CSP]	Cryptographic Service Provider Protection Profile BSI-CC-PP-0104-2019, Version 0.9.8, February 2019
[NIST]	**NIST references**
[FIPS197]	Federal Information Processing Standards Publication 197 ADVANCED ENCRYPTION STANDARD (AES), 2001 November 26
[FIPS 46]	DATA ENCRYPTION STANDARD (DES), 1999
[FIPS PUB 186-4]	NIST, Digital Signature Standard (DSS), , 2013
[FIPS PUB 180-4]	NIST, Secure Hash Standard (SHS), 2012
[NIST-SP800-38A]	NIST, SP800-38A Recommendation for Block Cipher Modes of Operation: Methods and Techniques
[NIST-SP800-38B]	NIST, SP800-38B Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, , May 2005
[NIST-SP800-38C]	NIST, Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality, , May 2004
[NIST-SP800-38D]	NIST, SP800-38D Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, , November 2007
[NIST-SP800-38F]	NIST , SP800-38F Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping, , 2012
[NIST-SP800-56C]	NIST, Recommendation for Key Derivation through Extraction-then-Expansion, Special Publication SP800-56C, , November 2011
[NIST FIPS 186-3]	NIST, Digital Signature Standard (DSS), , 2009
[ISO]	**ISO references**

[ISO/IEC 10116]	ISO/IEC 10116 Information Technology - Security techniques, Modes of operation for an n-bit block cipher, , 2017
[ISO/IEC 14888-2]	ISO/IEC 14888-2 Information technology – Security techniques, Digital signatures with appendix – Part 2: Integer factorization based mechanisms, , 2008
[ISO/IEC 18033-3]	ISO/IEC 18033-3 Information technology - Security techniques, Encryption algorithms - Part 3: Block ciphers, , 2010
[ISO/IEC 9797-1]	ISO/IEC 9797-1 Information Technology - Security techniques, Message Authentication Codes (MACs), Part 1: Mechanisms using a block cipher, , 2011
[ISO/IEC 9797-2]	ISO/IEC 9797-2 Information Technology - Security techniques, Message Authentication Codes (MACs), Part 2: Mechanisms using a dedicated hash-function, , 2011
[GP]	**Global Platform references**
[GP23]	Global Platform Card Specification Version 2.3.1 March 2018
[GP23 Amend A]	GlobalPlatform Technology Confidential Card Content Management Card Specification v2.3 – Amendment A Version 1.2 July 2019
[GP23 Amend B]	Global Platform Remote Application Management over HTTP, Amendment B Version 1.1.3 May 2015
[GP23 Amend C]	GlobalPlatform Technology – Contactless services – Card Specification v2.3 – Amendment C Version 1.3 July 2019
[GP23 Amend D]	GlobalPlatform Technology Secure Channel Protocol '03' Card Specification v2.3 – Amendment D Version 1.1.2 March 2019
[GP23 Amend E]	Card Technology Security Upgrade for Card Content Management Card Specification v2.3 – Amendment E v1.1 November 2016
[GP23 Amend F]	GlobalPlatform Technology Secure Channel Protocol '11' Card Specification v2.3 – Amendment F Version 1.2.1 – March 2019
[GP23 Amend H]	GlobalPlatform Card Executable Load File Upgrade Card Specification v2.3 – Amendment H Version 1.0 – Feb 2017
[GP23 Privacy]	Global Platform, Privacy Framework Version 1.0 Feb 2017
[GP23 SE Config]	Global Platform, Secure Element Configuration Version 1.0 October 2012
[Others]	**Others specification references**
[ICAO Doc9303]	ICAO: Machine Readable Travel Documents, ICAO Doc9303, Part 11: Security Mechanisms for MRTDSs, seventh edition, 2015
[PKCS#1]	PKCS #1 v2.2: RSA Cryptographic Standard, https://www.emc.com/emc-plus/rsa- labs/pkcs/files/h11300-wp-pkcs-1v2-2-rsa-cryptography-standard.pdf, , 27.10.2012
[RFC2104]	RFC2104, HMAC: Keyed-Hashing for Message Authentication
[RFC5639]	RFC5639, Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, http://www.ietf.org/rfc/rfc5639.txt, 2010
[RFC5903]	RFC5903, Elliptic Curve Groups modulo a Prime (ECP Groups) for IKE and IKEv2
[RFC6954]	RFC6954, Using the Elliptic Curve Cryptography (ECC) Brainpool Curves for the Internet. Key Exchange Protocol Version 2 (IKEv2),
[TPMLib,Part 1]	Trusted Platform Module Library, Part 1: Architecture, Family "2.0", Level 00, Revision 01.38, September 29, 2016
[TR-03110]	BSI, Technical Guideline TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 2 - Protocols for electronic IDentification, Authentication and trust Services (eIDAS), Version 2.21, 2016
[TR-03111]	BSI, Elliptic Curve Cryptography, BSI Technical Guideline TR-03111, Version 2.1, 1.6.2018

[AIS 20/31]	A proposal for: Functionality classes for random number generators, version 2.0, 18.09.2011, Bundesamt für Sicherheit in der Informationstechnik
[PKI]	MRTD Technical Report, PKI for Machine Readable Travel Documents Offering ICC Read-Only Access, International Civil Aviation Organization, Version 1.1, October 01 2004
[ANSI-X9.63]	ANSI-X9.63, Key Agreement and Key Transport Using Elliptic Curve Cryptography, , 2011
[FIDO-ECDAA]	FIDO Alliance, Alliance Proposed Standard FIDO ECDAA Algorithm, https://fidoalliance.org/specs/fido-u2f-v1.2-ps-20170411/fido-ecdaa-algorithm-v1.2-ps-20170411.html, 11 April 2017

[JCS]	**Javacard references**
[JCRE305]	Java Card 3.0.5 Runtime Environment (JCRE) Specification, Classic Edition – May 2015 - Published by Oracle.
[JCVM305]	Java Card 3.0.5 Virtual Machine (JCVM) Specification, Classic Edition – May 2015 - Published by Oracle
[JCAPI305]	Java Card 3.0.5 Application Programming Interface, Classic Edition - May 2015 - Published by Oracle.

[ST]	**SECURITY TARGET**
[ST-CSP]	CSP security target v1.3p – public version
[ST-PLTF]	Upteq NFC422 V1.0 security target v1.2p – public version
[ST-IC]	S3NSEN4 rev1 security target

1.1.2 Internal References [IR]

[CSP-SPEC]	CSP specification: 2019_01_24_csp_api_def v1.4
[AGD]	D1516184 v1.2 - Operational guidance on CC platforms – Operational guidance on CC platforms With or Without Controlling Authority And Optional Verification Authority - Operational Guidance
[AGD-VA]	D1516183 v1.0 - Operational guidance on CC platforms for VA - Operational guidance on CC platforms for Verification Authority - Operational Guidance
[AGD-CSP]	CSP_API_Programming_Guidelines_0.5
[AGD-PRE]	D1516186 v1.0 - Preparative guidance on CC platforms - Preparation Guidance
[ALC-DVS]	R1R28368_ALC_DVS_v1.0 - ALC DVS document
[ALC-DEL]	R1R28368_ALC_DEL_v1.0 - ALC DEL document
[Applet guidance]	D1516182 v1.1 - Guidance for secure application development on CC platforms

1.2 ACRONYMS AND GLOSSARY

AES	Advanced Encryption Standard
APDU	Application Protocol Data Unit
API	Application Programming Interface
CAD	Card Acceptance Device
CC	Common Criteria
CPU	Central Processing Unit
CSP	Cryptographic Service Provider
DES	Data Encryption Standard
EAL	Evaluation Assurance Level
ECC	Elliptic Curve Cryptography
EEPROM	Electrically-Erasable Programmable Read-Only Memory
ES	Embedded Software
GP	Global Platform
IC	Integrated Circuit
IT	Information Technology
JCRE	JavaCard Runtime Environment
JCS	JavaCard System
JCVM	JavaCard Virtual Machine
NVM	Non-Volatile Memory
OP	Open Platform
PIN	Personal Identification Number
PP	Protection Profile
RMI	Remote Method Invocation
RNG	Random Number Generator
ROM	Read-Only Memory
RSA	Rivest Shamir Adleman
SAR	Security Assurance Requirement
SC	Smart Card
SCP	Secure Channel Protocol
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
ST	Security Target
TOE	Target Of Evaluation
TSF	TOE Security Functionality

2 SECURITY TARGET INTRODUCTION

2.1 SECURITY TARGET IDENTIFICATION

Title :	Security Target for CSP on Upteq NFC422 v1.0 JCS platform
Version :	1.3p
ST Reference :	R1R28368_CSP_ST
Author :	THALES
IT Security Evaluation Facility :	BRIGHTSIGHT
IT Security Certification scheme :	NSCIB

2.2 TOE IDENTIFICATION

Product Name :		CSP v1.0
Security Controllers :		S3NSEN4 Rev1
TOE Name :		CSP v1.0 on Upteq NFC422 v1.0 JCS
TOE Version :	CSPApi plugin	CE020100
	de.bsi.csp	CE020002
TOE documentation :		Guidance [AGD]
Composition elements:	Composite TOE identifier:	Refer to [ST-PLTF]
	Composite TOE Version:	Refer to [ST-PLTF]

The TOE identification is provided using a dedicated command GET STATUS.

- CSPApi plugin version:
  - The response of the GET STATUS is: 4F0CA000000018435350415049 02 [8 bytes MAC]
  - The part identifying the TOE version is CE020100 referring to CSPApi plugin version: [major version][minor version]
- de.bsi.csp package version:
  - The response of the GET STATUS is: 4F08E804007F00070308 [8 bytes MAC]
  - The part identifying the TOE version is CE020002 referring to de.bsi.csp package version [major version][minor version]

2.3 SECURITY TARGET DOCUMENT OVERVIEW

The current Security Target document describes the TOE and its environment and the scope of the evaluation refining security objectives for TOE and its environment and TOE security features under evaluation.

The main objectives of this ST are:

- To introduce TOE and the relevant environment,
- To define the scope of the TOE and its security features,
- To describe the security environment of the TOE, including the assets to be protected and the threats to be countered by the TOE and its environment during the product development, production and usage.
- To describe the security objectives of the TOE and its environment supporting in terms of integrity and confidentiality of application data and programs and of protection of the TOE.
- To specify the security requirements which includes the TOE security functional requirements, the TOE assurance requirements and TOE security functions.

2.4 TOE OVERVIEW

The Target of Evaluation (TOE) is the cryptographic service provider (CSP) package and the underlying java Card platform, Upteq NFC422 v1.0 which supports its functionality. The TOE provides cryptographic services for the protection of the confidentiality and the integrity of user data and for entity authentication addressing the consumer electronics mobile market.

2.4.1 Product Architecture

CSP is implemented as CSP full. It is part of product design.
The product's design is modular. Some functionalities are mandatory features, also name "core features" and some others are considered as "plug-ins functionalities" and could be activated/deactivated/removed from the product configuration.

The high-level architecture of the CSP on UpTeq NFC422 v1.0 can be represented as follows:

Figure 1: CSP on Upteq NFC422 v1.0 architecture

2.4.2 TOE description

The certification of this TOE is a composite certification. This means that for the certification of this TOE some other certifications of components which are part of this TOE are re-used.

TOE components	Description	Target	Type	Developer	Certification ID
CSP v1.0	Javacard package	Provide cryptographic services	Software	Thales	This

TOE components	Description	Target	Type	Developer	Certification ID
Upteq NFC422 v1.0	Javacard 3.0.5[JCS]	Provide platform OS for secure execution environment, and secure services for the application running on the top	Software	Thales	Re-used of NSCIB-CC-0089864
	GP 2.3 Amdt A, C, D, E, F, H and Privacy Framework [GP]				
	OS update				
	Cryptographic libraries				
S3NSEN4 rev1	Integrated Circuit	Provide secure IC features	Hardware	Samsung Electronics Co., Ltd	Re-used of ANSSI-2019/29
Guidance	[AGD] [AGD-PRE] [AGD-VA] [AGD-CSP]		Document	Thales	This

Table 1: TOE description

2.4.2.1 CSP v1.0 description

CSP V1.0 is a cryptographic service provider package that provide cryptographic services for the protection of the confidentiality and the integrity of user data, and for entity authentication.

It is compliant [CSP-SPEC] and provides the following services:

- Authentication of users,
- Authentication and attestation of the platform to entities,
- Data authentication and non-repudiation including time stamps,
- Encryption and decryption of user data,
- Trusted channel including mutual authentication of the communicating entities, encryption and message authentication proof for the sent data, decryption and message authentication verification for received data,
- Management of cryptographic keys with security attributes including key generation, key derivation and key agreement, internal storage of keys, import and export of keys with protection of their confidentiality and integrity,
- Generation of random bits which may be used for security services outside the platform.
- Management of certificates including import
- Management of import and export of user data and access control
- Security management including management of security functions behavior, of Authentication reference data, of security attributes of cryptographic keys, maintaining roles, restricting the ability to manage security functions such as password authentication and trusted channel to the Administrator
- Protection management including management of the integrity or confidentiality of data and TSF data that required integrity or confidentiality, management of the residual information protection, management of failures, management of physical attack, management of self-tests

It is compliant with:

- Oracle's Java Card 3.0.5 [JCS], which consists of the Java Card 3.0.5 Virtual Machine, Java Card 3.0.5 Runtime Environment and the Java Card 3.0.5 Application Programming Interface. Java Card RMI is not implemented in the TOE.

2.4.2.2 Upteq NFC422 v1.0 platform description

The Upteq NFC422 v1.0 is a secured open platform. The description is given in [ST-PLTF].

The Upteq NFC422 v1.0 has been certified in a previous certification and the results are re-used for this certification.
The exact reference to the previous certification is given in the following table above.

2.4.2.3 S3NSEN4 rev1 IC description

The Micro Controller is a secure smart card controller from Samsung based on ARM architecture. The Micro Controller contains a co-processor for symmetric cipher, supporting AES and DES operations, and a co-processor for asymmetric algorithms. It contains volatile (RAM) memory and non-volatile Flash memory. The description is given in [ST-IC].
The Micro Controller has been certified in a previous certification and the results are re-used for this certification.
The exact reference to the previous certification is given in the Table 1.

2.4.3 TOE boundaries

The TOE boundaries encompass:

- **The CSP V1.0 package made of the following parts:**
  The CSP V1.0 package software based on [CSP-SPEC]
- **The Upteq NFC422 v1.0 Javacard Platform**
  The platform is based on [JCS], [GP], OS Update application, which supports the execution of the CSP v1.0 package and provides cryptographic services
- **The Samsung S3NSEN4 rev1 Integrated Circuit**
- **The guidance documentation [AGD]**

The following figure illustrates the evaluation boundaries for the TOE. In this figure, the TSF components have been put in red color. The other components (in blue color) do not participate to the TOE security. The generic applets (STD Java App, Sensitive Java App and CSP compatible) are outside of the TOE.

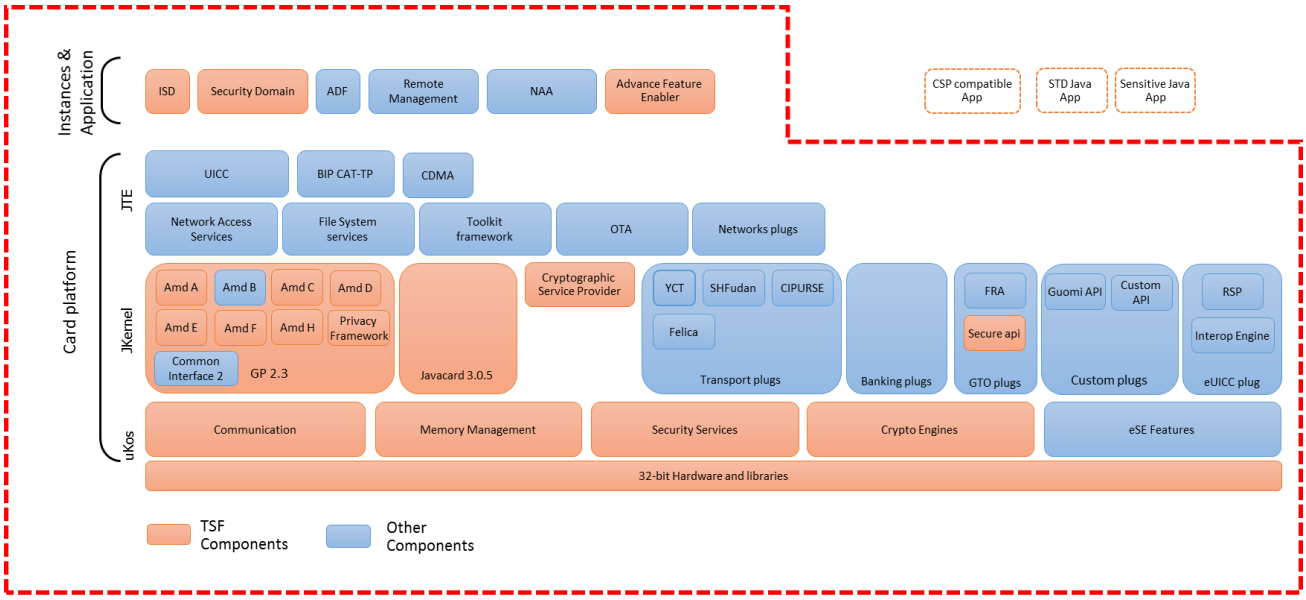


Figure 2: TOE boundaries

2.4.4 Life-cycle

2.4.4.1 Product Life-cycle

The product life cycle is composed of the 7 phases described in the following table. The table also mentions the actor(s) involved in each phase.

Notes related to applications:
CSP package loading into Flash memory can be done in phase 5. Package loading in phase 7 is also allowed. This means post-issuance loading of package can be done for a certified JCS TOE.

Phase n°	Phase designation	Phase description	Actor
1	Embedded Software Development	- Development of Java Card Platform and applications - Generation of flash image, mapping description - Script generation for initialization and pre-personalization - Management of the TOE and pre-personalization scripts delivery process from Thales R&D to Thales PE team. Then, Thales PE provides production scripts templates to CPC team.	Embedded Software Developer (Thales)
2	IC development	Development of IC and associated tools	IC Developer (Samsung LSI)
3	IC Manufacturing	Manufacturing of virgin chip integrated circuits embedding the Samsung flash Loader and protected by a dedicated transport key. JCS storage may be done at this stage.	IC manufacturer (Samsung LSI)
4	IC packaging	IC packaging & testing	Module creation (Samsung LSI)
5	Pre-personalization	Product loading, based on script generated	Composite Product manufacturer (Samsung LSI) **TOE DELIVERY**
6	Personalization	Personalization and final tests	Personalizer
7	End-usage	The Consumer (Original Equipment Manufacturer) of the product is responsible for smartcard product delivery to the end-user	Mobile phone Holder

Figure 3: Life cycle description

The evaluation process is limited to phases 1 to 5. The product delivery can be done at the end of phase5 or phase7.

For the present evaluation (cf Figure 3), the IC is manufactured at Samsung site. It is then shipped to another Samsung site where it is initialized and pre-personalized and then shipped to the Personalizer. During the shipment from Thales to Samsung, the product is protected by a diversified key.

2.4.4.2 TOE Life-cycle

The TOE life cycle distinguishes stages for:

1. Development

2. Production: Storage, pre-personalization and testing
3. Preparation: Personalization and testing
4. Operational Use: Final usage

Development and production of the TOE together constitute the development phase of the TOE. The development phase is subject of CC evaluation according to the assurance life cycle (ALC) class.

The TOE storage is not necessarily a single step in the life cycle since it can be stored in parts. The TOE delivery occurs before storage and may take place more than once if the TOE is delivered in parts.

These four stages map to the product life cycle phases as shown in Figure 4.

The different guides accompanying the TOE and parts of the TOE are the ones specified in [AGD] section. They are delivered in form of electronic documents by Thales Technical representative sent by email and ciphered using PGP key.

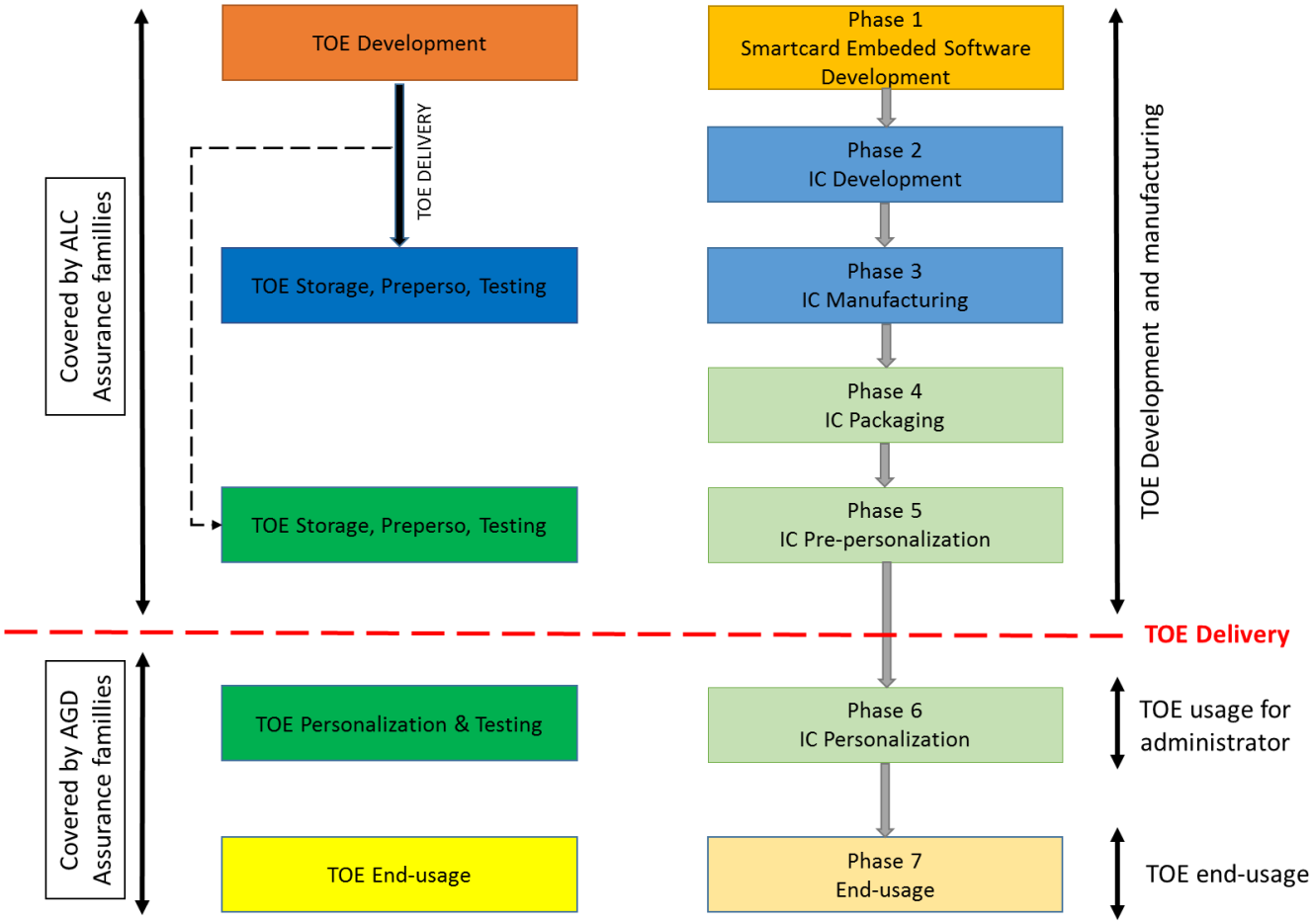


Figure 4: TOE Life Cycle within Product Life Cycle

The CSP and JCS Development is performed during Phase 1. This includes CSP, JCS conception, design, implementation, testing and documentation. The development shall occur in a controlled environment that avoids disclosure of source code, data and any critical documentation and that guarantees the integrity of these elements. The present evaluation includes the CSP and JCS development environment.

In Phase 3, the IC Manufacturer may store, initialize the TOE and potentially conduct tests on behalf of the TOE developer. The IC Manufacturing environment shall protect the integrity and confidentiality of the TOE and of any related material, for instance test suites. The present evaluation includes the whole IC Manufacturing environment, in particular those locations where the JCS is accessible for installation

or testing. As the Security IC has already been certified against [PP-IC] there is no need to perform the evaluation again.

In Phase 5, the SC Pre-Personalizer may store, load the CSP package and pre-personalize the TOE and potentially conduct tests on behalf of the TOE developer. The SC Pre-Personalization environment shall protect the integrity and confidentiality of the TOE and of any related material, for instance test suites.

(Part of) TOE storage in Phase 5 implies a TOE delivery after Phase 5. Hence, the present evaluation includes the SC Pre-Personalization environment. The TOE delivery point is placed at the end of Phase 5, since the entire TOE is then built and embedded in the Security IC.

The TOE is personalized in Phase 6, if necessary. The SC Personalization environment is not included in the present evaluation. Appropriate security recommendations are provided to the SC Personalizer through the [AGD] documentation.

The TOE final usage environment is that of the product where the TOE is embedded in. It covers a wide spectrum of situations that cannot be covered by evaluations. The TOE and the product shall provide the full set of security functionalities to avoid abuse of the product by untrusted entities.

2.4.5 TOE intended usage

The TOE is intended to be used with different applications, mainly related to digital ID services, which will use TOE security services. The TOE security services are logically separated and provided through well-defined external interfaces [CSP-SPEC].

2.4.6 Non-TOE hardware/software/firmware available to the TOE

The TOE does not need non-TOE hardware, firmware or software to run.

3 CONFORMANCE CLAIMS

3.1 CC CONFORMANCE CLAIM

Common criteria Version:
This ST conforms to CC Version 3.1 revision 5 [CC-1] [CC-2] [CC-3].

Conformance to CC part 2 and 3:
- Conformance of this ST with respect to CC part 2 [CC-2] extended.
- CC part 3 conformant.

3.2 PP CLAIM

This security target claims strict conformance to the Protection Profile “Cryptographic Service Provider”, ([PP-CSP]).

3.3 PACKAGE CLAIM

This ST is conforming to assurance package EAL4 augmented with ALC_DVS.2 and AVA_VAN.5 defined in CC part 3 [CC-3].

3.4 CONFORMANCE STATEMENT

This ST strictly conforms to [PP-CSP] and TOE type is the same as the [PP-CSP] ones.

The certification of this TOE is a composite certification. Therefore the CSP security target is a composite security target, including the **Upteq NFC422 v1.0** security target CC certified:

- Certification done under the NSCIB scheme
- Certification report NSCIB-CC-0089864
- Security Target [ST-PLTF] conformant to Javacard Protection Profile, Open configuration [PP-JCS]
- Common criteria version: 3.0.5
- Assurance level: EAL4+ (ALC_DVS.2 and AVA_VAN.5 augmentations)

However the security problem definition, the objectives, and the SFR of the **Upteq NFC422 v1.0** are not described in this document.
But this evaluation includes additional composition tasks defined in the CC supporting document “Composite product evaluation for smart cards and similar devices” [CCDB].

Note: the **Upteq NFC422 v1.0** platform was also evaluated in composition with the S3NSEN4 Rev1 integrated circuit, and relied upon on the chip certificate and evaluation results:

- Certification done under the ANSSI scheme
- Certification report ANSSI-CC-2019/29
- Security Target [S3NSEN4_N3_v1.0] strictly conformant to IC Protection Profile [PP-IC]
- Common criteria version: 3.1 rev 5
- Assurance level: EAL6+ (ASE_TSS.2 augmentations)

4 SECURITY PROBLEM DEFINITION

4.1 INTRODUCTION

4.1.1 Assets

The assets of the TOE are
- user data which integrity and confidentiality shall be protected,
- cryptographic services and keys which shall be protected against unauthorized use or misuse,
- Update Code Packages (UCP).

The cryptographic keys are TSF data because they are used for cryptographic operations protecting user data and the enforcement of the SFR relies on these data for the operation of the TOE.

4.1.2 User and subjects

The TOE knows external entities (users) as
- human user communicating with the TOE for security management of the TOE,
- application component using the cryptographic and other security services of the TOE and supporting the communication with remote entities (e. g. by providing certificates),
- remote entity exchanging user data and TSF data with the TOE over insecure media.

The TOE communicates with
- human user through a secure channel,
- application component through a secure channel,
- remote entities over a trusted channel using cryptographic mechanisms including mutual authentication.

The subjects as active entities in the TOE perform operations on objects. They obtain their associated security attributes from the authenticated users on behalf they are acting, or by default.

4.1.3 Objects

The TSF operates user data objects and TSF data objects (i. e. passive entities, that contain or receive information, and upon which subjects perform operations).
User data objects are imported, used in cryptographic operation, temporarily stored, exported and destroyed after use. The Update Code Packages are user data objects imported and stored in the TOE until use for creation of an updated CSP.
TSF data objects are created, temporarily or permanently stored, imported, exported and destroyed as objects of the security management. They may contain e. g. cryptographic keys with their security attributes, certificates, Authentication Data Records with authentication reference data of a user. Cryptographic keys are objects of the key management.

4.1.4 Security attributes

The security attributes of user known to the TOE are stored in Authentication Data Records containing
- User Identity (User-ID),
- Authentication reference data,
- Role with detailed access rights.

Passwords as Authentication Reference Data have the security attributes
- status: values initial password, operational password,
- number of unsuccessful authentication attempts.

Certificates contain security attributes of users including User identity, a public key and security attributes of the key. If certificates are used as authentication reference data for cryptographic entity authentication mechanisms they may contain the Role of the entity.

The user uses authentication verification data to prove its identity to the TOE. The TSF uses Authentication reference data to verify the claimed identity of a user. The TSF supports

- human user authentication by knowledge where the authentication verification data is a password and the authentication reference data is a password or an image of the password e. g. a salted hash value or a derived cryptographic key,
- human user authentication by possession of a token or as user of a terminal implementing user authentication by cryptographic entity authentication mechanism,
- cryptographic entity authentication mechanisms where the authentication verification data is a secret or private key and the authentication reference data is a secret or public key.

A human user may authenticate themselves to the TOE and the TOE authenticates to an external entity in charge of the authenticated authorized user.

The TOE knows at least the following roles taken by a user or a subject acting on behalf of a user:

- Unidentified User: this role is associated with any user not (successfully) identified by the TOE. This role is assumed after start-up of the TOE. The TSF associated actions allowed for the Unidentified User are defined in SFR FIA_UID.1.
- Unauthenticated User: this role is associated with an identified user but not (successfully) authenticated user. The TSF associated actions allowed for the Unauthenticated User are defined in SFR FIA_UAU.1.
- Administrator: successful authenticated user allowed to access the TOE in order to perform management functions. It is taken by a human user or a subject acting on behalf of a human user after successful authentication as Administrator.

  The Administrator role may be split in more detailed roles:
  - Crypto-Officer: role that is allowed to access the TOE in order to perform management of a cryptographic TSF.
  - User Administrator: role that is allowed to access the TOE in order to perform user management.
  - Update Agent: authorized user for import and verification of Update Code Package.

  The SFR uses the general term Administrator or a selection between Administrator role and these detailed roles in case they are supported by the TOE and separation of duties is appropriate.

- Key Owner: successful authenticated user allowed to perform cryptographic operation with their own keys. This role may be claimed by human user or an entity.
- Application Component: subjects in this role are allowed to use assigned security services of the TOE without authenticated human user session (e. g. export and import of wrapped keys). This role may be assigned to an entity communicating through a physically separated secure channel or through a trusted channel (which requires assured identification of its end points).

The TOE is delivered with initial Authentication Data Records for Unidentified User, Unauthenticated User and administrator role(s). The Authentication Data Records for Unidentified User and Unauthenticated User have no Authentication Reference Data. The roles are not exclusive, i. e. a user or subject may be in more then one role, e. g. a human user may claim the Crypto-Officer and Key Owner role at the same time. The SFR may define limitation on roles one user may associated with.

Cryptographic keys have at least the security attributes

- Key identity that uniquely identifies the key,
- Key entity, i. e. the identity of the entity this key is assigned to,
- Key type, i. e. as secret key, private key, public key,
- Key usage type, identifying the cryptographic mechanism or service the key can be used for, e. g. a private signature key may be used by a digital signature-creation mechanism (cf. FCS_COP.1/CDS-ECDSA or FCS_COP.1/CDS-RSA), and depending on the certificate for data authentication with identity of guarantor (cf. FDP_DAU.2/Sig) by key usage type “DigSign” or attestation (cf. FDP_DAU.2/Att) by key usage type “Attestation”.
- Key access control attributes, i. e. list of combinations of the identity of the user, the role for which the user is authenticated and the allowed key management function or cryptographic operation, including

- Import of the key is allowed or forbidden,
- Export of the key is allowed or forbidden,

and may have the security attribute
- Key validity time period, i. e. the time period for operational use of the key; the key must not be used before or after this time slot,
- Key usage counter, i. e. the number of operations performed with this key e. g. number of signature created with a private signature key.

The UCP have at least the security attributes
- Issuer of the UCP,
- Version Number of the UCP.

4.2 THREATS

T.DataCompr Compromise of communication data
An unauthorized entity gets knowledge of the information contained in data stored on TSF controlled media or transferred between the TOE and authenticated external entities.

T.DataMani Unauthorized generation or manipulation of communication data
An unauthorized entity generates or manipulates user data stored on TSF controlled media or transferred between the TOE and authenticated external entities and accepted as valid data by the recipient.

T.Masqu Masquerade authorized user
A threat agent might masquerade as an authorized entity in order to gain unauthorized access to user data, TSF data, or TOE resources.

T.ServAcc Unauthorized access to TOE security services
A attacker gets as TOE user unauthorized access to security services of the TOE.

T.PhysAttack Physical attacks
An attacker gets physical access to the TOE and may (1) disclose or manipulate user data under TSF control and TSF data, and (2) affect TSF by (a) physical probing and manipulation, (b) applying environmental stress or (c) exploiting information leakage from the TOE.

T.FaUpD Faulty Update Code Package
An unauthorized entity provides an unauthorized faulty Update Code Package enabling attacks against integrity of TSF implementation, confidentiality and integrity of user data and TSF data after installation of the faulty Update Code Package.

4.3 ORGANISATIONAL SECURITY POLICIES

OSP.SecCryM Secure cryptographic mechanisms
The TOE uses only secure cryptographic mechanisms as confirmed by the certification body for the specified TSF, the assurance security requirements and the operational environment.

OSP.SecService Security services of the TOE
The TOE provides security services to the authorized users for encryption and decryption of user data, authentication prove and verification of user data, entity authentication to external entities including attestation, trusted channel and random bit generation.

OSP.KeyMan Key Management
The key management ensures the integrity of all cryptographic keys and the confidentiality of all secret or private keys over the whole life cycle which comprises their generation, storage, distribution, application, archiving and deletion. The cryptographic keys and cryptographic key components shall be generated, operated and managed by secure cryptographic mechanisms and assigned to the secure cryptographic mechanisms they are intended to be used with and to the entities authorized for their use.

OSP.TC Trust center
The trust centers provide secure certificates for trustworthy certificate holder with correct security attributes. The TOE uses certificates for identification and authentication of users, access control and secure use of security services of the TOE including key management and attestation.

OSP.Update Authorized Update Code Packages
The Update Code Packages are delivered in encrypted form and signed by the authorized issuer. The TOE verifies the authenticity of the received Update Code Package using the CSP before storing in the TOE. The TOE restricts the storage of authentic Update Code Package to an authorized user.

4.4 ASSUMPTIONS

The assumptions in this Security Target are those named and described in [PP-CSP]. The assumptions stated in [PP-JCS] and relevant for the TOE are listed here. Others can be found in [ST-PLTF].

A.SecComm Secure communication
Remote entities support trusted channel using cryptographic mechanisms. The operational environment shall protect the local communication channels by trusted channels using cryptographic mechanisms or by secure channel using non-cryptographic security measures.

5 SECURITY OBJECTIVES

5.1 SECURITY OBJECTIVES FOR THE TOE

The security objectives in this Security Target are those named and described in [PP-CSP]. The security objectives stated in [PP-JCS] and relevant for the TOE are listed here. Others can be found in [ST-PLTF].

O.AuthentTOE Authentication of the TOE to external entities
The TOE authenticates themselves in charge of authorized users to external entities by means of secure cryptographic entity authentication and attestation.

O.Enc Confidentiality of user data by means of encryption and decryption
The TOE provides secure encryption and decryption as security service for the users to protect the confidentiality of user data imported, exported or stored on media in the scope of TSF control.

O.DataAuth Data authentication by cryptographic mechanisms
The TOE provides secure symmetric and asymmetric data authentication mechanisms as security services for the users to protect the integrity and authenticity of user data.

O.RBGS Random bit generation service
The TOE provide cryptographically secure random bit generation service for the users.

O.TChann Trusted channel
The TSF provides trusted channel using secure cryptographic mechanisms for the communication between the TSF and external entities. The TOE provides authentication of all communication end points, ensures the confidentiality and integrity of the communication data exchanged through the trusted channel.

Note the TSF can establish the trusted channel by means of secure cryptographic mechanisms only if the other endpoint supports these secure cryptographic mechanisms as well. If trusted channel cannot be established by means of secure cryptographic mechanisms due to missing security functionality of the user then the operational environment shall provide a secure channel protecting the communication by non-cryptographic security measures, cf. A.SecComm and OE.SecComm.

O.I&A Identification and authentication of users
The TOE shall uniquely identify users and verify the claimed identity of the user before providing access to any controlled resources with the exception of self-test, identification of the TOE and authentication of the TOE. The TOE shall authenticate IT entities using secure cryptographic mechanisms.

O.AccCtrl Access control
The TOE provides access control on security services, operations on user data, management of TSF and TSF data.

O.SecMan Security management
The TOE provides security management of users, TSF, TSF data and cryptographic keys by means of secure cryptographic mechanisms and using certificates. The TSF generates, derives, agrees, import and export cryptographic keys as security service for users and for internal use. The TSF shall destruct unprotected secret or private keys in such a way that any previous information content of the resource is made unavailable.

O.TST Self-test
The TSF performs self-tests during initial start-up, at the request of the authorised user and after power-on. The TSF enters secure state if self-test fails or attacks are detected.

O.PhysProt Physical protection
The TSF protects the confidentiality and integrity of user data, TSF data and its correct operation against physical attacks and environmental stress. In case of platform architecture the TSF protects the secure execution environment for and the communication with the application component running on the TOE.

O.SecUpCP Secure import of Update Code Package
The TSF verifies the authenticity of received encrypted Update Code Package, decrypts authentic Update Code Package and allows authorized users to store decrypted Update Code Package.

5.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

The security objectives for the environment in this Security Target are those named and described in [PP-CSP]. The security objectives stated in [PP-JCS] and relevant for the TOE are listed here. Others can be found in [ST-PLTF].

OE.CommInf Communication infrastructure
The operational environment shall provide public key infrastructure for entities in the communication networks. The trust centers generate secure certificates for trustworthy certificate holder with correct security attributes. They distribute securely their certificate signing public key for verification of digital signature of the certificates and run a directory service for dissemination of certificates and provision of revocation status information of certificates.

OE.AppComp Support of the Application component
The Application component supports the TOE for communication with users and trust centers.

OE.SecManag Security management
The operational environment shall implement appropriate security management for secure use of the TOE including user management, key management. It ensures secure key management outside the TOE and uses the trust center services to determine the validity of certificates. The cryptographic keys and cryptographic key components shall be assigned to the secure cryptographic mechanisms they are intended to be used with and to the entities authorized for their use.

OE.SecComm Protection of communication channel
Remote entities shall support trusted channels with the TOE using cryptographic mechanisms. The operational environment shall protect the local communication channels by trusted channels using cryptographic mechanisms or by secure channel using non-cryptographic security measures.

OE.SUCP Signed Update Code Packages
The secure Update Code Package is delivered in encrypted form and signed by the authorized issuer together with its security attributes.

5.3 SECURITY OBJECTIVES RATIONALE

The following table traces the security objectives for the TOE back to threats countered by that security objective and OSPs enforced by that security objective, and the security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective.

5.3.1 Security Objective rationale

	T.DataCompr	T.DataMani	T.Masqu	T.ServAcc	T.PhysAttack	T.FaUpD	OSP.SecCryM	OSP.SecService	OSP.KeyMan	OSP.TC	OSP.Update	A.SecComm
O.AccCtrl				x								
O.AuthentTOE							x	x				
O.DataAuth		x					x	x				
O.Enc	x						x	x				
O.I&A			x	x			x	x				
O.PhysProt					x							
O.RBGS							x	x				
O.SecMan			x				x		x	x		
O.SecUpCP						x					x	
O.Tchann	x	x	x	x			x	x				
O.TST					x							
OE.AppComp	x	x		x						x		
OE.CommInf	x	x		x				x	x	x		
OE.SecComm	x	x		x								x
OE.SecManag			x					x	x			
OE.SUCP						x					x	

Table 2: Security Objective rationale

The following part of the chapter demonstrate that the security objectives counter all threats and enforce all OSPs, and the security objectives for the operational environment uphold all assumptions.

The threat T.DataCompr “Compromise of communication data”: is countered by the security objectives for the TOE and the operational environment

- O.Enc requires the TOE to provide encryption and decryption as security service for the users to protect the confidentiality of user data,

- O.TChann requires the TOE to support trusted channel between TSF and the application component, and between TSF and other users, and the application component and other users with authentication of all communication end points, protected communication ensuring the confidentiality and integrity of the communication and to prevent misuse of the session of authorized users.

- OE.AppComp requires the application component to support the TOE for communication with users and trust center.

- OE.CommInf requires the operational environment to provide the communication infrastructure especially trust center services.

- OE.SecComm requires the operational environment to protect the confidentiality and integrity of communication over local communication channel by physical security measures and remote entities to support trusted channels by means of cryptographic mechanisms. If a trusted channel cannot be established due to missing security functionality of the application component or human user communication channel the operational environment shall protect the communication, cf. A.SecComm and OE.SecComm.

The threat T.DataMani “Unauthorized generation or manipulation of communication data” is countered by the security objectives for the TOE and the operational environment:

- O.DataAuth requires the TOE to provide symmetric and asymmetric data authentication mechanisms as security service for the users to protect the integrity and authenticity of user data.

- O.TChann requires the TOE to support trusted channel for authentication of all communication end points, protected communication with the application component and other users to ensure the confidentiality and integrity of the communication and to prevent misuse of the session of authorized users

- OE.AppComp requires the application component to support the TOE for communication with users and trust center.

- OE.CommInf requires the operational environment to provide trust center services and securely distribute root public keys.

- OE.SecComm requires the operational environment to protect the confidentiality and integrity of communication with the TOE. Remote entities shall support trusted channels with the TOE using cryptographic mechanisms. The operational environment shall protect the local communication channels by trusted channels using cryptographic mechanisms or by secure channel using non-cryptographic security measures.

The threat T.Masqu “Masquerade authorized user” is countered by the security objectives for the TOE and the operational environment:

- O.I&A requires the TSF to identify uniquely users and verify the claimed identity of the user before providing access to any controlled resources with the exception of self-test, identification of the TOE and authentication of the TOE.

- O.TChann requires the TSF to provide authentication of all communication end points of the trusted channel.

- O.SecMan requiring the TSF to provides security management of users, TSF, TSF data and cryptographic keys by means of secure cryptographic mechanisms and using certificates.

- OE.SecMan requiring the operational environment to implement appropriate security management for secure use of the TOE including user management.

The threat T.ServAcc “Unauthorized access to TOE security services” is countered by the security objectives for the TOE and the operational environment:

- O.I&A requires the TSF to uniquely identify users and to authenticate users before providing access to any controlled resources with the exception of self-test, identification of the TOE and authentication of the TOE. Note an unauthenticated user is allowed to request authentication of the TOE.

- O.AccCtrl requires the TSF to control access on security services, operations on user data, management of TSF and TSF data.

- O.Tchann requires mutual authentication of the external entity and the TOE and the authentication of communicated data to prevent misuse of the communication with external entities. The operational environment is required by OE.SecComm to ensure secure channels if trusted channel cannot be established.

- The operational environment OE.CommInf requires provision of a public key infrastructure for entity authentication and OE.AppComp requires the application to support communication with trust centers.

The threat T.PhysAttack“Physical attacks” is directly countered by the security objectives

- O.PhysProt requires the TSF to protects the confidentiality and integrity of user data, TSF data and its correct operation against physical attacks and environmental stress.

- O.TST requires the TSF to perform self-tests and to enter secure state if self-test fails or attacks are detected as means to ensure robustness against perturbation.

-

The threat T.FaUpD ”Faulty Update Code Package” is directly countered by the security objective O.SecUpCP verifying the authenticity of UCP under the condition that trustworthy UCP are signed as required by OE.SUCP

- O.SecUpCP “Secure import of Update Code Package” requires the TOE to verify the authenticity of received encrypted Update Code Package before decrypting and storing authentic an Update Code Package.

- OE.SUCP “Signed Update Code Packages” requires the Issuer to sign secure Update Code packages together with its security attributes.

The organizational security policy OSP.SecCryM “Secure cryptographic mechanisms” is implemented by means of secure cryptographic mechanisms required in

- O.I&A “Identification and authentication of users” and O.AuthentTOE “Authentication of the TOE to external entities” requiring secure entity authentication mechanisms of users and TOE,

- O.Enc “Confidentiality of user data by means of encryption and decryption” and O.DataAuth ”Data authentication by cryptographic mechanisms” requiring secure cryptographic mechanisms for protection of confidentiality and integrity of user data,

- O.TChann “Trusted channel” requiring secure cryptographic mechanisms for entity authentication mechanisms of users and TOE, protection of confidentiality and integrity of communication data.

- O.RBGS “Random bit generation service” requires the TOE to provide cryptographically secure random bit generation service for the users.

- O.SecMan “Security management” requiring security management of TSF data and cryptographic keys by means of secure cryptographic mechanisms and using certificates.

The organizational security policy OSP.SecService “Security services of the TOE” is directly implemented by security objectives for the TOE O.Enc “Confidentiality of user data by means of encryption and decryption”, O.DataAuth ”Data authentication by cryptographic mechanisms”, O.I&A “Identification and authentication of users”, O.AuthentTOE “Authentication of the TOE to external entities”, O.TChann “Trusted channel” and O.RBGS “Random bit generation service” requiring TSF to provide cryptographic security services for the user. The OSP.SecService is supported by OE.CommInf “Communication infrastructure” and OE.SecManag “Security management” providing the necessary measure for the secure use of these services.

The organizational security policy OSP.KeyMan “Key Management” is directly implemented by O.SecMan “Security management” and supported by trust center services according to OE.CommInf “Communication infrastructure” and OE.SecManag “Security management”.

The organizational security policy OSP.TC “Trust center” is implemented by security objectives for the TOE and the operational environment:

- O.SecMan “Security management” uses certificates for security management of users, TSF, TSF data and cryptographic keys.

- OE.CommInf “Communication infrastructure” requires trust centers to generate secure certificates for trustworthy certificate holder with correct security attributes and to distribute certificates and revocation status information.

- OE.AppComp “Support of the Application component” requires the Application component to support the TOE for communication with trust centers.

The organizational security policy OSP.Update “Authorized Update Code Packages” is implemented directly by the security objectives for the TOE O.SecUpCP and the operational environment OE.SUCP.

The assumption A.SecComm “Secure communication” assumes that the operational environment protects the confidentiality and integrity of communication data and ensures reliable identification of its end points. The security objective for the operational environment OE.SecComm requires the operational environment to protect local communication physically and the remote entities to support trusted channels using cryptographic mechanisms.

5.3.2 Compatibility between Security Objectives of [ST-CSP] and [ST-PLTF]

5.3.2.1 Compatibility between objectives for the TOE

The following table lists the relevant security objectives of the Platform NFC422 V1.0 and provides the link to the security objectives related to the composite product, showing that there is no contradiction between the two.

Platform objective label	Platform objective short description (refer to [ST-PLTF] for the full description)	Link to the composite-product
O.SID	The TOE shall uniquely identify every subject (applet, or package) before granting it access to any service.	O.I&A
O.FIREWALL	The TOE shall ensure controlled sharing of data containers owned by applets of different	O.AccCtrl

Platform objective label	Platform objective short description (refer to [ST-PLTF] for the full description)	Link to the composite-product
	packages, or the JCRE and between applets and the TSFs.	
O.GLOBAL_ARRAYS_CONFID	The TOE shall ensure that the APDU buffer that is shared by all applications is always cleaned upon applet selection. The TOE shall ensure that the global byte array used for the invocation of the install method of the selected applet is always cleaned after the return from the install method.	O.AccCtrl
O.GLOBAL_ARRAYS_INTEG	The TOE shall ensure that only the currently selected applications may have a write access to the APDU buffer and the global byte array used for the invocation of the install method of the selected applet.	O.AccCtrl
O.NATIVE	The only means that the Java Card VM shall provide for an application to execute native code is the invocation of a method of the Java Card API, or any additional API.	No contradiction with the security objectives of the composite TOE
O.OPERATE	The TOE must ensure continued correct operation of its security functions.	O.PhysProt
O.REALLOCATION	The TOE shall ensure that the re-allocation of a memory block for the runtime areas of the Java Card VM does not disclose any information that was previously stored in that block.	O.AccCtrl
O.RESOURCES	The TOE shall control the availability of resources for the applications.	No contradiction with the security objectives of the composite TOE
O.ALARM	The TOE shall provide appropriate feedback information upon detection of a potential security violation.	O.TST O.PhysProt
O.CIPHER	The TOE shall provide a means to cipher sensitive data for applications in a secure way. In particular, the TOE must support cryptographic algorithms consistent with cryptographic usage policies and standards.	O.Enc O.DataAuth O.SecMan
O.RNG	The TOE shall ensure the cryptographic quality of random number generation. For instance random numbers shall not be predictable and shall have sufficient entropy. The TOE shall ensure that no information about the produced random numbers is available to an attacker since they might be	O.RBGS

Platform objective label	Platform objective short description (refer to [ST-PLTF] for the full description)	Link to the composite-product
	used for instance to generate cryptographic keys.	
O.KEY-MNGT	The TOE shall provide a means to securely manage cryptographic keys. This concerns the correct generation, distribution, access and destruction of cryptographic keys.	O.SecMan
O.PIN-MNGT	The TOE shall provide a means to securely manage PIN objects (including the PIN try limit, PIN try counter and states). If the PIN try limit is reached, no further PIN authentication must be allowed.	No contradiction with the security objectives of the composite TOE
O.TRANSACTION	The TOE must provide a means to execute a set of operations atomically.	No contradiction with the security objectives of the composite TOE
O.OBJ-DELETION	The TOE shall ensure the object deletion shall not break references to objects.	No contradiction with the security objectives of the composite TOE
O.DELETION	The TOE shall ensure that both applet and package deletion perform as expected.	No contradiction with the security objectives of the composite TOE
O.LOAD	The TOE shall ensure that the loading of a package into the card is safe. Besides, for code loaded post-issuance, the TOE shall verify the integrity and authenticity evidences generated during the verification of the application package by the verification authority. This verification by the TOE shall occur during the loading or later during the install process.	O.SecUpCP
O.INSTALL	The TOE shall ensure that the installation of an applet performs as expected. Besides, for codes loaded post-issuance, the TOE shall verify the integrity and authenticity evidences generated during the verification of the application package by the verification authority. If not performed during the loading process, this verification by the TOE shall occur during the install process.	No contradiction with the security objectives of the composite TOE
O.SCP.IC	The SCP shall provide all IC security features against physical attacks.	O.PhysProt

Platform objective label	Platform objective short description (refer to [ST-PLTF] for the full description)	Link to the composite-product
	This security objective for of the TOE refers to the security aspect #.SCP: It is required that the IC is designed in accordance with a well-defined set of policies and Standards (likely specified in another protection profile), and will be tamper resistant to actually prevent an attacker from extracting or altering security data (like cryptographic keys) by using commonly employed techniques (physical probing and sophisticated analysis of the chip). This especially matters to the management (storage and operation) of cryptographic keys.	
O.SCP.RECOVERY	If there is a loss of power, or if the smart card is withdrawn from the CAD while an operation is in progress, the SCP must allow the TOE to eventually complete the interrupted operation successfully, or recover to a consistent and secure state. This security objective of the TOE refers to the security aspect #.SCP.1: The smart card platform must be secure with respect to the SFRs. Then after a power loss or sudden card removal prior to completion of some communication protocol, the SCP will allow the TOE on the next power up to either complete the interrupted operation or revert to a secure state	O.PhysProt
O.SCP.SUPPORT	The SCP shall support the TSFs of the TOE. This security objective of the TOE refers to the security aspects 2, 3, 4 and 5 of #.SCP: (2) It does not allow the TSFs to be bypassed or altered and does not allow access to other low-level functions than those made available by the packages of the API. That includes the protection of its private data and code (against disclosure or modification) from the Java Card System. (3) It provides secure low-level cryptographic processing to the Java Card System. (4) It supports the needs for any update to a single persistent object or class field to be atomic, and possibly a low-level transaction mechanism.	No contradiction with the security objectives of the composite TOE

Platform objective label	Platform objective short description (refer to [ST-PLTF] for the full description)	Link to the composite-product
	(5) It allows the Java Card System to store data in "persistent technology memory" or in volatile memory, depending on its needs (for instance, transient objects must not be stored in non-volatile memory). The memory model is structured and allows for low-level control accesses (segmentation fault detection).	
O.CARD-MANAGEMENT	The card manager shall control the access to card management functions such as the installation, update, extradition or deletion of applets and GP registry updates. It shall also implement the card issuer's policy on the card.	No contradiction with the security objectives of the composite TOE
O.APPLI-AUTH	The card manager shall enforce the application security policies established by the card issuer by requiring application authentication during application loading on the card. This security objective is a refinement of the Security Objective O.LOAD from [PP-JCS-Open].	O.SecUpCP
O.DOMAIN-RIGHTS	The Card issuer shall not get access or change personalized AP Security Domain keys which belong to the AP. Modification of a Security Domain keyset is restricted to the AP who owns the security domain.	O.AccCtrl
O.COMM_AUTH	The TOE shall authenticate the origin of the card management requests that the card receives, and authenticate itself to the remote actor	No contradiction with the security objectives of the composite TOE
O.COMM_INTEGRITY	The TOE shall verify the integrity of the card management requests that the card receives	No contradiction with the security objectives of the composite TOE
O.COMM_CONFIDENTIALITY	The TOE shall be able to process card management requests containing encrypted data	No contradiction with the security objectives of the composite TOE
O.CONFID-OS-UPDATE.LOAD	The TOE shall be able to decrypt the additional code received for loading and installation. The following Security Objectives have been added to comply to JIL "Security requirements for post-delivery code loading" [JIL-SECREQ]	O.SecUpCP

Platform objective label	Platform objective short description (refer to [ST-PLTF] for the full description)	Link to the composite-product
O.Secure_Load_ACode	The TOE shall check an evidence of authenticity and integrity of the additional code to be loaded. The TOE enforces that only an allowed version of the additional code can be loaded. The TOE shall forbid the loading of an additional code not intended to be assembled with the TOE. During the loading of the additional code, the TOE shall remain secure	O.SecUpCP
O.Secure_AC_Activation	Activation of the additional code and update of the Identification Data shall be performed at the same time in an atomic way. All the operations needed for the code to be able to operate as in the Updated TOE shall be completed before activation	no direct link with composite toe ojectives nevertheless it is used for secure update code package installation
O.TOE_Identification	The TOE provides means to store Identification Data in its non-volatile memory and guarantees the integrity of these data. After atomic activation of the additional code, the Identification Data of the Updated TOE allows identifications of both the Initial TOE and additional code. The user must be able to uniquely identify Initial TOE and additional code(s) which are embedded in the Updated TOE	no direct link with composite toe ojectives nevertheless it is used for secure update code package installation
O.REMOTE_SERVICE_ACTIVATION	The TOE shall perform remote optional platform service activation only when service activation is authorized and only by an authorized actor. Limited to [GemActivate Administrator (usually Thales)] under control of [OEM].	No contradiction with the security objectives of the composite TOE
O.REMOTE_SERVICE_AUDIT	The TOE shall perform remote service audit only when optional platform service audit is authorized and only by an authorized actor. Limited to [OEM or GemActivate Administrator (usually Thales)].	No contradiction with the security objectives of the composite TOE
O.Secure_API	The TOE shall provide a dedicated API - named Secure API - to applications, so as to optimize control on their sensitive operations. The Secure API shall provide security services such as secure array management, loss of data integrity detection, inconsistent	O.PhysProt

Platform objective label	Platform objective short description (refer to [ST-PLTF] for the full description)	Link to the composite-product
	execution flow detection, reaction against tearing or fault induction.	
O.JCAPI-Services	The TOE shall ensure that data manipulated during SHA services as defined in [JCAPI301] cannot be observed.	O.PhysProt
OT.AC_Pers_EAC2	The TOE must ensure that the TOE and Application data requiring PACE usage* and associated TSF data can be written by authorized Personalisation Agents only in personalisation phase. The TOE and Application data requiring PACE usage (e.g. logical travel document data in EF.DG1 to EF.DG16) and associated TSF data may be written only during and cannot be changed after personalisation phase.	No contradiction with the security objectives of the composite TOE
OT.Data_Integrity	The TOE must ensure integrity of the User Data and the TSF-data stored on it by protecting these data against unauthorised modification (physical manipulation and unauthorised modifying).The TOE must ensure integrity of the User Data and the TSF-data during their exchange between the TOE and the terminal connected (and represented by PACE authenticated BIS-PACE) after the PACE Authentication.	O.PhysProt O.DataAuth O.TChann
OT.Data_Authenticity	The TOE must ensure authenticity of the User Data and the TSF-data stored on it by enabling verification of their authenticity at the terminal-side[1].The TOE must ensure authenticity of the User Data and the TSF-data during their exchange between the TOE and the terminal connected (and represented by PACE authenticated BIS-PACE) after the PACE Authentication. It shall happen by enabling such a verification at the terminal-side (at receiving by the terminal) and by an active verification by the TOE itself (at receiving by the TOE).	O.DataAuth O.TChann
OT.Data_Confidentiality	The TOE must ensure confidentiality of the User Data and the TSF data by granting read access only to the PACE authenticated BIS-PACE connected. The TOE must ensure confidentiality of the User Data and the TSF-data during their exchange between the TOE and the terminal connected (and represented by PACE authenticated BIS-PACE) after the PACE Authentication.	O.Enc O.TChann
OT.Identification	The TOE must provide means to store Initialisation and Pre-Personalisation Data in its non-volatile memory. The Initialisation Data must provide a unique identification of	No contradiction with the security

Platform objective label	Platform objective short description (refer to [ST-PLTF] for the full description)	Link to the composite-product
	the IC during the manufacturing and the card issuing life cycle phases of the application data requiring PACE usage (e.g. travel document for MRTD). The storage of the Pre-Personalisation data includes writing of the Personalisation Agent Key(s).	objectives of the composite TOE
OT.Prot_Abuse_Func	The TOE must prevent that functions of the TOE, which may not be used in TOE operational phase, can be abused in order (i) to manipulate or to disclose the User Data stored in the TOE, (ii) to manipulate or to disclose the TSF-data stored in the TOE, (iii) to manipulate (bypass, deactivate or modify) soft-coded security functionality of the TOE.	O.Enc O.AccCtrl
OT.Prot_Inf_Leak	The TOE must provide protection against disclosure of confidential User Data or/and TSF-data stored and/or processed by the TOE • by measurement and analysis of the shape and amplitude of signals or the time between events found by measuring signals on the electromagnetic field, power consumption, clock, or I/O lines, • by forcing a malfunction of the TOE and/or • by a physical manipulation of the TOE	O.PhysProt
OT.Prot_Phys_Tamper	The TOE must provide protection of confidentiality and integrity of the User Data, the TSF-data and the TOE's Embedded Software by means of • measuring through galvanic contacts representing a direct physical probing on the chip's 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 electrical charges (using tools used in solid-state physics research and IC failure analysis), • manipulation of the hardware and its security functionality, as well as • controlled manipulation of memory contents (User Data, TSF-data) • with a prior reverse-engineering to understand the design and its properties and functionality.	O.PhysProt

Platform objective label	Platform objective short description (refer to [ST-PLTF] for the full description)	Link to the composite-product
OT.Prot_Malfunction	The TOE must ensure its correct operation. The TOE must prevent its operation outside the normal operating conditions where reliability and secure operation have not been proven or tested. This is to prevent functional errors in the TOE. The environmental conditions may include external energy (esp. electromagnetic) fields, voltage (on any contacts), clock frequency or temperature.	O.PhysProt
OT.Sens_Data_EAC2	The TOE must ensure confidentiality of sensitive user data by granting access to sensitive data only to EAC2 terminals with corresponding access rights. The authorization of an EAC2 terminal is the minimum set of the access rights drawn from the terminal certificate used for successful authentication and the corresponding DV and CVCA certificates, and the access rights sent to the electronic document as part of PACE	O.AccCtrl, O.I&A

Table 3 Compatibility between objectives for the TOE

We can therefore conclude that the objectives for the TOE of [ST-CSP] and [ST-PLTF] are consistent.

5.3.2.2 Compatibility between objectives for the environment

Platform objective label	Platform objective short description (refer to [ST-PLTF] for the full description)	Link to the composite-product
OE.APPLET	No applet loaded post-issuance shall contain native methods	CSP package is full javacard package thus does not contain native methods
OE.VERIFICATION	All the bytecodes shall be verified at least once, before the loading, before the installation or before the execution, depending on the card capabilities, in order to ensure that each bytecode is valid at execution time.	CSP package has passed byte code verification
OE.CODE-EVIDENCE	For application code loaded pre-issuance, evaluated technical measures implemented by the TOE or audited organizational measures must ensure that loaded	If CSP package loaded pre-issuance: fulfilled by audited organizational measures

Platform objective label	Platform objective short description (refer to [ST-PLTF] for the full description)	Link to the composite-product
	application has not been changed since the code verifications required in OE.VERIFICATION. For application code loaded post-issuance and verified off-card according to the requirements of OE.VERIFICATION, the verification authority shall provide digital evidence to the TOE that the application code has not been modified after the code verification and that he is the actor who performed code verification. For application code loaded post-issuance and partially or entirely verified on-card, technical measures must ensure that the verification required in OE.VERIFICATION are performed. On-card bytecode verifier is out of the scope of this Protection Profile	If CSP package loaded post-issuance: fulfilled by technical measures
OE.SECURITY-DOMAINS	Security domains can be dynamically created, deleted and blocked during usage phase in post-issuance mode.	Not managed by CSP package
OE.QUOTAS	Security domains and applets instances are subject to quotas of memory at creation and during their life time	Not managed by CSP package
OE.KEY-CHANGE	The security domain keys of the VA must be securely generated prior storage in the Secure Element	Not managed by CSP package
OE.VERIFICATION-AUTHORITY	The VA should be a trusted actor who is able to guarantee and check the digital signature attached to an application	Not managed by CSP package

Platform objective label	Platform objective short description (refer to [ST-PLTF] for the full description)	Link to the composite-product
OE.CONTROLLING-AUTHORITY	The VA should be a trusted actor who is able to guarantee and check the digital signature attached to an application.	Not managed by CSP package
OE.APPS-PROVIDER	The AP shall be a trusted actor that provides basic or secure applications. He must be responsible of his security domain keys	Not managed by CSP package
OE.TRUSTED-APPS-DEVELOPER	The trusted application developer shall be a trusted actor that provides basic or secure application where correct usage of the TOE has been verified applying a secure development process in a secure development environment	CSP package developer is THALES and is a trusted actor enforcing secure development process in a secure development environment
OE.TRUSTED-APPS_PRE-ISSUANCE-LOADING	The pre-issuance loading on the platform must be done only using trusted or verified applets, and applying an audited process in a secure environment	CSP package is a trusted and verified applets, and THALES is applying an audited process in a secure environment
OE.GEMACTIVATE-ADMIN	The GemActivate administrator (Thales) shall be a trusted actor responsible for additional code loading/activation and optional platform service activation in post issuance	THALES is a trusted actor responsible for additional code loading/activation and optional platform service activation in post issuance
OE.OS-UPDATE-EVIDENCE	For additional code loaded pre-issuance, evaluated technical measures implemented by the TOE or audited organizational measures must ensure that the additional code (1) has been issued by the genuine OS Developer (2) has not been altered since it was issued by the genuine OS Developer. For additional code loaded post-issuance, the OS Developer shall provide	Not managed by CSP package

Platform objective label	Platform objective short description (refer to [ST-PLTF] for the full description)	Link to the composite-product
	digital evidence to the TOE that (1) he is the genuine developer of the additional code and (2) the additional code has not been modified since it was issued by the genuine OS Developer.	
OE.OS-UPDATE-ENCRYPTION	For additional code loaded post-issuance, the OS Developer shall encrypt the additional code so that its confidentiality is ensured when it is transmitted to the TOE for loading and installation.	OE.SUCP
OE.Secure_ACode_Management	Key management processes related to the OS Update capability shall take place in a secure and audited environment. The key generation processes shall guarantee that cryptographic keys are of sufficient quality and appropriately secured to ensure confidentiality, authenticity and integrity of the keys	OE.SecManag OE.SUCP
OE.Personalisation	The Issuer must ensure that the Personalisation Agents acting on his behalf (i) establish the correct identity of the applicative user (e.g. travel document holder) and create the accurate applicative data* and write them in TOE.	Not managed by CSP package
OE.Terminal	The terminal operators must operate their terminals as follows: 1.) The related terminals (basic inspection systems, cf. above) are used by terminal operators and by application users	Not managed by CSP package

Platform objective label	Platform objective short description (refer to [ST-PLTF] for the full description)	Link to the composite-product
	(e.g.travel document presenter for MRTD) as defined in [PKI]. 2.) The related terminals implement the terminal parts of the PACE protocol. The PACE terminal uses randomly and (almost) uniformly selected nonces, if required by the protocols (for generating ephemeral keys for Diffie-Hellmann). 3.) The related terminals need not to use any own credentials. The related terminals and their environment must ensure confidentiality and integrity of respective data handled by them (e.g. confidentiality of the PACE passwords, integrity of PKI certificates, etc.), where it is necessary for a secure operation of the TOE according to the current ST.	
OE.Prot_Logical_Data	The inspection system of the applicative entity (e.g. receiving State or Organisation) ensures the confidentiality and integrity of the data read from the TOE and applicative data (e.g. logical travel document). The inspection system will prevent eavesdropping to their	Not managed by CSP package

Platform objective label	Platform objective short description (refer to [ST-PLTF] for the full description)	Link to the composite-product
	communication with the TOE before secure messaging is successfully established.	
OE.User_Obligations	The application user (e.g. travel document holder) may reveal, if necessary, his or her verification values of the PACE password to an authorized person or device who definitely act according to respective regulations and are trustworthy.	Not managed by CSP package
OE.Chip_Auth_Key	The electronic document issuer has to ensure that the electronic document's chip authentication key pair and the Restricted Identification key pair are generated securely, that the private keys of these key pairs are stored correctly in the electronic document's chip, and that the corresponding public keys are distributed to the EAC2 terminals that are used according to [TR03110] to check the authenticity of the electronic document's chip.	Not managed by CSP package
OE.Terminal_Authentication	The electronic document issuer shall establish a public key infrastructure for the card verifiable certificates used for Terminal Authentication. For this aim, the electronic document issuer shall run a Country Verifying Certification Authority. The instances of the PKI shall fulfill the requirements and rules of the corresponding certificate policy. The electronic document issuer shall make the CVCA certificate available to the personalization agent or the manufacturer.	Not managed by CSP package

Table 4 Compatibility between objectives for the environment

6 EXTENDED COMPONENTS DEFINITION

6.1 GENERATION OF RANDOM NUMBERS (FCS_RNG)

Family behaviour

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

Component levelling:

FCS_RNG: Random number generation	1

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

Management: FCS_RNG.1
There are no management activities foreseen.

Audit: FCS_RNG.1
There are no auditable events foreseen.

FCS_RNG.1 Random number generation

Hierarchical to: No other components
Dependencies: No dependencies

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

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

6.2 CRYPTOGRAPHIC KEY DERIVATION (FCS_CKM.5)

This chapter describes a component of the family Cryptographic key management (FCS_CKM) for key derivation as process by which one or more keys are calculated from either a pre-shared key or a shared secret and other information. Key derivation is the deterministic repeatable process by which one or more keys are calculated from both a pre-shared key or shared secret, and other information, while key generation required by FCS_CKM.1 uses internal random numbers.

The component FCS_CKM.5 is on the same level as the other components of the family FCS_CKM.

Management: FCS_CKM.5
There are no management activities foreseen

Audit: FCS_CKM.5
The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:
a) Minimal: Success and failure of the activity.

b) Basic: The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys).

FCS_CKM.5 Requires the TOE to provide key derivation.

FCS_CKM.5 Cryptographic key derivation

Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.5.1	The TSF shall derive cryptographic keys [assignment: *key type*] from [assignment: *input parameters*] in accordance with a specified cryptographic key derivation algorithm [assignment: *cryptographic key derivation algorithm*] and specified cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

6.3 AUTHENTICATION PROOF OF IDENTITY (FIA_API)

To describe the IT security functional requirements of the TOE a sensitive family (FIA_API) of the Class FIA (Identification and authentication) is defined here. This family describes the functional requirements for the proof of the claimed identity for the authentication verification by an external entity where the other families of the class FIA address the verification of the identity of an external entity.

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

Component levelling:

FIA_API.1 Authentication Proof of Identity, provides prove of the identity of the TOE to an external entity.

Management: FIA_API.1
The following actions could be considered for the management functions in FMT:
a) Management of authentication information used to prove the claimed identity.

Audit: FIA_API.1
There are no auditable events foreseen.

FIA_API.1 Authentication Proof of Identity

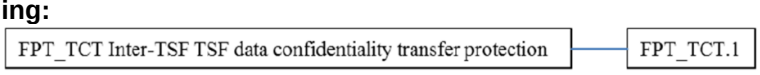
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_API.1.1	The TSF shall provide a [assignment: authentication mechanism] to prove the identity of the [assignment: *object, authorized user or role*] to an external entity.

6.4 INTER-TSF TSF DATA CONFIDENTIALITY TRANSFER PROTECTION (FPT_TCT)

This section describes the functional requirements for confidentiality protection of inter-TSF transfer of TSF data. The family is similar to the family Basic data exchange confidentiality (FDP_UCT) which defines functional requirements for confidentiality protection of exchanged user data.

Family Behaviour
This family requires confidentiality protection of exchanged TSF data.

Component levelling:



FPT_TCT.1 Requires the TOE to protect the confidentiality of information in exchanged the TSF data.

Management: FPT_TCT.1
There are no management activities foreseen.

Audit: FPT_TCT.1
There are no auditable events foreseen.

FPT_TCT.1 TSF data confidentiality transfer protection

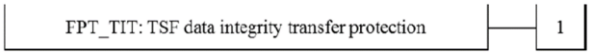
Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FMT_MTD.1 Management of TSF data or FMT_MTD.3 Secure TSF data]
FPT_TCT.1.1	The TSF shall enforce the [assignment: *access control SFP, information flow control SFP*] by providing the ability to [selection: *transmit, receive, transmit and receive*] TSF data in a manner protected from unauthorised disclosure.

6.5 INTER-TSF TSF DATA INTEGRITY TRANSFER PROTECTION (FPT_TIT)

This section describes the functional requirements for integrity protection of TSF data exchanged with another trusted IT product. The family is similar to the family Inter-TSF user data integrity transfer protection (FDP_UIT) which defines functional requirements for integrity protection of exchanged user data.

Family Behaviour
This family requires integrity protection of exchanged TSF data.

Component levelling:



FPT_TIT.1Requires the TOE to protect the integrity of information in exchanged the TSF data.

Management: FPT_TIT.1
There are no management activities foreseen.

Audit: FPT_TIT.1
There are no auditable events foreseen.

FPT_TIT.1 TSF data integrity transfer protection

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FMT_MTD.1 Management of TSF data or FMT_MTD.3 Secure TSF data]
FPT_TIT.1.1	The TSF shall enforce the [assignment: *access control SFP, information flow control SFP*] to [selection: *transmit, receive, transmit and receive*] TSF data in a manner protected from [selection: modification, deletion, insertion, replay] errors.

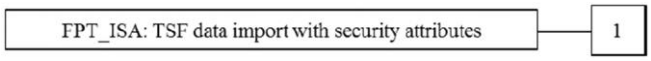
FPT_TIT.1.2	The TSF shall be able to determine on receipt of TSF data, whether [selection: *modification, deletion, insertion, replay*] has occurred.

6.6 TSF DATA IMPORT WITH SECURITY ATTRIBUTES (FPT_ISA)

This section describes the functional requirements for TSF data import with security attributes from another trusted IT product. The family is similar to the family Import from outside of the TOE (FDP_ITC) which defines functional requirements for user data import with security attributes.

Family Behaviour
This family requires TSF data import with security attributes.

Component levelling:



FPT_ISA.1 Requires the TOE to import TSF data with security attributes.

Management: FPT_ISA.1
There are no management activities foreseen.

Audit: FPT_ISA.1
There are no auditable events foreseen.

FPT_ISA.1 Import of TSF data with security attributes

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FMT_MTD.1 Management of TSF data or FMT_MTD.3 Secure TSF data FMT_MSA.1 Management of security attributes, or FMT_MSA.4 Security attribute value inheritance] FPT_TDC.1 Inter-TSF basic TSF data consistency
FPT_ISA.1.1	The TSF shall enforce the [assignment: *access control SFP, information flow control SFP*] when importing TSF data, controlled under the SFP, from outside of the TOE.
FPT_ISA.1.2	The TSF shall use the security attributes associated with the imported TSF data.
FPT_ISA.1.3	The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the TSF data received.
FPT_ISA.1.4	The TSF shall ensure that interpretation of the security attributes of the imported TSF data is as intended by the source of the TSF data.
FPT_ISA.1.5	The TSF shall enforce the following rules when importing TSF data controlled under the SFP from outside the TOE: [assignment: *additional importation control rules*].

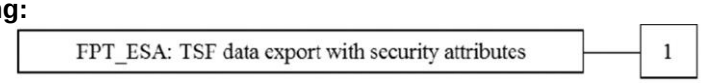
6.7 TSF DATA EXPORT WITH SECURITY ATTRIBUTES (FPT_ESA)

This section describes the functional requirements for TSF data export with security attributes to another trusted IT product. The family is similar to the family Export to outside of the TOE (FDP_ETC) which defines functional requirements for user data export with security attributes.

Family Behaviour

This family requires TSF data export with security attributes.

Component levelling:



FPT_ESA.1 Requires the TOE to export TSF data with security attributes.

Management: FPT_ESA.1
There are no management activities foreseen.

Audit: FPT_ESA.1
There are no auditable events foreseen.

FPT_ESA.1 Export of TSF data with security attributes

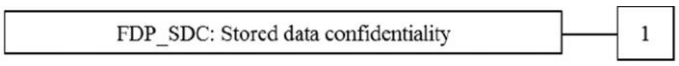
Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FMT_MTD.1 Management of TSF data or FMT_MTD.3 Secure TSF data] [FMT_MSA.1 Management of security attributes, or FMT_MSA.4 Security attribute value inheritance] FPT_TDC.1 Inter-TSF basic TSF data consistency
FPT_ESA.1.1	The TSF shall enforce the [assignment: access control SFP, information flow control SFP] when exporting TSF data, controlled under the SFP(s), outside of the TOE.
FPT_ESA.1.2	The TSF shall export the TSF data with the TSF data's associated security attributes.
FPT_ESA.1.3	The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported TSF data.
FPT_ESA.1.4	The TSF shall enforce the following rules when TSF data is exported from the TOE: [assignment: *additional exportation control rules*].

6.8 STORED DATA CONFIDENTIALITY (FDP_SDC)

To define the security functional requirements of the TOE an additional family (FDP_SDC.1) of the Class FDP (User data protection) is defined here.
The family “Stored data confidentiality (FDP_SDC)” is specified as follows.

Family behaviour
This family provides requirements that address protection of user data confidentiality while these data are stored within memory areas protected by the TSF. The TSF provides access to the data in the memory through the specified interfaces only and prevents compromise of their information bypassing these interfaces. It complements the family Stored data integrity (FDP_SDI) which protects the user data from integrity errors while being stored in the memory.

Component levelling



FDP_SDC.1Requires the TOE to protect the confidentiality of information of the user data in specified memory areas.

Management: FDP_SDC.1
There are no management activities foreseen.

Audit: FDP_SDC.1
There are no auditable events foreseen.

FDP_SDC.1Stored data confidentiality

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FDP_SDC.1.1	The TSF shall ensure the confidentiality of the information of the user data while it is stored in the [assignment: *memory area*].

7 SECURITY REQUIREMENTS

7.1 SECURITY FUNCTIONAL REQUIREMENTS

For this section, a presentation choice has been selected. Each SFR may present a table with different type of algorithms treated. For each case, there is no distinction regarding the technical objectives fulfilled by each row on the table (thus algorithm family). The technical objectives are the same disregarding this differentiation.

The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections that have been made by the ST authors are denoted as *italic* text and the original text of the PP component is given by a footnote. Selections filled in by the ST author appear in square brackets with an indication that a selection is to be made, [selection:], and are *italicized*.

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments that have been made by the ST authors are denoted by showing as *italic* text and the original text of the PP component is given by a footnote. Assignments filled in by the ST author appear in square brackets with an indication that an assignment is to be made [assignment:], and are *italicized*.

The TOE provides cryptographic security services for encryption and decryption of user data, entity authentication of external entities and to external entities, authentication prove and verification of user data, trusted channel and random number generation.

The TOE enforces the Cryptographic Operation SFP for protection of theses cryptographic services which subjects, objects, and operations are defined in the SFRs FDP_ACC.1/Oper and FDP_ACF/Oper.

The TOE provides hybrid encryption and decryption combined with data integrity mechanisms for the cipher text as cryptographic security service of the TOE. The encryption FCS_COP.1/HEM combines the generation of a data encryption key and message authentication code (MAC) key, the asymmetric encryption of the data encryption key with an asymmetric key encryption key, cf. FCS_CKM.1/ECKA-EG, FCS_CKM.1/RSA, and the symmetric encryption of the data with the data encryption key and data integrity mechanism with MAC calculation for the cipher text. The receiver reconstructs the data encryption key and the MAC key, cf. FCS_CKM.5/ECKA-EG, calculates the MAC for the cipher text and compares it with the received MAC. If the integrity of the cipher text is determined than the receiver decrypts the cipher text with the data decryption key, cf. FCS_COP.1/HDM.

In general, authentication is the provision of assurance of the claimed identity of an entity. The TOE authenticates human users by password, cf. FIA_UAU.5.1 clause 1. But a human user may authenticate themselves to a token and the token authenticates to the TOE. Cryptographic authentication mechanisms allow an entity to prove its identity or the origin of its data to a verifying entity by demonstrating its knowledge of a secret. The entity authentication is required by FIA_UAU.5.1 clauses (2) to (6). The chapter 6.3 describes SFR for the authentication of the TOE to external entities required by the SFR FIA_API.1. This authentication may include attestation of the TOE as genuine TOE sample, cf. 7.1.4. The authentication may be mutual as required for trusted channels in chapter 7.1.5.

Protocols may use symmetric cryptographic algorithms, where the proving and the verifying entity using the same secret key, may demonstrate that the proving entity belongs to a group of entities sharing this key, e.g. sender and receiver (cf. FTP_ITC.1, FCS_COP.1/TCM). In case of asymmetric entity authentication mechanisms the proving entity uses a private key and the verifying entity uses the corresponding public key closely linked to the claimed identity often by means of a certificate. The same cryptographic mechanisms for digital signature generation algorithm (FCS_COP.1/CDS-*) and signature verification algorithm (cf. FCS_COP.1/VDS-*) may be used for entity authentication, data authentication and non-repudiation depending on the security attributes of the cryptographic keys e.g. encoded in the certificate (cf. FPT_ISA.1/Cert).

Trusted channel requires mutual authentication of endpoints with key exchange of key agreement, protection of confidentiality by means of encryption and cryptographic data integrity protection.

The TSF provides security management for user and TSF data including cryptographic keys. The key management comprises administration and use of generation, derivation, registration, certification, deregistration, distribution, installation, storage, archiving, revocation and destruction of keying material in accordance with a security policy. The key management of the TOE supports the generation, derivation, export, import, storage and destruction of cryptographic keys. The cryptographic keys are managed together with their security attributes.

The TOE enforces the Key Management SFP to protect the cryptographic keys (as data objects fo TSF data) and the key management services (as operation, cf. to SFR of the FMT class) provided for Administrators, Crypto-Officers, Key Owners and (as subjects). Note the cryptographic keys will be used for cryptographic operations under Cryptographic Operation SFP as well.

The subjects, objects and operations of the Update SFP are defined in the SFR FDP_ACC.1/UCP and FDP_ACF.1/UCP.

The SFR for cryptographic mechanisms based on elliptic curves refer to the following table for selection of curves, key sizes and standards.

Elliptic curve	Key size	Standard
brainpoolP256r1	*256 bits*	*RFC5639 [RFC5639], TR-03111, section 4.1.3 [TR-03111]*
brainpoolP384r1,	*384 bits*	*RFC5639 [RFC5639], TR-03111, section 4.1.3 [TR-03111]*
brainpoolP512r1	*512 bits*	*RFC5639 [RFC5639], TR-03111, section 4.1.3 [TR-03111]]*
Curve P-256	*256 bits*	*FIPS PUB 186-4 B.4 and D.1.2.3 [FIPS PUB 186-4]*
Curve P-384	*384 bits*	*FIPS PUB 186-4 B.4 and D.1.2.4 [FIPS PUB 186-4]*
Curve P-521	*521 bits*	*FIPS PUB 186-4 B.4 and D.1.2.5 [FIPS PUB 186-4]*

***Table 5*: Elliptic curves, key sizes and standards**

For Diffie-Hellman key exchange refer to the following groups

Name	IANA no.	Specified in
256-bit random ECP group	19	[RFC5903]
384-bit random ECP group	20	[RFC5903]
521-bit random ECP group	21	[RFC5903]
brainpoolP256r1	28	[RFC6954]
brainpoolP384r1	29	[RFC6954]
brainpoolP512r1	30	[RFC6954]

***Table 6*: Recommended groups for the Diffie-Hellman key exchange**

7.1.1 Key management

7.1.1.1 Management of security attributes

FDP_ACC.1/KM Subset access control – Cryptographic operation

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/KM The TSF shall enforce the *Key Management SFP* on

(1) *subjects: [Administrator][2], Key Owner;*
(2) *objects: operational cryptographic keys*;
(3) *operations: key generation, key derivation, key import, key export, key destruction.*

FMT_MSA.1/KM Management of security attributes – Key security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or

DP_IFC.1 Subset information flow control]

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1/KM The TSF shall enforce the *Key Management SFP and Cryptographic Operation SFP* to restrict the ability to

(1) *change_default the security attributes Identity of the key, Key entity of the key, Key type, Key usage type, Key access control attributes, Key validity time period* to *[selection: Administrator][3],*

(2) ***modify or delete the security attributes Identity of the key, Key entity, Key type, Key usage type, Key validity time period of an existing key to none,***

(3) ***modify independent on key usage the security attributes Key usage counter of an existing key to none.***

(4) ***modify the security attributes Key access control attribute of an existing key to [selection: Administrator][4],***

(5) ***query the security attributes Key type, Key usage type, Key access control attributes, Key validity time period and Key usage counter of an identified key to [selection: Key Owner][5].***

FMT_MSA.3/KM Static attribute initialization – Key management

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

FMT_MSA.3.1/KM The TSF shall enforce the *Key Management SFP, Cryptographic Operation SFP and Update SFP* to provide *restrictive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/KM The TSF shall allow the [selection: *Administrator*][6] to specify alternative initial values to override the default values when a **cryptographic key** is created.

---

[2] [assignment: subjects: [selection: Administrator, Crypto-Officer]]
[3] [*selection: Administrator, Crypto-Officer*]
[4] [*selection: Administrator, Crypto-Officer*]
[5] [selection: Administrator, Crypto-Officer, Key Owner]
[6] [selection: *Administrator, Crypto-Officer*]

FMT_MTD.1/KM Management of TSF data – Key management

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1/KM The TSF shall restrict the ability to

(1) *create according to FCS_CKM.1* the *cryptographic keys* to [selection: *Administrator, Key Owner*][7],

(2) *import according to FPT_TCT.1/CK, FPT_TIT.1/CK and FPT_ISA.1/CK* the *cryptographic keys* to *[selection: Administrator][8]*,

(3) ***export according to FPT_TCT.1/CK, FPT_TIT.1/CK and FPT_ESA.1/CK* the *cryptographic keys* to *[selection: Administrator, Key Owner][9]* if *security attribute of the key allows export,***

(4) ***delete according to FCS_CKM.4* the *cryptographic keys* to *[selection: Administrator, Key Owner][10]*.**

7.1.1.2 Hash based functions

FCS_COP.1/Hash Cryptographic operation – Hash

Hierarchical to: No other components.

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

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/Hash The TSF shall perform *hash generation* in accordance with a specified cryptographic algorithm *SHA-256, SHA-384, SHA-512* and cryptographic key sizes *none* that meet the following: *FIPS 180-4 [FIPS PUB 180-4]*.

Application note 1: The hash function is a cryptographic primitive used for HMAC, cf. FCS_COP.1/HMAC, digital signature creation, cf. FCS_COP.1/CDS-*, digital signature verification, cf. FCS_COP.1/VDS-*, and key derivation, cf. FCS_CKM.5.

7.1.1.3 Management of Certificates

[7] [selection: *Administrator, Crypto-Officer, Key Owner*]
[8] *[selection: Administrator, Crypto-Officer]*
[9] *[selection: Administrator, Crypto-Officer, Key Owner]*
[10] *[selection: Administrator, Crypto-Officer, Key Owner]*

FMT_MTD.1/RK Management of TSF data – Root key

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1/RK The TSF shall restrict the ability to

(1) *create, modify, clear and delete* the *root key pair* to [selection: *Administrator*][11].
(2) import and delete a known as authentic public key of a certification authority in a PKI to [selection: Administrator][12]

Application note 2: The root key is defined here with respect to the key hierarchy known to the TOE. In case of clause (1), i. e. may be a key pair of an TOE internal key hierarchy. In clause (2) it may be a root public key of a PKI or a public key of another certification authority in a PKI known as authentic certificate signing key. The PKI may be used for user authentication, key management and signature-verification. The second bullet is a refinement to avoid an iteration of component and therefore printed in bold.

FPT_TIT.1/Cert TSF data integrity transfer protection – Certificates

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

[FMT_MTD.1 Management of TSF data or

FMT_MTD.3 Secure TSF data]

FPT_TIT.1.1/Cert The TSF shall enforce the *Key Management SFP* to *receive* **certificate** in a manner protected from *modification and insertion* errors.

FPT_TIT.1.2/Cert The TSF shall be able to determine on receipt of **certificate**, whether *modification and insertion* has occurred.

FPT_ISA.1/Cert Import of TSF data with security attributes - Certificates

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

[FMT_MTD.1 Management of TSF data or FMT_MTD.3 Secure TSF data]

[FMT_MSA.1 Management of security attributes, or

FMT_MSA.4 Security attribute value inheritance]

FPT_TDC.1 Inter-TSF basic TSF data consistency

FPT_ISA.1.1/Cert The TSF shall enforce the *Key management SFP* when importing **certificates**, controlled under the SFP, from outside of the TOE.

FPT_ISA.1.2/Cert The TSF shall use the security attributes associated with the imported **certificate**.

[11] [selection: *Administrator, Crypto-Officer*]
[12] [selection: Administrator, Crypto-Officer]

FPT_ISA.1.3/Cert The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the **certificates** received.

FPT_ISA.1.4/Cert The TSF shall ensure that interpretation of the security attributes of the imported **certificates** is as intended by the source of the **certificates**.

FPT_ISA.1.5/Cert The TSF shall enforce the following rules when importing **certificates** controlled under the SFP from outside the TOE:

(1) *The TSF imports the TSF data in certificates only after successful verification of the validity of the certificate in the certificate chain until known as authentic certificate according to FMT_MTD.1/RK.*

(2) *The validity verification of the certificate shall include*

(a) *the verification of the digital signature of the certificate issuer except for root certificates,*

(b) *the security attributes in the certificate pass the interpretation according to FPT_TDC.1*.

FPT_TDC.1/Cert Inter-TSF basic TSF data consistency - Certificate

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TDC.1.1/Cert The TSF shall provide the capability to consistently interpret *security attributes of cryptographic keys in the certificate and identity of the certificate issuer* when shared between the TSF and another trusted IT product.

FPT_TDC.1.2/Cert The TSF shall use **the following rules**:

(1) *the TOE reports about conflicts between the Key identity of stored cryptographic keys and cryptographic keys to be imported,*

(2) *the TOE does not change the security attributes Key identity, Key entity, Key type, Key usage type and Key validity time period of public key being imported from the certificate,*

(3) *the identity of the certificate issuer shall meet the identity of the signer of the certificate w*hen interpreting **the certificate from a trust center.**

Application note 3: The security attributes assigned to certificate holder and cryptographic key in the certificate are used as TSF data of the TOE. The certificate is imported from trust center directory service or any other source but verified by the TSF (i.e. if verified successfully the source is the trusted IT product trust center directory server).

7.1.1.4 Key generation, agreement and destruction

Key generation (cf. FCS_CKM.1/ECC, FCS_CKM.1/RSA) is a randomized process which uses random secrets (cf. FCS_RNG.1), applies key generation algorithms and defines security attributes depending on the intended use of the keys and which has the property that it is computationally infeasible to deduce the output without prior knowledge of the secret input. *Key derivation* (cf. FCS_CKM.5/ECC) is a deterministic process by which one or more keys are calculated from a pre-shared key or shared secret or other information. It allows repeating the key generation if the same input is provided. *Key agreement* (cf. FCS_CKM.5/ECDHE) is a key-establishment procedure process for establishing a shared secret key between entities in such a way that neither of them can predetermine the value of that key

independently of the other party's contribution. Key agreement allows each participant to enforce the cryptographic quality of the agreed key. The component FCS_CKM.1 was refined for key agreement because it normally uses random bits as input. Hybrid cryptosystems (FCS_CKM.1/ECKA-EG, FCS_CKM.1/AES_RSA) are a combination of a public key cryptosystem with an efficient symmetric key cryptosystem.

The user may need to specify the type of key, the cryptographic key generation algorithm, the security attributes and other necessary parameters.

FCS_RNG.1 Random number generation

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RNG.1.1 The TSF shall provide a [selection: *hybrid deterministic*][13] random number generator that implements: [assignment: Enhanced backward secrecy and Enhanced forward secrecy][14].

FCS_RNG.1.2 The TSF shall provide random numbers that meet [assignment: [AIS 20/31] Test Procedure A][15].

Application note 4: The random bit generation shall be used for key generation and key agreement according to all instantiations of FCS_CKM.1, challenges in cryptographic protocols and cryptographic operations using random values according to FCS_COP.1/HEM and FCS_COP.1/TCE. The TOE provides the random number generation as security service for the user.

FCS_CKM.1/AES Cryptographic key generation – AES key

Hierarchical to: No other components.

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

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1/AES The TSF shall generate cryptographic **AES** keys in accordance with a specified cryptographic key generation algorithm *AES* and specified cryptographic key sizes *128 bits, [*selection: *256 bits]*[16] that meet the following: *ISO 18033-3 [ISO/IEC 18033-3]*.

Application note 5: The cryptographic key may be used with FCS_COP.1/ED, e. g. for internal purposes.

FCS_CKM.5/AES Cryptographic key derivation – AES key derivation

Hierarchical to: No other components.

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

[13] [selection: *physical, non-physical true, deterministic, hybrid physical, hybrid deterministic*]
[14] [assignment: *list of security capabilities*]
[15] [assignment: *a defined quality metric*]
[16] *[*selection: *256 bits, no other key size]*

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.5.1/AES The TSF shall derive cryptographic *AES* key from [assignment: *Key derivation buffer*][17] in accordance with a specified cryptographic key derivation algorithms *AES key generation using bit string derived from input parameters with KDF* and specified cryptographic key sizes *128 bits, [*selection: *no other key size]*[18] that meet the following: *NIST SP800- 56C [NIST-SP800-56C]*.

FCS_CKM.1/ECC Cryptographic key generation – Elliptic curve key pair ECC

Hierarchical to: No other components.

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

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1/ECC The TSF shall generate cryptographic **elliptic curve** keys ***pair*** in accordance with a specified cryptographic key generation algorithm *ECC key pair generation with [selection: all elliptic curves in the* Table 5*]*[19] and specified cryptographic key sizes *[selection: all key size in the* Table 5*]*[20] that meet the following: *[selection: all standards in the* Table 5*]*[21].

Application note 6: The elliptic key pair generation uses a random bit string as input for the ECC key generation algorithm. The keys generation according to FCS_CKM.1/ECC and key derivation according to FCS_CKM.5/ECC are intended for different key management use cases but the keys itself may be used for same cryptographic operations.

FCS_CKM.5/ECC Cryptographic key derivation – ECC key pair derivation

Hierarchical to: No other components.

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

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.5.1/ECC The TSF shall derive cryptographic *elliptic curve* keys *pair* from [assignment: *Key derivation buffer*][22] in accordance with a specified cryptographic key derivation algorithm *ECC key pair generation with [selection: all elliptic curves in* Table 5*]*[23] *using bit string derived from input parameters with [assignment: KDF]*[24] and specified cryptographic key sizes *[selection: all key size in the* Table 5*]*[25] that meet the following: *[selection: all standards in the* Table 5*]*[26]*, [TR-03111]*.

Application note 7: The elliptic key pair derivation applies a key derivation function (KDF), e.g. from *[TR-03111] (Section 4.3.3.)* to the input parameter. It uses the output string of KDF instead of the random bit string as input for the ECC key generation algorithm (*[TR-03111], Section 4.1.1, Algorithms 1 or 2)*. The input

[17] [assignment: *input parameters*]
[18] *[*selection: *256 bits, no other key size]*
[19] *[selection: elliptic curves in the table]*
[20] *[selection: key size in the table]*
[21] *[selection: standards in the table]*
[22] [assignment: *input parameters*]
[23] *[selection: elliptic curves in table]*
[24] *[assignment: KDF]*
[25] *[selection: key size in the table]*
[26] *[selection: standards in the table]*

parameters shall include a secret of the length at least of the key size to ensure the confidentiality of the private key. The input parameters may include public known values or even values provided by external entities.

FCS_CKM.1/RSA Cryptographic key generation – RSA key pair

Hierarchical to: No other components.

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

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1/RSA The TSF shall generate cryptographic **RSA** key **pair** in accordance with a specified cryptographic key generation algorithm *RSA* and specified cryptographic key sizes [assignment: *2048 and 3072 bits*] that meet the following: *PKCS#1 v2.2 [PKCS#1]*.

Application note 8: The cryptographic key sizes assigned in FCS_CKM.1/RSA must be at least 2000 bits. Cryptographic key sizes of at least 3000 bits are recommended. The FCS_CKM.1/RSA assigns given security attributes *Key identity* and *Key entity.* The security attribute *Key usage type* is DS-RSA for the private signature-creation key and public signature-verification key, RSA_ENC for public RSA encryption key and private RSA decryption key.

FCS_CKM.5/ECDHE Cryptographic key derivation – Elliptic Curve Diffie-Hellman ephemeral key agreement

Hierarchical to: No other components.

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

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.5.1/ECDHE The TSF shall derive cryptographic *ephemeral* keys **for data encryption and MAC with AES-128**, [**selection**: ***none other***] [27] from *an agreed shared secret* in accordance with a specified cryptographic key derivation algorithm *Elliptic Curve Diffie- Hellman ephemeral key agreement [selection: all elliptic curves in* Table 5*][28]and [selection: all DH group in* Table 5*][29]with a key derivation from the shared secret [assignment: key derivation function X.963][30]* and specified cryptographic key sizes *128 bits [selection: none other]*[31] that meet the following: *TR-03111 [TR-03111]*.

Application note 9: The input parameters for key derivation is an agreed shared secret established by means of Elliptic Curve Diffie-Hellman. The Table 5 lists elliptic curves and Table 6 lists the Diffie-Hellman Groups for agreement of the shared secret. The SHA-1 shall be supported for generation of 128 bits AES keys. The SHA-256 shall be selected and used to generate 256 bits AES keys.

[27] [selection: *AES-256, none other*]
[28] *[selection: elliptic curves in table]*
[29] *[selection: DH group in table]*
[30] *[assignment: key derivation function]*
[31] *[selection:256 bits, none other]*

FCS_CKM.1/ECKA-EG Cryptographic key generation – ECKA-EG key generation with ECC encryption

Hierarchical to: No other components.

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

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1/ECKA-EG The TSF shall generate **an ephemeral** cryptographic **elliptic curve** key **pair for ECKGA- EG***[TR-03111], sender role*) in accordance with a specified cryptographic key generation algorithm *ECC key pair generation with [all: elliptic curves in the* Table 5*]*[32] and specified cryptographic key sizes *[all key size in the* Table 5*]*[33] that meet the following: *[all: standards in the* Table 5*]*[34].

FCS_CKM.5/ECKA-EG Cryptographic key derivation – ECKA-EG key derivation

Hierarchical to: No other components.

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

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.5.1/ECKA-EG The TSF shall derive cryptographic *data encryption and MAC* keys *for AES-128, [none other]*[35] from *a private and a public ECC key* in accordance with a specified cryptographic key derivation algorithms *ECKGA-EG[TR-03111] [all: elliptic curves in* Table 5*]*[36] *and X9.63 Key Derivation Function* and specified cryptographic **symmetric** key sizes *128 bits [none other]*[37] that meet the following: *TR- 03111[TR-03111], chapter 4.3.2.2*.

Application note 10: FCS_CKM.5/ECKA-EG is used by both the sender (encryption) and the recipient (decryption) to compute a secret point SAB on an elliptic curve and the derived shared secret ZAB. The shared secret is then used as input to the key derivation function to derive two symmetric keys, the encryption key and the MAC key which are used to encrypt or decrypt the message according to FCS_COP.1/HEM or FCS_COP.1/HDM, respectively. Sender and recipient use however different inputs to FCS_CKM.5/ECKA-EG. The sender first generates an ephemeral ECC key pair according to FCS_CKM.1/ECKA-EG and uses the generated ephemeral private key and the static public key of the recipient as input. The recipient first extracts the ephemeral public key from the encrypted message and uses the ephemeral public key and the static private key (cf. FCS_CKM.1/ECC for key generation) as input. The selection of elliptic curve, the ECC key size and length of the shared secret shall correspond to the selection of the AES key size, e. g. brainpoolP256r1 and 256 bits seed, ECC key and AES keys. FCS_CKM.1/ECKA-EG and FCS_CKM.5/ECKA-EG do not provide self-contained security services for the user but are necessary steps for FCS_COP.1/HEM and FCS_COP.1/HDM (refer to the next section 7.1.3).

FCS_CKM.1/AES_RSA Cryptographic key generation – Key generation and RSA encryption

Hierarchical to: No other components.

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

FCS_CKM.4 Cryptographic key destruction

[32] *[selection: elliptic curves in the table]*
[33] *[selection: key size in the table]*
[34] *[selection: standards in the table]*
[35] *[selection: AES-256, none other]*
[36] *[selection: elliptic curves in table]*
[37] *[selection:256 bits, none other]*

FCS_CKM.1.1/AES_RSA The TSF shall generate **and encrypt seed, derive** cryptographic keys **from seed for data encryption and MAC with AES-128**, [**selection**: ***none other***][38] in accordance with a specified cryptographic key generation algorithm *X9.63 Key Derivation Function[ANSI-X9.63] and RSA EME-OAEP[PKCS#1]* and specified cryptographic **symmetric** key sizes *128 bits [selection: none other]*[39] that meet the following: *ISO/IEC18033-3 [ISO/IEC 18033-3]*, *PKCS #1 v2.2 [PKCS#1]*.

Application note 11: The asymmetric cryptographic key sizes used in FCS_CKM.1/AES_RSA must be at least 2000 bits. Cryptographic key sizes of at least 3000 bits are recommended. FCS_CKM.1/AES_RSA and FCS_CKM.5/AES_RSA do not provide self-contained security services for the user but they are only necessary steps for FCS_COP.1/HEM respective FCS_COP.1/HDM (refer to the next section 7.1.3).

FCS_CKM.5/AES_RSA Cryptographic key derivation – RSA key derivation and decryption

Hierarchical to: No other components.

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

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.5.1/AES_RSA The TSF shall derive cryptographic *data encryption* key *and MAC* key *for AES-128, [selection: none other]*[40] from **decrypted** *RSA encrypted seed* in accordance with a specified cryptographic key derivation algorithm *RSA EME-OAEP[PKCS#1] and X9.63[ANSI-X9.63] Key Derivation Function* and specified cryptographic **symmetric** key sizes *128 bits [selection: none other]*[41] that meet the following: *ISO/IEC 14888-2 [ISO/IEC 14888-2]*.

FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

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

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: *clear key destruction method*][42] that meets the following: [assignment: [JCAPI305] standard][43].

Refinement: The destruction of cryptographic keys shall ensure that any previous information content of the resource about the key is made unavailable upon the deallocation of the resource.

7.1.1.5 Key import and export

FCS_COP.1/KW Cryptographic operation – Key wrap

[38] [selection: *AES-256, none other*]
[39] *[selection:256 bits, none other]*
[40] *[selection:AES-256, none other]*
[41] *[selection:256 bits, none other]*
[42] [assignment: *cryptographic key destruction method*]
[43] [assignment: *list of standards*]

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/KW	The TSF shall perform *key wrap* in accordance with a specified cryptographic algorithm *AES-Keywrap [selection: KW][44]* and cryptographic key sizes **of the *key encryption key*** *128 bits [selection: none other][45]* that meet the following: *NIST SP800-38F [NIST-SP800-38F]*.

Application note 12: The selection of the length of the key encryption key shall be equal or greater than the security bits of the wrapped key for its cryptographic algorithm.

FCS_COP.1/KU Cryptographic operation – Key unwrap

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/KU	The TSF shall perform *key unwrap* in accordance with a specified cryptographic algorithm *AES-Keywrap [selection: KW][46]* and cryptographic key sizes **of the *key encryption key*** *128 bits [selection: none other][47]* that meet the following: *NIST SP800-38F [NIST-SP800-38F]*.

FPT_TCT.1/CK TSF data confidentiality transfer protection – Cryptographic keys

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FMT_MTD.1 Management of TSF data or FMT_MTD.3 Secure TSF data]
FPT_TCT.1.1/CK	The TSF shall enforce the *Key Management SFP* by providing the ability to *transmit and receive* **cryptographic key** in a manner protected from unauthorized disclosure **according to FCS_COP.1/KW and FCS_COP.1/KU**.

[44] *[selection: KW, KWP]*
[45] *[selection:256 bits, none other]*
[46] *[selection: KW, KWP]*
[47] *[selection:256 bits, none other]*

FPT_TIT.1/CK TSF data integrity transfer protection – Cryptographic keys

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FMT_MTD.1 Management of TSF data or FMT_MTD.3 Secure TSF data]
FPT_TIT.1.1/CK	The TSF shall enforce the *Key Management SFP* to *transmit and receive* **cryptographic keys** in a manner protected from *modification and insertion* errors **according to FCS_COP.1/KW**.
FPT_TIT.1.2/CK	The TSF shall be able to determine on receipt of **cryptographic keys**, whether *modification and insertion* has occurred **according to FCS_COP.1/KU**.

FPT_ISA.1/CK Import of TSF data with security attributes – Cryptographic keys

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FMT_MTD.1 Management of TSF data or FMT_MTD.3 Secure TSF data] [FMT_MSA.1 Management of security attributes, or FMT_MSA.4 Security attribute value inheritance] FPT_TDC.1 Inter-TSF basic TSF data consistency
FPT_ISA.1.1/CK	The TSF shall enforce the *Key Management SFP* when importing **cryptographic key**, controlled under the SFP, from outside of the TOE.
FPT_ISA.1.2/CK	The TSF shall use the security attributes associated with the imported **cryptographic key**.
FPT_ISA.1.3/CK	The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the **cryptographic key** received.
FPT_ISA.1.4/CK	The TSF shall ensure that interpretation of the security attributes of the imported **cryptographic key** is as intended by the source of the **cryptographic key**.
FPT_ISA.1.5/CK	The TSF shall enforce the following rules when importing **cryptographic key** controlled under the SFP from outside the TOE: (1) *The TSF imports the TSF data in certificates only after successful verification of the validity of the certificate including verification of digital signature of the issuer and validity time period.* (2) *[assignment: NO additional importation control rules]*[48].

Application note 13: The operational environment is obligated to use trust center services for secure key management, cf. OE.SecManag.

[48] *[assignment: additional importation control rules]*

FPT_TDC.1/CK Inter-TSF basic TSF data consistency – Key import

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_TDC.1.1/CK	The TSF shall provide the capability to consistently interpret *security attributes of* the *imported cryptographic keys* when shared between the TSF and another trusted IT product.
FPT_TDC.1.2/CK	The TSF shall use **the following rules**: (1) *the TOE reports about conflicts between the Key identity of stored cryptographic keys and cryptographic keys to be imported,* (2) *the TOE does not change the security attributes Key identity, Key type, Key usage type and Key validity time period of the key being imported* when interpreting **the imported key data object.**

FPT_ESA.1/CK Export of TSF data with security attributes – Cryptographic keys

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FMT_MTD.1 Management of TSF data or FMT_MTD.3 Secure TSF data] [FMT_MSA.1 Management of security attributes, or FMT_MSA.4 Security attribute value inheritance] FPT_TDC.1 Inter-TSF basic TSF data consistency
FPT_ESA.1.1/CK	The TSF shall enforce the *Key Management SFP* when exporting **cryptographic key**, controlled under the SFP(s), outside of the TOE.
FPT_ESA.1.2/CK	The TSF shall export the **cryptographic key** with the **cryptographic key's** associated security attributes.
FPT_ESA.1.3/CK	The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported **cryptographic key**.
FPT_ESA.1.4/CK	The TSF shall enforce the following rules when **cryptographic key** is exported from the TOE: [assignment: Export of keys and Public key according to [CSP-SPEC] by Administrator or Key Owner only]49.

Application note 14 : There are no fixed rules for presentation of security attributes defined. The element FPT_ESA.1.4/CK must define rules expected in FPT_TDC.1 Inter-TSF basic TSF data consistency if inter-TSF key exchange is intended.

[49] [assignment: *additional exportation control rules*]

7.1.2 Data encryption

FCS_COP.1/ED Cryptographic operation – Data encryption and decryption

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/ED The TSF shall perform *data encryption and decryption* in accordance with a specified cryptographic algorithm *symmetric data encryption according to AES-128 and [selection: no other algorithm]*[50] *in CBC and [selection: CRT, OFB, CFB*[51] *mode* and cryptographic key size *128 bits, [*selection: *256 bits]*[52]that meet the following: *NIST-SP800-38A[NIST-SP800-38A], ISO 18033-3 [ISO/IEC 18033-3], ISO 10116[ISO/IEC 10116].*

Application note 15: Data encryption and decryption should be combined with data integrity mechanisms in Encrypt-then-MAC order, i. e. the MAC is calculated for the ciphertext and verified before decryption. The modes of operation should combine encryption with data integrity mechanisms to authenticated encryption, e. g. the Cipher Block Chaining Mode (CBC, cf. NIST SP800-38A) should be combined with CMAC (cf. FCS_COP.1/MAC) or HMAC (cf. FCS_COP.1/HMAC). For combination of symmetric encryption, decryption and data integrity mechanisms by means of CCM or GCM refer to the next section 7.1.3.

7.1.3 Hybrid encryption with MAC for user data

FCS_COP.1/HEM Cryptographic operation – Hybrid data encryption and MAC calculation

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/HEM The TSF shall perform *hybrid data encryption and MAC calculation* in accordance with a specified cryptographic algorithm *asymmetric key encryption according to [selection: FCS_CKM.1/AES_RSA, FCS_CKM.5/ECDHE]*[53]*, symmetric data encryption according to AES-128, [selection: none other]*[54]*[FIPS197] in [selection: CBC[NIST-SP800-38A], CCM[NIST-SP800-38C], GCM[NIST-SP800-38D]]*[55] *mode with [selection: CMAC[NIST-SP800-38B], GMAC[NIST-SP800-38D], HMAC[RFC2104]]*[56]*calculation* and cryptographic **symmetric** key

[50] *[selection: AES-256, no other algorithm]*
[51] *[selection: CRT, OFB, CFB, no other]*
[52] *[*selection: *256 bits, no other key size]*
[53] *[selection: FCS_CKM.1/ECKA-EG, FCS_CKM.1/AES_RSA, FCS_CKM.5/ECDHE]*
[54] *[selection: AES-256, none other]*
[55] *selection: CBC[NIST-SP800-38A], CCM[NIST-SP800-38C], GCM[NIST-SP800-38D]]*
[56] *[selection: CMAC[NIST-SP800-38B], GMAC[NIST-SP800-38D], HMAC[RFC2104]]*

sizes *128 bits,* [selection: *256 bits]*[57] that meet the following: *the referenced standards above according to the chosen selection*.

Application note 16: Hybrid data encryption and MAC calculation is a self-contained security services of the TOE. The generation and encryption of the seed, derivation of encryption and MAC keys as well as the AES encryption and MAC calculation are only a steps of this service. The hybrid encryption is combined with MAC as data integrity mechanisms for the cipher text, i. e. encrypt-then-MAC creation for CMAC.

FCS_COP.1/HDM Cryptographic operation – Hybrid data decryption and MAC verification

Hierarchical to: No other components.

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

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/HDM The TSF shall perform *hybrid MAC verification and data decryption* in accordance with a specified cryptographic algorithm *asymmetric key decryption according to [selection: FCS_CKM.5/ECDHE]*[58]*, verification of [selection: CMAC[NIST-SP800-38B], GCM[NIST-SP800-38D], HMAC[RFC2104]]*[59] *and symmetric data decryption according to AES with [selection: AES-128][FIPS197]*[60] *in mode [selection: CBC[NIST-SP800-38A], CCM[NIST-SP800-38C], GMAC[NIST-SP800-38D]]*[61] and cryptographic **symmetric** key sizes *128 bits, [selection: 256 bits]*[62] that meet the following: *the referenced standards above according to the chosen selection*.

Application note 17: Hybrid data decryption and MAC verification is a self-contained security services of the TOE. The decryption of the seed and derivation of the encryption key and MAC keys as well as the AES decryption and MAC verification are only a steps of this service. The used symmetric key shall meet the AES CMAC or GMAC and the AES algorithm for decryption of the cipher text for MAC, e. g. verification-then- decrypt for CMAC.

7.1.4 Data integrity mechanisms

Cryptographic data integrity mechanisms comprise 2 types of mechanisms – symmetric message authentication code mechanisms and asymmetric digital signature mechanisms. A message authentication code mechanism comprises the generation of a MAC for original message, the verification of a given pair of message and MAC and symmetric key management. The MAC may be applied to plaintext without encryption but if combined with encryption it should be applied to ciphertexts in Encrypt-then-MAC order.

[57] [selection: *256 bits, no other key size]*
[58] *[selection: FCS_CKM.5/ECDHE, FCS_CKM.5/ECKA-EG, FCS_CKM.5/AES_RSA]*
[59] *[selection: CMAC[NIST-SP800-38B], GCM[NIST-SP800-38D], HMAC[RFC2104]]*
[60] *[selection: AES-128, AES-256][FIPS197]*
[61] *[selection: CBC[NIST-SP800-38A], CCM[NIST-SP800-38C], GMAC[NIST-SP800-38D]]*
[62] *[selection: 256 bits, no other key size]*

FCS_COP.1/MAC Cryptographic operation – MAC using AES

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/MAC The TSF shall perform *MAC generation and verification* in accordance with a specified cryptographic algorithm *AES-128 and [selection: none other]*[63] *[FIPS197] CMAC[NIST-SP800-38B] and [selection: GMAC[NIST-SP800-38D]*[64] and cryptographic key sizes *128 bits [selection: 256 bits*[65]*]* that meet the following: *the referenced standards above according to the chosen selection*.

Application note 18: The MAC may be applied to plaintext and cipher text. The AES-128 CMAC is mandatory. The selection of AES-256 and the key sizes shall correspond to each other.

FCS_COP.1/HMAC Cryptographic operation – HMAC

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/HMAC The TSF shall perform *HMAC generation and verification* in accordance with a specified cryptographic algorithm *HMAC-SHA256 and [selection: HMAC-SHA-1, HMAC-SHA384]*[66] and cryptographic key sizes [assignment: *128, 192 and 256 bits*][67] that meet the following: *RFC2104 [RFC2104] , ISO 9797-2 [ISO/IEC 9797-2]*.

Application note 19: The cryptographic key is a random bit string generated by. FCS_RNG.1 or a referenced internal secret. The cryptographic key sizes assigned in FCS_COP.1/HMAC must be at least 128 bits.

FCS_COP.1/CDS-ECDSA Cryptographic operation – Creation of digital signatures ECDSA

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

[63] *[selection: AES-256, none other]*
[64] *[selection: GMAC[NIST-SP800-38D], no other]*
[65] *[selection: 256 bits, no other key size]*
[66] *[selection: HMAC-SHA-1, HMAC-SHA384, no other]*
[67] [assignment: *cryptographic key sizes*]

FCS_COP.1.1/CDS-ECDSA The TSF shall perform *signature-creation* in accordance with a specified cryptographic algorithm *ECDSA with [selection: all elliptic curves in the Table 5]*[68] and cryptographic key sizes *[selection:all key size in the Table 5]]*[69] that meet the following: *[selection: all standards in the Table 5]]*[70].

Application note 20: The selection of elliptic curve and cryptographic key sizes shall correspond to each other, e. g. elliptic curve *brainpoolP256r1* and key size *256 bits*.

FCS_COP.1/VDS-ECDSA Cryptographic operation – Verification of digital signatures ECDSA

Hierarchical to: No other components.

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

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/VDS-ECDSA The TSF shall perform *signature-verification* in accordance with a specified cryptographic algorithm *ECDSA with [selection:all elliptic curves in the Table 5]]*[71] and cryptographic key sizes *[selection: all key size in the Table 5]]*[72] that meet the following: *[selection:all standards in the Table 5]]*[73].

FCS_COP.1/CDS-RSA Cryptographic operation – Creation of digital signatures RSA

Hierarchical to: No other components.

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

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/CDS-RSA The TSF shall perform *signature-creation* in accordance with a specified cryptographic algorithm *RSA and EMSA-PSS* and cryptographic key sizes [assignment: *2048, 3072 bits*][74] that meet the following: *ISO/IEC 14888-2 [ISO/IEC 14888-2], PKCS #1, v2.2 [PKCS#1]*.

Application note 21: The cryptographic key sizes assigned in FCS_CKM.1/RSA must be at least 2000 bits. Cryptographic key sizes of at least 3000 bits are recommended.

[68] *[selection: elliptic curves in the table]*
[69] *[selection: key size in the table]*
[70] *[selection: standards in the table]*
[71] *[selection: elliptic curves in the table]*
[72] *[selection: key size in the table]*
[73] *[selection: standards in the table]*
[74] [assignment: *cryptographic key sizes*]

FCS_COP.1/VDS-RSA Cryptographic operation – Verification of digital signatures RSA

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/VDS-RSA The TSF shall perform *signature-verification* in accordance with a specified cryptographic algorithm *RSA and EMSA-PSS* and cryptographic key sizes [assignment: *2048 and 3072 bits*][75] that meet the following: *ISO/IEC 14888-2 [ISO/IEC 14888-2]*, *PKCS #1, v2.2 [PKCS#1]*.

Application note 22: The cryptographic key sizes assigned in FCS_CKM.1/RSA must be at least 2000 bits. Cryptographic key sizes of at least 3000 bits are recommended.

FDP_DAU.2/Sig Data Authentication with Identity of Guarantor - Signature

Hierarchical to: FDP_DAU.1 Basic Data Authentication

Dependencies: FIA_UID.1 Timing of identification

FDP_DAU.2.1/Sig The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of *user data* **imported according to FDP_ITC.2/UD by means of [selection: *FCS_COP.1/CDS-RSA, FCS_COP.1/CDS-ECDSA*][76] and keys holding the security attributes Key identity assigned to the guarantor and Key usage type "Signature service"**.

FDP_DAU.2.2/Sig The TSF shall provide *external entities* with the ability to verify evidence of the validity of the indicated information and the identity of the user that generated the evidence.

Application note 23: The TSF according to FDP_DAU.2/Sig is intended for a signature service for user data. The user data source shall select the security attributes *Key entity* of the guarantor and *Key usage type* "*Signature service*" of the cryptographic key for the signature service in the security attributes provided with the user data. The user data source subject shall meet the *Key access control attributes* for the signature-creation operation. The verification of the evidence requires a certificate showing the identity of the key entity as user generated the evidence and the key usage type as digital signature.

7.1.5 Authentication and attestation of the TOE, trusted channel

FIA_API.1/PACE Authentication Proof of Identity – PACE authentication to Application component

Hierarchical to: No other components.

Dependencies: No dependencies.

[75] [assignment: *cryptographic key sizes*]
[76] [selection: *FCS_COP.1/CDS-RSA, FCS_COP.1/CDS-ECDSA*]

FIA_API.1.1/PACE The TSF shall provide a *PACE in ICC role* to prove the identity of the *TOE* to an external entity **and establishing a trusted channel according to FTP_ITC.1 case 1 or 2.**

FIA_API.1/CA Authentication Proof of Identity – Chip authentication to user

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1/CA The TSF shall provide a *Chip Authentication Version 2 according to [TR-03110] section 3.4* to prove the identity of the *TOE* to an external entity **and establishing a trusted channel according to FTP_ITC.1 case 3.**

FDP_DAU.2/Att Data Authentication with Identity of Guarantor – Attestation

Hierarchical to: FDP_DAU.1 Basic Data Authentication

Dependencies: FIA_UID.1 Timing of identification

FDP_DAU.2.1/Att The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of *attestation data* **by means of *[AES-128 cryptographic authentication mechanism]*[77] and keys holding the security attributes Key identity assigned to the TOE sample and Key usage type "Attestation".**

FDP_DAU.2.2/Att The TSF shall provide *external entities* with the ability to verify evidence of the validity of the indicated information and the identity of the user that generated the evidence.

Application note 24: The attestation data shall represent the TOE sample as genuine sample of the certified product. The attestation data may include the identifier of the certified product, the serial number of the device or a group of product samples as certified product, the hash value of the TSF implementation and some TSF data as result of self-test, or other data. It may be generated internally or may include internally generated and externally provided data. The assigned cryptographic mechanisms shall be appropriate for attestation meeting OSP.SecCryM, e. g. digital signature, a group signature or a direct anonymous attestation mechanism as used for Trusted Platform Modules ***[TPMLib,Part 1]*** or FIDO U2F Authenticators ***[FIDO-ECDAA]***.

FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_ITC.1.1 The TSF shall provide a communication channel between TSF and another trusted IT product that is **[selection: *logically separated from other***

[77] *[assignment: other cryptographic authentication mechanism]*]

communication channels[78] and provides assured identification of its end points **[selection**: ***Authentication of TOE and remote entity according to the case in Table 7***]79 and protection of the channel data from modification or disclosure **[assignment: *according to the case in Table 7*]**[80] **as required by [selection: *cryptographic operation according to the case in Table 7*]**[81]**.**

FTP_ITC.1.2 *The TSF shall permit the remote trusted IT product* **determined according to FMT_MOF.1.1 clause (3)** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for *communication with entities defined according to FMT_MOF.1 clause (4)***.**

Case	Authentication of TOE and remote entity	Key agreement	Protection of communication data	Cryptographic operation
1	FIA_API.1/PACE, FIA_UAU.5.1 (2)	FCS_CKM.1/PACE	modification	FCS_COP.1/TCM
2	FIA_API.1/PACE, FIA_UAU.5.1 (2)	FCS_CKM.1/PACE	modification	FCS_COP.1/TCM
			disclosure	FCS_COP.1/TCE
3	FIA_API.1/CA, FIA_UAU.5.1 (4) or (5), and (6)	FCS_CKM.1/TCAP	modification	FCS_COP.1/TCM
			disclosure	FCS_COP.1/TCE

***Table 7*: Operation in SFR for trusted channel**

FCS_CKM.1/PACE Cryptographic key generation – Key agreement for trusted channel PACE

Hierarchical to: No other components.

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

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1/PACE The TSF shall generate cryptographic keys ***for MAC with for FCS_COP.1/TCM and if selected encryption keys for FCS_COP.1/TCE*** in accordance with a specified cryptographic key **agreement** algorithm *PACE with [selection: elliptic curves in Table 5]*[82] *and Generic Mapping in ICC role* and specified cryptographic key sizes *[selection: 128 bits, 192 bits and 256 bits]*[83] that meet the following: *ICAO Doc9303*, *Part 11, section 4.4 [ICAO Doc9303]*.

Application note 25: PACE is used to authenticate the TOE and the application component, or TOE and human user using a terminal. It establishes a trusted channel with MAC integrity protection and if selected encryption.

[78] *[selection: logically separated from other communication channels, using physical separated ports]*
[79] *[selection: Authentication of TOE and remote entity according to the case in table]*
[80] *[assignment: according to the case in table]*
[81] *[selection: cryptographic operation according to the case in table]*
[82] *[selection: elliptic curves in table]*
[83] *[selection: 128 bits, 192 bits, 256 bits]*

FCS_CKM.1/TCAP Cryptographic key generation – Key agreement by Terminal and Chip authentication protocols

Hierarchical to: No other components.

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

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1/TCAP The TSF shall generate cryptographic keys **for *encryption according to FCS_COP.1/TCE and MAC according to FCS_COP.1/TCM*** in accordance with a specified cryptographic key **agreement** algorithms *Terminal Authentication version 2 and Chip Authentication Version 2* and specified cryptographic key sizes *[selection: 128 bits, 192 bits and 256 bits]*[84] that meet the following: *BSI TR-03110 [TR-03110], section 3.3 and 3.4*.

Application note 26: The terminal authentication protocol version 2 is used for authentication of the Application component according to FIA_UAU.5 and is a prerequisite for Chip Authentication Version 2.

FCS_COP.1/TCE Cryptographic operation - Encryption for trusted channel

Hierarchical to: No other components.

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

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/TCE The TSF shall perform *encryption and decryption* in accordance with a specified cryptographic algorithm *AES in [selection: CBC[NIST-SP800-38A]*[85] *mode* and cryptographic key sizes [*selection: 128 bits, 192 bits and 256 bits]*[86] that meet the following: *[FIPS197]*.

FCS_COP.1/TCM Cryptographic operation - MAC for trusted channel

Hierarchical to: No other components.

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

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/TCM The TSF shall perform *MAC calculation and MAC verification* in accordance with a specified cryptographic algorithm *AES [selection: CMAC[NIST-SP800-38B]*[87] and cryptographic key sizes *[selection: 128 bits, 192 bits and 256 bits]*[88] that meet the following: *[FIPS197]*.

[84] *[selection: 128 bits, 192 bits, 256 bits]*
[85] *[selection: CBC[NIST-SP800-38A], CCM[NIST-SP800-38C], GCM[NIST-SP800-38D]]*
[86] [*selection: 128 bits, 192 bits, 256 bits]*
[87] *AES [selection: CMAC[NIST-SP800-38B], GMAC[NIST- SP800-38D]]*
[88] *[selection: 128 bits, 192 bits, 256 bits]*

7.1.6 User identification and authentication

FIA_ATD.1 User attribute definition – Identity based authentication

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

(1) *Identity*,

(2) *Authentication reference data,*

(3) *Role*.

FMT_MTD.1/RAD Management of TSF data – Authentication reference data

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1/RAD The TSF shall restrict the ability to

(1) *create* the *initial Authentication reference data of all authorized users* to *[selection: Administrator]*[89],

(2) *delete the Authentication reference data of an authorized user to [selection: Administrator]*[90],

(3) ***modify* the *Authentication reference data* to *the corresponding authorized user***.

(4) *create the permanently stored session key of trusted channel as Authentication reference data to [selection: Administrator]*[91]

(5) *define* the *time in range [assignment: time frame]*[92] *after which the user security attribute Role is reset according to FMT_SAE.1 to [selection: Administrator, User Administrator]*[93],

(6) *define the value [selection: Unauthenticated user]*[94] *to which the security attribute Role shall be reset according to FMT_SAE.1to [selection: Administrator]*[95].

Application note 27: The Administrator is responsible for user management. The Administrator install and revoke a user as known authorized user of the TSF as defined in clause (1). The Administrator may define additional authentication reference data as described in clause (3), i. e. the trusted channel combines initial authentication of communication endpoints (cf. FIA_UAU.5.1 clause (3) and (4)) with agreement of session

[89] *[selection: Administrator, User Administrator]*
[90] *[selection: Administrator, User Administrator]*
[91] *[selection: Administrator, User Administrator]*
[92] *[assignment: time frame]*
[93] *[selection: Administrator, User Administrator]*
[94] *[selection: Unidentified user, Unauthenticated user]*
[95] *[selection: Administrator, User Administrator]*

keys used for authentication of exchanged messages (cf. FIA_UAU.5.1 clause (5)). The session keys may be permanently stored for the trusted communication with the known authorized entity. The user manages its own authentication reference data to prevent impersonation based of known authentication data (e.g. as addressed by FMT_MTD.3).

Clause(5) is trivially met since not supported by the product.

FMT_MTD.3 Secure TSF data

Hierarchical to: No other components.

Dependencies: FMT_MTD.1 Management of TSF data

FMT_MTD.3.1 The TSF shall ensure that only secure values are accepted for *passwords* **by enforcing change of initial passwords after first successful authentication of the user to different operational password**.

FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when [selection: [assignment: *number of retries counter*], *an* ***[selection: Administrator]]***[96] *configurable positive integer within [assignment: 1-127,*][97] unsuccessful authentication attempts occur related to [assignment: Open secure channel, password/PIN authentication][98].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [selection:*met*][99], the TSF shall [assignment: return error status and authentication will fail][100].

FIA_USB.1 User-subject binding

Hierarchical to: No other components.

Dependencies: FIA_ATD.1 User attribute definition

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user:

(1) *Identity*,

(2) *Role*.

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: *the initial role of the user is Unidentified user*.

[96] [selection: [assignment: *positive integer number*], *an [selection: Administrator, User Administrator]*
[97] *[assignment: range of acceptable values]*]
[98] [assignment: *list of authentication events*]
[99] [selection:*met, surpassed*]
[100] [assignment: *list of actions*]

FIA_USB.1.3	The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: (1) *after successful identification of the user the attribute Role of the subject shall be changed from Unidentified user to Unauthenticated user;* (2) *after successful authentication of the user for a selected role the attribute Role of the subject shall be changed from Unauthenticated User to that role;* (3) *after successful re-authentication of the user for a selected role the attribute Role of the subject shall be changed to that role*.

FMT_SAE.1 Time-limited authorization

Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles FPT_STM.1 Reliable time stamps
FMT_SAE.1.1	The TSF shall restrict the capability to specify an expiration time for *Role* to *[selection: Administrator, User Administrator]*[101].
FMT_SAE.1.2	For each of these security attributes, the TSF shall be able to *reset the Role to the value assigned according to FMT_MTD.1/RAD, clause (6)* after the expiration time for the indicated security attribute has passed.

Application note 28: The TSF shall implement means to handle expiration time for the roles whithin a session (i.e. between power-up and power-down of the TOE) which may not necessarily meet the requirements for a reliable time stamp as required by FPT_STM.1. If the security target require FPT_STM.1 (e.g. if the PP-module "Time Stamp and Audit" claimed) this time stamp shall be used to meet FMT_SAE.1.

FMT_SAE.1.1 is trivially met since not supported by the product.

FIA_UID.1 Timing of identification

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UID.1.1	The TSF shall allow (1) *self test according to FPT_TST.1*, (2) *identification of the TOE to the user*, (3) *[assignment: No other TSF-mediated actions]*[75] on behalf of the user to be performed before the user is identified.
FIA_UID.1.2	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of **the Unauthenticated User**.

[101] *[selection: Administrator, User Administrator]*

FIA_UAU.1 Timing of authentication

Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification
FIA_UAU.1.1	The TSF shall allow (1) *self test according to FPT_TST.1*, (2) *authentication of the TOE to the user*, (3) *identification of the user to the TOE and selection of [selection: a role]*[102] *for authentication,* (4) *[assignment: no other TSF mediated actions]*[103] 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 29: Clause (2) and (3) in FIA_UAU.1.1 allows mutual identification for mutual authentication, eg. by exchange of certificates.

FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UAU.5.1	The TSF shall provide (1) *password authentication*, (2) *PACE with Generic Mapping with TOE in ICC and user in PCD context with establishment of trusted channel according to FTP_ITC.1,* (3) *certificate based Terminal Authentication Version 2 according to section 3.3 in [TR-03110] with the TOE in ICC and user in PCD context,* (4) *Terminal Authentication Version 2 with the TOE in ICC context and user in PCD context modified by omitting the verification of the certificate chain,* (5) *Chip Authentication Version 2 with establishment of trusted channel according to FTP_ITC.1,* (6) *message authentication by MAC verification of received messages* to support user authentication.
FIA_UAU.5.2	The TSF shall authenticate any user's claimed identity according to the **rules** (1) *password authentication shall be used for authentication of human users if enabled according to FMT_MOF.1.1, clause (1)*, (2) *PACE shall be used for authentication of human users using terminals with*

[102] *[selection: a role, a set of role]*
[103] *[assignment: list of other TSF mediated actions]*

establishment of trusted channel according to FTP_ITC.1,

(3) PACE may be used for authentication of IT entities with establishment of trusted channel according to FTP_ITC.1,

(4) certificate based Terminal Authentication Version 2 may be used for authentication of users which certificate imported as TSF data,

(5) simplified version of Terminal Authentication Version 2 may be used for authentication of identified users associated with known user's public key,

(6) *message authentication by MAC verification of received messages shall be used after initial* authentication of remote entity according to clauses (2) or (3) for trusted channel according to FTP_ITC.1,

(7) [assignment: No additional rules][104].

FIA_UAU.6 Re-authenticating Hierarchical to:

Hierarchical to: No other components.

Dependencies: No dependencies.

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

(1) changing to a role not selected for the current valid authentication session,

(2) power on or reset,

(3) every message received from entities after establishing trusted channel according to FIA_UAU.5.1, clause (2), (3) or (6),

(4) [Trusted channel termination, Trusted channel disconnection][105],

7.1.7 Access control

FDP_ITC.2/UD Import of user data with security attributes – User data

Hierarchical to: No other components.

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

[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]

FPT_TDC.1 Inter-TSF basic TSF data consistency

FDP_ITC.2.1/UD The TSF shall enforce the *Cryptographic Operation SFP* when importing user data, controlled under the SFP, from outside of the TOE.

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

FDP_ITC.2.3/UD 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/UD 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.

[104] *[assignment: additional rules]*
[105] *[assignment: list of other conditions under which re-authentication is required]*

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

(1) *user data imported for encryption according to FCS_COP.1/ED shall be imported with Key identity of the key and the identification of the requested cryptographic operation,*

(2) *user data imported for encryption according to FCS_COP.1/HEM shall be imported with Key identity of the public key encryption key or key agreement method,*

(3) *user data imported for decryption according to FCS_COP.1/HDM shall be imported with Key identity of the asymmetric decryption key, encrypted seed and data integrity check sum*,

(4) *user data imported for digital signature creation shall be imported with the Key identity of the private signature key,*

(5) *user data imported for digital signature verification shall be imported with digital signature and Key identity of the public signature key*.

Application note 30: Keys to be used for the cryptographic operation of the imported user data are identified by security attribute *Key identity*.

FDP_ETC.2 Export of user data with security attributes

Hierarchical to: No other components.

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

FDP_ETC.2.1 The TSF shall enforce the *Cryptographic Operation SFP* 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:

(1) *user data exported as ciphertext according to FCS_COP.1/HEM shall be exported with reference to key decryption key, encrypted data encryption key and data integrity check sum*,

(2) *user data exported as plaintext according to FCS_COP.1/HDM shall be exported only if the MAC verification confirmed the integrity of the ciphertext,*

(3) *user data exported as signed data according to FCS_COP.1/CDS-ECDSA or FCS_COP.1/CDS-RSA shall be exported with digital signature and Key identity of the used signature-creation key*.

Application note 31: The TOE imports data to be signed by CSP shall be imported with Key identity of the signature key and exports the signature. In case of internally generated data exported as signed data shall be exported with Key identity of the used key in order to enable identification of the corresponding signature-verification key. Note, the TOE may implement more than one signature-creation key for signing internally generated data.

FDP_ETC.1 Export of user data without security attributes

Hierarchical to: No other components.

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

FDP_ETC.1.1 The TSF shall enforce the *Cryptographic Operation SFP* when exporting user data **as plaintext according to FCS_COP.1/HDM**, controlled under the SFP(s), outside of the TOE.

FDP_ETC.1.2 The TSF shall export the **successfully MAC verified and decrypted ciphertext as plaintext according to FCS_COP.1/HDM** without the user data's associated security attributes.

FDP_ACC.1/Oper Subset access control – Cryptographic operation

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/Oper The TSF shall enforce the *Cryptographic Operation SFP* on

(1) *subjects: [selection: Administrator][106], Key Owner, [assignment: No other roles][107];*

(2) *objects: operational cryptographic keys*, *user data*;

(3) *operations: cryptographic operation*

FDP_ACF.1/Oper Security attribute based access control – Cryptographic operations

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1/Oper The TSF shall enforce the *Cryptographic Operation SFP* to objects based on the following:

(1) *subjects: subjects with security attribute Role [selection: Administrator,][108], Key Owner, [assignment: No other roles][109]*;

(2) *objects:*

(a) *cryptographic keys with security attributes: Identity of the key, Key entity, Key type, Key usage type, Key access control attributes, Key validity time period*;

(b) *user data*.

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

(1) *Subject in [selection: Administrator][110] role is allowed to perform*

[106] *[selection: Administrator, Crypto-Officer]*
[107] *[assignment: other roles]*
[108] *[selection: Administrator, Crypto-Officer]*
[109] *[assignment: other roles]*
[110] *[selection: Administrator, Crypto-Officer]*

cryptographic operation on cryptographic keys in accordance with their security attributes.

(2) *Subject Key Owner is allowed to perform cryptographic operation on user data with cryptographic keys in accordance with the security attribute Key entity, Key type, Key usage type, Key access control attributes and Key validity time period*;

(3) *[assignment: No other rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]*[111].

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

(1) *subjects with security attribute Role are allowed to perform cryptographic operation on user data and cryptographic keys with security attributes as shown in the rows of* Table 5

(2) [assignment: *No additional rules, based on security attributes, that explicitly authorize access of subjects to objects*][112].

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

(1) *No subject is allowed to use cryptographic keys by cryptographic operation other than those identified in the security attributes Key usage type and the Key access control attributes*;

(2) *No subject is allowed to decrypt ciphertext according to FCS_COP.1/HDM if MAC verification fails.*

(3) *[assignment: No additional rules, based on security attributes, that explicitly deny access of subjects to objects]* [113]

Access control rules for cryptographic operation:

Security attribute Role of the subject	Security attribute of the cryptographic key	Cryptographic operation referenced by SFR allowed for the subject on user data with the cryptographic key
[selection: Administrator]	*Key type: symmetric Key usage type: Key wrap Key validity time period:*	*FCS_COP.1/KW*
[selection: Administrator]	*Key type: symmetric Key usage type: Key unwrap Key validity time period:*	*FCS_COP.1/KU*

[111] *[assignment: other rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]*
[112] [assignment: *additional rules, based on security attributes, that explicitly authorize access of subjects to objects*]
[113] *[assignment: additional rules, based on security attributes, that explicitly deny access of subjects to objects]*

(any authenticated user)	*Key type: public* *Key usage type: ECKA-EG Key* *validity time period: as in certificate*	*FCS_COP.1/HEM,* *FCS_CKM.1/ECKA-EG*
Key Owner	*Key type: private* *Key usage type: ECKA-EG Key* *validity time period:*	*FCS_COP.1/HDM* *FCS_CKM.5/ECKA-EG*
(any authenticated user)	*Key type: public* *Key usage type: RSA_ENC Key* *validity time period: as in certificate*	*FCS_COP.1/HEM* *FCS_CKM.1/AES_RSA*
Key Owner	*Key type: private* *Key usage type: RSA_ENC Key* *validity time period: as in certificate*	*FCS_COP.1/HDM* *FCS_CKM.5/AES_RSA*
Key Owner	*Key type: private* *Key usage type: DS-ECDSA Key* *validity time period:*	*FCS_COP.1/CDS-ECDSA*
(any authenticated user)	*Key type: public* *Key usage type: DS-ECDSA Key* *validity time period:*	*FCS_COP.1/VDS-ECDSA*
Key Owner	*Key type: private* *Key usage type: DS-RSA Key* *validity time period:*	*FCS_COP.1/CDS-RSA*
(any authenticated user)	*Key type: public* *Key usage type: DS-RSA Key* *validity time period:*	*FCS_COP.1/VDS-RSA*

***Table 8*: Security attributes and access control**

7.1.8 Security Management

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

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

(1) *management of security functions behaviour (FMT_MOF.1)*,

(2) *management of Authentication reference data (FMT_MTD.1/RAD),*

(3) *management of security attributes of cryptographic keys (FMT_MSA.1/KM, FMT_MSA.2, FMT_MSA.3/KM,*

(4) *[assignment: No additional list of security management functions to be provided by the TSF]*[114].

[114] *[assignment: additional list of security management functions to be provided by the TSF]*

FMT_SMR.1 Security roles

Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification
FMT_SMR.1.1	The TSF shall maintain the roles: *Unidentified User, Unauthenticated User, Key Owner, Application component, [selection: Administrator][115] [selection: no other roles]*[116].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

Application note 32: The ST may select the general role *Administrator* or more detailed administrator roles as supported by the TOE.

FMT_MSA.2 Secure security attributes

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
	FMT_MSA.1 Management of security attributes
	FMT_SMR.1 Security roles
FMT_MSA.2.1	The TSF shall ensure that only secure values are accepted for *security attributes*
	(1) *Key identity,*
	(2) *Key type,*
	(3) *Key usage type,*
	(4) *[assignment: Access control rules - which user is allowed to conduct which key operation]*[117].
	The cryptographic keys shall have
	(1) **Key identity uniquely identifying the key among all keys implemented in the TOE,**
	(2) **exactly one Key type as secret key, private key, public key,**
	(3) **exactly one Key usage type identifying exactly one cryptographic mechanism the key can be used for.**

FMT_MOF.1 Management of security functions behaviour

Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles
	FMT_SMF.1 Specification of Management Functions
FMT_MOF.1.1	The TSF shall restrict the ability to
	(1) *Enable* the functions *password authentication according to FIA_UAU.5.1, clause (1)* to *[selection: Administrator]*[118].

[115] *[selection: Administrator, Crypto-Officer, User Administrator, Update Agent]*
[116] *[selection: [assignment: other roles], no other roles]*
[117] *[assignment: additional security attributes]*
[118] *[selection: Administrator, User Administrator]*

(2) ***disable*** **the functions** ~~**s**~~ ***password authentication according to FIA_UAU.5.1, clause (1)*** **to** ***[selection: Administrator]***[119]**,**

(3) ***determine the behaviour of*** **the functions** ***trusted channel according to FDP_ITC.1.2*** **by defining the remote trusted IT products permitted to initiate communication via the trusted channel to** ***[selection: Administrator]***[120]**,**

(4) ***determine the behaviour of*** **the functions** ***trusted channel according to FDP_ITC.1.3*** **by defining the entities for which the TSF shall enforce communication via the trusted channel to** ***[selection: Administrator]***[121]**.**

Application note 33: The refinements of FMT_MOF.1.1 in bullets (2) to (4) are made in order to avoid iteration of the component. In case of client-server architecture the applications using the TOE and supporting cryptographically protected trusted channel belong to the entities for which the TSF shall enforce trusted channel according to FDP_ITC.1, cf. FMT_MOF.1.1 in bullet (4).

7.1.9 Protection of the TSF

FDP_SDC.1	Stored data confidentiality
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FDP_SDC.1.1	The TSF shall ensure the confidentiality of the information of the ~~user~~ data while it is stored in the [assignment: NVM – persistent memory, RAM][122] **by encryption according to *FCS_COP.1/SDE.***

Application note 34: The memory encryption does not distinguish between user data and TSF data when encrypting memory areas. The refinement extends the SFR to any data in the assigned memory area, which may contain user data, TSF data, software and firmware as TSF implementation.

FCS_CKM.1/SDEK	Cryptographic key generation – Stored data encryption key generation
Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1.1/SDEK	The TSF shall generate cryptographic **stored data encryption** keys in accordance with a specified cryptographic key generation algorithm [*assignment: cryptographic key generation algorithm*][123] **using random bit generation according to FCS_RNG.1** and specified cryptographic key sizes *[assignment: cryptographic key sizes]*[124] that meet the following: *[assignment: list of standards]*[125].

[119] *[selection: Administrator, User Administrator]*
[120] *[selection: Administrator, User Administrator]*
[121] *[selection: Administrator, User Administrator]*
[122] [assignment: *memory area*]
[123] [assignment: c*ryptographic key generation algorithm*]
[124] *[assignment: cryptographic key sizes]*
[125] *[assignment: list of standards]*

cryptographic key generation algorithm	*cryptographic key sizes*	*list of standards*
AES	128, 192, 256	[PKCS #1]
RSA	up to 3072	[FIPS197]
ECC	256, 384, 512	[NIST-SP800-38A] [RFC6954] [NIST FIPS 186-3]
ANSI X9.63	160, 192, 224, 256, 320, 384, 512, 521	[TR-03111]

FCS_COP.1/SDE Cryptographic operation – Stored data encryption

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/SDE The TSF shall perform *stored data encryption and decryption* in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*][126] and cryptographic key sizes [assignment: *cryptographic key sizes*][127] that meet the following: [assignment: *list of standards*][128].

cryptographic algorithm	*cryptographic key sizes*	*list of standards*
AES	128, 192, 256	[PKCS#1]
RSA	up to 3072	[FIPS197]
ECC	256, 384, 512	[NIST-SP800-38A] [RFC6954] [NIST FIPS 186-3]
ANSI X9.63	160, 192, 224, 256, 320, 384, 512, 521	[TR-03111]

Application note 35: The generation of data encryption keys according to FCS_CKM.1/SDEK, the encryption and the decryption according to FCS_COP.1/SDE are only used for stored data in the memory areas assigned in FDP_SDC.1.1. They are not a security services of the TOE to the user. If cryptographic algorithm does not provide integrity protection for stored user data the stored data should contain redundancy for detection of data manipulation, e. g. in order to meet FPT_TST.1.2 and FPT_TST.1.3.

FRU_FLT.2 Limited fault tolerance

Hierarchical to: FRU_FLT.1 Degraded fault tolerance

[126] [assignment: *cryptographic algorithm*]
[127] [assignment: *cryptographic key sizes*]
[128] [assignment: *list of standards*]

Dependencies: FPT_FLS.1 Failure with preservation of secure state.

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

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

Application note 36: Environmental conditions include but are not limited to power supply, clock, and other external signals (e. g. reset signal) necessary for the TOE operation.

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

Dependencies: No dependencies.

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

(1) *self test fails*,
(2) *exposure to operating conditions which may not be tolerated according to the requirement Limited fault tolerance (FRU_FLT.2) and where therefore a malfunction could occur,*
(3) *manipulation and physical probing is detected and secure state is reached as response (FPT_PHP.3)*.

Refinement**: When the TOE is in a secure error mode the TSF shall not perform any cryptographic operations and all data output interfaces shall be inhibited by the TSF.**

FPT_TST.1 TSF testing

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TST.1.1 The TSF shall run a suite of self tests *during initial start-up, at the request of the authorized user and after power-on* to demonstrate the correct operation of [assignment:

- NVM checksum check
- Writing & reading in RAM
- Writing & reading NVM page
- Encryption engine verification
- Chip serial number identification]129.

FPT_TST.1.2 The TSF shall provide authorized users with the capability to verify the integrity of *TSF data*.

FPT_TST.1.3 The TSF shall provide authorized users with the capability to verify the integrity of *TSF **implementation***.

129 [assignment: *parts of TSF]*

FPT_PHP.3 Resistance to physical attack

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_PHP.3.1 The TSF shall resist

(1) *physical probing and manipulation and (2) perturbation and environmental stress* to the *(1) TSF implementation and (2) the TSF* by responding automatically such that the SFRs are always enforced.

Refinement: The TSF will implement appropriate mechanisms to continuously counter physical probing and manipulation. In case of platform architecture the resistance to physical attacks shall include the secure execution environment for and the communication with the application component running on the TOE.

Application note 37: "Automatic response" of protection against physical probing and manipulation means (i) assuming that there might be an attack at any time and (ii) countermeasures are provided at any time. Perturbation and environmental stress to the TSF is relevant when the TOE is running. Note, exploration of information leakage from the TOE like side channels is addressed as bypassability of TSF by the security architecture (cf. ADV_ARC.1.1D and ADV_ARC.1.5C) and shall consider these physical attack scenarios.

7.1.10 Import and verification of Update Code Package

The TOE imports Update Code Package as user data objects with security attributes according to FDP_ITC.2/UCP, verifies the authenticity of the received Update Code Package according to FCS_COP.1/VDSUCP, decrypts authentic Update Code Package according to FCS_COP.1/DecUCP.

FDP_ITC.2/UCP Import of user data with security attributes – Update Code Package

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

[FTP_ITC.1 Inter-TSF trusted channel, or

FTP_TRP.1 Trusted path]

FPT_TDC.1 Inter-TSF basic TSF data consistency

FDP_ITC.2.1/UCP The TSF shall enforce the *Update SFP* when importing user data, controlled under the SFP, from outside of the TOE.

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

FDP_ITC.2.3/UCP 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/UCP 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/UCP The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE:

(1) *storing of encrypted Update Code Package only after successful verification of authenticity according to FCS_COP.1/VDSUCP,*

(2) *decrypts authentic Update Code Package according to FCS_COP.1/DecUCP*.

FPT_TDC.1/UCP Inter-TSF basic TSF data consistency

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TDC.1.1/UCP The TSF shall provide the capability to consistently interpret *security attributes Issuer and Version Number* when shared between the TSF and another trusted IT product.

FPT_TDC.1.2/UCP The TSF shall use **the following rules**:

(1) *the Issuer must be identified and known,*

(2) *the Version Number must be identified*

when interpreting the TSF data from another trusted IT product.

FCS_COP.1/VDSUCP Cryptographic operation – Verification of digital signature of the Issuer

Hierarchical to: No other components.

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

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/VDSUCP The TSF shall perform *verification of the digital signature of the authorized Issuer* in accordance with a specified cryptographic algorithm [assignment: *DES-128*][130] and cryptographic key sizes [assignment: *128 bits*][131] that meet the following: [assignment: ISO/IEC 9797-1 MAC Method 2 Algo 3][132].

Application note 38: The authorized *Issuer* is identified in the security attribute of the received Update Code Package and the public key of the authorized *Issuer* shall be known as TSF data before receiving the Update Code Package. Only public key of the authorized Issuer shall be used for verification of the digital signature of the Update Code Package.

FCS_COP.1/DecUCP Cryptographic operation – Decryption of authentic Update Code Package

Hierarchical to: No other components.

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

FDP_ITC.2 Import of user data with security attributes, or

[130] [assignment: *cryptographic algorithm*]
[131] [assignment: *cryptographic key sizes*]
[132] [assignment: *list of standards*]

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/DecUCP The TSF shall perform *decryption of authentic encrypted Update Code Package* in accordance with a specified cryptographic algorithm [assignment: *DES-128*][133] and cryptographic key sizes [assignment: *128 bits*][134] that meet the following: [assignment: ISO/IEC 9797 M2 padding, FIPS 197 (AES), FIPS 46 (DES)][135].

FDP_ACC.1/UCP Subset access control – Update code Package

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/UCP The TSF shall enforce the *Update SFP* on

(1) *subjects: [selection: Administrator and Update Agent][136];*

(2) *objects: Update Code Package*;

(3) *operations: import, store.*

FDP_ACF.1/UCP Security attribute based access control – Import Update Code Package

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1/UCP The TSF shall enforce the *Update SFP* to objects based on the following:

(1) *subjects: [selection: Administrator or Update Agent][137];*

(2) *objects: Update Code Package with security attributes Issuer and Version Number*.

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

(1) *[selection: Update Agent][111] is allowed to import Update Code Package according to FDP_ITC.2/UCP.*

(2) *[selection: Update Agent][138] is allowed to store Update Code Package if*

(a) *authenticity is successful verified according to FCS_COP.1/VDSUCP and decrypted according to FCS_COP.1/DecUCP*

(b) *the Version Number of the Update Code Package is equal or higher than*

[133] [assignment: *cryptographic algorithm*]
[134] [assignment: *cryptographic key sizes*]
[135] [assignment: *list of standards*]
[136] *[selection: Administrator, Update Agent]*
[137] *[selection: Administrator, Update Agent]*
[138] *[selection: Administrator, Update Agent]*

the Version Number of the TSF.

FDP_ACF.1.3/UCP The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [assignment: *User Agent authenticated*][139].

FDP_ACF.1.4/UCP The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: *User Agent authenticated*][140].][141].

FDP_RIP.1/UCP Subset residual information protection

Hierarchical to: No other components

Dependencies: No dependencies.

FDP_RIP.1.1/UCP The TSF shall ensure that any previous information content of a resource is made unavailable upon the *deallocation of the resource* ***after unsuccessful verification of the digital signature of the Issuer according to FCS_COP.1/VDSUCP*** the following objects: *received Update Code Package*.

7.2 SECURITY ASSURANCE REQUIREMENTS

The security assurance requirement level is EAL4 augmented with AVA_VAN.5 and ALC_DVS.2.

7.3 SECURITY REQUIREMENTS RATIONALE

7.3.1 Dependency rationale

This chapter demonstrates that each dependency of the security requirements is either satisfied, or justifies the dependency not being satisfied.

Note, the column SFR components showing the concrete SFR satisfying the dependencies are typical use cases. It does not exclude that the SFR in the first column may solve dependencies of other SFR as well. E. g. the SFR FCS_CKM.1 defines requirements for ECC key generation and the ECC key pair may be directly used for ECDSA digital signatures according to FCS_COP.1/CDS-RSA and FCS_COP.1/VDS-RSA but also for encryption and decryption of the AES key in FCS_COP.1/HEM and FCS_COP.1/HDM.

[139] [assignment: *rules, based on security attributes, that explicitly authorize access of subjects to objects*]
[140] [assignment: *rules, based on security attributes, that explicitly authorize access of subjects to objects*]
[141] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]

SFR	Dependencies of the SFR	SFR components
FCS_CKM.1/AES	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1/ED FCS_CKM.4
FCS_CKM.1/AES_RSA	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1/HEM with FCS_CKM.1/AES_RSA, FCS_CKM.4
FCS_CKM.1/ECC	FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1/CDS-ECDS, FCS_COP.1/VDS-ECDS, FCS_CKM.4
FCS_CKM.1/ECKA-EG	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1/HEM with FCS_CKM.1/ECKA-EG, FCS_CKM.4
FCS_CKM.1/PACE	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1/TCE, FCS_COP.1/TCM, FCS_CKM.4
FCS_CKM.1/RSA	FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1/CDS-RSA, FCS_COP.1/VDS-RSA FCS_CKM.4
FCS_CKM.1/SDEK	FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1/SDE, FCS_CKM.4
FCS_CKM.1/TCAP	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1/TCE, FCS_COP.1/TCM, FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]	FCS_CKM.1/ECC, FCS_CKM.1/RSA, FCS_CKM.1/ECKA-EG, FCS_CKM.1/AES_RSA, FCS_CKM.1/TCAP, FCS_CKM.1/PACE
FCS_CKM.5/AES	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1/ED FCS_CKM.4
FCS_CKM.5/AES_RSA	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key	FCS_COP.1/HDM with FCS_CKM.5/AES_RSA, FCS_CKM.4

SFR	Dependencies of the SFR	SFR components
	destruction	
FCS_CKM.5/ECC	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1/CDS-ECDS, FCS_COP.1/VDS-ECDS, FCS_CKM.4
FCS_CKM.5/ECDHE	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1/HEM with FCS_CKM.5/ECDHE, FCS_CKM.4
FCS_CKM.5/ECKA-EG	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1/HDM with FCS_CKM.5/ECKA-EG, FCS_CKM.4
FCS_COP.1/CDS-ECDSA	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1/ECC, FCS_CKM.4
FCS_COP.1/CDS-RSA	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1/RSA, FCS_CKM.4
FCS_COP.1/DecUCP	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	Import of UCP decryption key as TSF data with confidentiality protection FPT_TCT.1/CK and FCS_COP.1/KU, FCS_CKM.4
FCS_COP.1/ED	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1/AES, FCS_CKM.4
FCS_COP.1/Hash	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	Hash functions do not use keys

SFR	Dependencies of the SFR	SFR components
FCS_COP.1/HDM	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.5/ECKA-EG, FCS_CKM.5/AES_RSA, FCS_CKM.5/ECDHE (note deterministic FCS_CKM.5 play the role of randomized FCS_CKM.1) FCS_CKM.4
FCS_COP.1/HEM	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1/ECKA-EG, FCS_CKM.1/AES_RSA, FCS_CKM.5/ECDHE, FCS_CKM.1/AES_RSA FCS_CKM.4
FCS_COP.1/HMAC	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_RNG.1 generates random strings as HMAC keys FCS_CKM.4
FCS_COP.1/KU	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1/AES FCS_CKM.4
FCS_COP.1/KW	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes,, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1/AES FCS_CKM.4
FCS_COP.1/MAC	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction MT_MSA.2 Secure security attributes	FCS_CKM.1/AES, FCS_CKM.4
FCS_COP.1/SDE	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1/SDEK, FCS_CKM.4

SFR	Dependencies of the SFR	SFR components
FCS_COP.1/TCE	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1/TCAP, FCS_CKM.1/PACE, FCS_CKM.4
FCS_COP.1/TCM	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1/TCAP, FCS_CKM.1/PACE, FCS_CKM.4
FCS_COP.1/VDS-ECDSA	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FPT_ISA.1/Cert (note keys are TSF data), FCS_CKM.4
FCS_COP.1/VDS-RSA	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FPT_ISA.1/Cert (note keys are TSF data), FCS_CKM.4
FCS_COP.1/VDSUCP	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	Import of signature verification key of UCP Issuer as TSF data FPT_ISA.1/Cert, FPT_TIT.1/Cert, FCS_CKM.4
FCS_RNG.1	No dependencies	
FDP_ACC.1/KM	FDP_ACF.1 Security attribute based access control	Dependency on FDP_ACF.1 is not fulfilled. Access control to key management functions are specified by FMT_MTD.1/KM because cryptographic keys are TSF data.
FDP_ACC.1/Oper	FDP_ACF.1 Security attribute based access control	FDP_ACF.1/Oper
FDP_ACC.1/UCP	FDP_ACF.1 Security attribute based access control	FDP_ACF.1/UCP
FDP_ACF.1/Oper	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation	FDP_ACC.1/Oper, FMT_MSA.3/KM

SFR	Dependencies of the SFR	SFR components
FDP_ACF.1/UCP	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation	FDP_ACC.1/UCP, FMT_MSA.3 is not included, because the security attributes of UCP are imported according to FDP_ITC.2/UCP without default values.
FDP_DAU.2/Att	FIA_UID.1 Timing of identification	FIA_UID.1
FDP_DAU.2/Sig	FIA_UID.1 Timing of identification	FIA_UID.1
FDP_ETC.1	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	FDP_ACC.1/Oper
FDP_ETC.2	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	FDP_ACC.1/Oper
FDP_ITC.2/UCP	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] FPT_TDC.1 Inter-TSF basic TSF data consistency	FDP_ACC.1/UCP trusted communication is provided by FCS_COP.1/VDSUCP and FCS_COP.1/DecUCP, FPT_TDC.1/UCP
FDP_ITC.2/UD	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] FPT_TDC.1 Inter-TSF basic TSF data consistency	FDP_ACC.1/Oper trusted communication is provided by FCS_COP.1/HDM and FCS_COP.1/VDS-*, FPT_TDC.1/CK because import of user data is intended for cryptographic operation with key
FDP_RIP.1/UCP	No dependencies	
FDP_SDC.1	No dependencies	
FIA_AFL.1	FIA_UAU.1 Timing of authentication	FIA_UAU.1
FIA_API.1/CA	No dependencies	
FIA_API.1/PACE	No dependencies	
FIA_ATD.1	No dependencies	
FIA_UAU.1	FIA_UID.1 Timing of identification	FIA_UID.1
FIA_UAU.5	No dependencies	
FIA_UAU.6	No dependencies	
FIA_UID.1	No dependencies	
FIA_USB.1	FIA_ATD.1 User attribute definition	FIA_ATD.1
FMT_MOF.1	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMF.1, FMT_SMR.1

SFR	Dependencies of the SFR	SFR components
FMT_MSA.1/KM	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FDP_ACC.1/KM, FDP_ACC.1/Oper, FMT_SMF.1, FMT_SMR.1
FMT_MSA.2	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FDP_ACC.1/KM, FDP_ACC.1/Oper, FMT_MSA.1/KM, FMT_SMR.1
FMT_MSA.3/KM	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA.1/KM, FMT_SMR.1
FMT_MTD.1/KM	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1/RAD	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1/RK	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMF.1, FMT_SMR.1
FMT_MTD.3	FMT_MTD.1 Management of TSF data	FMT_MTD.1/RAD
FMT_SAE.1	FMT_SMR.1 Security roles, FPT_STM.1 Reliable time stamps	FMT_SMR.1, dependency on FPT_STM.1 is not fulfilled, cf. to the application note to FMT_STM.1
FMT_SMF.1	No dependencies	
FMT_SMR.1	FIA_UID.1 Timing of identification	FIA_UID.1
FPT_ESA.1/CK	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FMT_MTD.1 Management of TSF data or FMT_MTD.3 Secure TSF data] [FMT_MSA.1 Management of security attributes, or FMT_MSA.4 Security attribute value inheritance] FPT_TDC.1 Inter-TSF basic TSF data consistency	FDP_ACC.1/KM, FMT_MTD.1/KM FMT_MSA.1/KM FPT_TDC.1/CK
FPT_FLS.1	No dependencies	

SFR	Dependencies of the SFR	SFR components
FPT_ISA.1/Cert	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FMT_MTD.1 Management of TSF data or FMT_MTD.3 Secure TSF data] [FMT_MSA.1 Management of security attributes, or FMT_MSA.4 Security attribute value inheritance] FPT_TDC.1 Inter-TSF basic TSF data consistency	FDP_ACC.1/KM, FMT_MTD.1/RK, FMT_MSA.1/KM FPT_TDC.1/Cert
FPT_ISA.1/CK	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FMT_MTD.1 Management of TSF data or FMT_MTD.3 Secure TSF data] [FMT_MSA.1 Management of security attributes, or FMT_MSA.4 Security attribute value inheritance] FPT_TDC.1 Inter-TSF basic TSF data consistency	FDP_ACC.1/KM, FMT_MTD.1/RK, FMT_MTD.1/KM FMT_MSA.1/KM FPT_TDC.1/Cert
FPT_PHP.3	No dependencies	
FPT_TCT.1/CK	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FMT_MTD.1 Management of TSF data or FMT_MTD.3 Secure TSF data]	FDP_ACC.1/KM, FMT_MTD.1/RK, FMT_MTD.1/KM
FPT_TDC.1/Cert	No dependencies	
FPT_TDC.1/CK	No dependencies	
FPT_TDC.1/UCP	No dependencies	
FPT_TIT.1/Cert	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FMT_MTD.1 Management of TSF data or FMT_MTD.3 Secure TSF data]	FDP_ACC.1/KM, FMT_MTD.1/RK
FPT_TIT.1/CK	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FMT_MTD.1 Management of TSF data or FMT_MTD.3 Secure TSF data]	FDP_ACC.1/KM, FMT_MTD.1/KM
FPT_TST.1	No dependencies	
FRU_FLT.2	FPT_FLS.1 Failure with preservation of secure state	FPT_FLS.1
FTP_ITC.1	No dependencies	

***Table 9*: Dependency rationale**

7.3.2 Security functional requirements rationale

The table below trace each SFR back to the security objectives for the TOE.

	O.I&A	O.AuthentTOE	O.Enc	O.DataAuth	O.RBGS	O.Tchann	O.AccCtrl	O.SecMan	O.PhysProt	O.TST	O.SecUpCP
FCS_CKM.1/AES			x	x				x			
FCS_CKM.1/AES_RSA			x	x				x			
FCS_CKM.1/ECC		x	x	x				x			
FCS_CKM.1/ECKA-EG			x	x				x			
FCS_CKM.1/PACE		x				x		x			
FCS_CKM.1/RSA		x	x	x				x			
FCS_CKM.1/SDEK									x		
FCS_CKM.1/TCAP		x				x		x			
FCS_CKM.4			x	x				x			
FCS_CKM.5/AES			x	x				x			
FCS_CKM.5/AES_RSA			x	x				x			
FCS_CKM.5/ECC			x	x				x			
FCS_CKM.5/ECDHE			x	x				x			
FCS_CKM.5/ECKA-EG			x	x				x			
FCS_COP.1/CDS-ECDSA		x		x							
FCS_COP.1/CDS-RSA		x		x							
FCS_COP.1/DecUCP											x
FCS_COP.1/ED			x					x			
FCS_COP.1/Hash				x				x			
FCS_COP.1/HDM			x	x							
FCS_COP.1/HEM			x	x							
FCS_COP.1/HMAC		x		x							
FCS_COP.1/KU								x			
FCS_COP.1/KW								x			
FCS_COP.1/MAC				x							
FCS_COP.1/SDE									x		
FCS_COP.1/TCE						x					
FCS_COP.1/TCM						x					
FCS_COP.1/VDS-ECDSA				x							
FCS_COP.1/VDS-RSA				x							
FCS_COP.1/VDSUCP											x

	O.I&A	O.AuthentTOE	O.Enc	O.DataAuth	O.RBGS	O.Tchann	O.AccCtrl	O.SecMan	O.PhysProt	O.TST	O.SecUpCP
FCS_RNG.1					x			x			
FDP_ACC.1/KM							x	x			
FDP_ACC.1/Oper							x				
FDP_ACC.1/UCP											x
FDP_ACF.1/Oper							x				
FDP_ACF.1/UCP											x
FDP_DAU.2/Att		x									
FDP_DAU.2/Sig				x							
FDP_ETC.1				x							
FDP_ETC.2			x	x							
FDP_ITC.2/UCP											x
FDP_ITC.2/UD			x	x							
FDP_RIP.1/UCP											x
FDP_SDC.1									x		
FIA_AFL.1	x										
FIA_API.1/CA	x	x				x					
FIA_API.1/PACE	x	x				x					
FIA_ATD.1	x						x	x			
FIA_UAU.1	x										
FIA_UAU.5	x					x					
FIA_UAU.6	x										
FIA_UID.1	x										
FIA_USB.1	x										
FMT_MOF.1	x					x					
FMT_MSA.1/KM			x	x		x	x	x			
FMT_MSA.2							x	x			
FMT_MSA.3/KM							x	x			x
FMT_MTD.1/KM								x			
FMT_MTD.1/RAD	x										
FMT_MTD.1/RK	x		x	x				x			
FMT_MTD.3	x										
FMT_SAE.1	x										
FMT_SMF.1								x			

	O.I&A	O.AuthentTOE	O.Enc	O.DataAuth	O.RBGS	O.Tchann	O.AccCtrl	O.SecMan	O.PhysProt	O.TST	O.SecUpCP
FMT_SMR.1	x							x			
FPT_ESA.1/CK								x			
FPT_FLS.1									x	x	
FPT_ISA.1/Cert	x			x				x			x
FPT_ISA.1/CK								x			
FPT_PHP.3									x		
FPT_TCT.1/CK								x			x
FPT_TDC.1/CK			x	x				x			
FPT_TDC.1/Cert	x		x	x				x			
FPT_TDC.1/UCP											x
FPT_TIT.1/Cert	x			x				x			x
FPT_TIT.1/CK								x			
FPT_TST.1										x	
FRU_FLT.2									x		
FTP_ITC.1						x					

***Table 10*: Security functional requirement rationale**

The following part of the chapter demonstrate that the SFRs meet all security objectives for the TOE.

The security objective for the TOE O.I&A “Identification and authentication of users” is met by the following SFR:

- The SFR FIA_ATD.1 lists the security attributes *Identity*, *Authentication reference data* and *Role* belonging to individual users and the SFR FMT_SMR.1 defines the security roles maintained by TSF.
- The SFR FIA_USB.1 requires the TSF to associate the user security attributes *Identity* and *Role* with subjects acting on the behalf of that user.
- The SFR FIA_UID.1 defines the TSF-mediated actions allowed on behalf of Unidentified User.
- The SFR FIA_UAU.1 defines the TSF-mediated actions allowed on behalf of Unauthenticated User.
- The SFR FIA_UAU.5 requires the TSF lists the authentication mechanisms and the rules for their application.
- The SFR FIA_API.1/CA and FIA_API.1/PACE require the TSF to authenticate external entities using Chip Authentication and PACE to communication endpoints of trusted channels.
- The SFR FIA_UAU.6 requires the TSF to request re-authentication of users under the listed conditions.
- The SFR FMT_MOF.1 requires the TSF to enable and disable of human user authentication.
- The SFR FMT_MTD.1/RAD and The SFR FMT_MTD.1/RK defines the management function of and the access limitation to authentication mechanisms and their TSF data including the root

public keys.

- The SFR FMT_MTD.3 enforce secure values for password mechanisms.
- The SFR FMT_SAE.1 requires the TSF to limit the validity of user authentication and reset the security attribute Role to a values defined by an administrator according to FMT_MTD.1/RAD.
- The SFR FIA_AFL.1 requires the TSF to detect and react on failed authentication attempts.
- The SFR FPT_ISA.1/Cert and FPT_TIT.1/Cert require the TSF to import certificates integrity protected and with their security attributes including those for entity authentication.
- The SFR FPT_TDC.1/Cert requires the TSF to interpret the certificates correctly.

The security objective for the TOE O.AuthentTOE "Authentication of the TOE to external entities" is met by the following SFR:

- The SFR FCS_CKM.1/ECC, FCS_CKM.1/RSA require the TSF to generate TOE authentication keys and SFR FCS_CKM.1/PACE and FCS_CKM.1/TCAP require the TSF to agree keys for authentication of the TOE to external entities.
- The SFR FCS_COP.1/CDS-ECDSA and FCS_COP.1/CDS-RSA require the TSF to generate digital signatures for authentication of the TOE to external entities.
- SFR FCS_COP.1/HMAC requires the TSF to generate HMAC for authentication of the TOE to external entities.
- The SFR FIA_API.1/CA, and FIA_API.1/PACE require the TSF to authenticate themselves using Chip Authentication, and PACE to communication endpoints of trusted channels.
- The SFR FDP_DAU.2/Att requires the TSF to generate evidence that can be used as a guarantee of the validity of attestation data to external entities.

The security objective for the TOE O.Enc "Confidentiality of user data by means of encryption and decryption" is met by the following SFR:

- The SFR FCS_CKM.1/ECC and FCS_CKM.1/RSA require (long term) key generation for the encryption and decryption security service of the TSF.
- The SFR FCS_CKM.1/AES, FCS_CKM.1/AES_RSA, FCS_CKM.5/ECDHE, and FCS_CKM.1/ECKA-EG, require key generation and FCS_CKM.5/AES, FCS_CKM.5/AES_RSA, FCS_CKM.5/ECKA-EG and FCS_CKM.5/ECC require key derivation for encryption and decryption security service of the TSF. Note the keys must be generated or agreed with the appropriate key type for encryption respectively for decryption or in case of symmetric cryptographic mechanisms for both according to FMT_MSA.1/KM.
- The FCS_COP.1/ED requires encryption and decryption as cryptographic operations for the encryption and decryption security service of the TSF.
- The FCS_COP.1/HDM requires hybrid decryption and the SFR FCS_COP.1/HEM requires hybrid encryption and decryption as cryptographic operations for the encryption and decryption security service of the TSF.
- The SFR FDP_ETC.2 require the TSF to export encrypted user data with reference to the key and data integrity checksums for decryption and FDP_ITC.2/UD require import of encrypted user data with reference to decryption key and data integrity checksums for decryption.
- The SFR FCS_CKM.4 requires the TSF to implement secure key destruction.
- The SFR FMT_MTD.1/RK requires the TSF management of root keys for key hierarchy known to the TSF if used for encryption.

- The SFR FPT_TDC.1/Cert requires the TSF to interpret consistently the security attributes of certificates (including those used for encryption and decryption).
- The SFR FPT_TDC.1/CK requires the TSF to interpret consistently the security attributes of keys (including those used for encryption and decryption).

The security objective for the TOE O.DataAuth "Data authentication by cryptographic mechanisms" is met by the following SFR:

- The SFR FCS_CKM.1/ECC and FCS_CKM.1/RSA require (long term) key generation for the signature security service of the TSF. The SFR FCS_CKM.1/AES, FCS_CKM.1/ECKA-EG, FCS_CKM.1/AES_RSA require key generation and FCS_CKM.5/AES_RSA, FCS_CKM.5/ECDHE, FCS_CKM.5/ECC, FCS_CKM.5/ECKA-EG key derivation for MAC generation and verification. Note the keys must be generated or agreed with the appropriate key type for signature-creation, signature-verification or, in case of symmetric cryptographic mechanisms for data authentication according to FMT_MSA.1/KM.
- The SFR FDP_ETC.2 require the TSF to export signed data with and signature and public key reference for signature verification and FDP_ITC.2/UD import of signed data with signature and public key reference for signature verification. The SFR FDP_ETC.1 require the TSF to export successfully MAC verified and decrypted ciphertext as plaintext according to FCS_COP.1/HDM without the user data's associated security attributes:
- The SFR FCS_COP.1/Hash requires the TSF to implement cryptographic primitive hash function used for HMAC, cf. FCS_COP.1/HMAC, digital signature creation, cf. FCS_COP.1/CDS-*and digital signature verification, cf. FCS_COP.1/VDS-*.
- The FCS_COP.1/CDS-ECDSA and FCS_COP.1/CDS-RSA require asymmetric cryptographic mechanisms for signature-creation.
- The SFR FCS_COP.1/VDS-ECDSA and FCS_VDS/RSA require asymmetric cryptographic mechanisms for signature-verification.
- The SFR for keyed hash FCS_COP.1/HMAC and block cipher based MAC FCS_COP.1/MAC require the TSF to provide symmetric data integrity mechanisms.
- The SFR FCS_COP.1/HEM requires hybrid MAC calculation and FCS_COP.1/HDM requires hybrid MAC verification for the ciphertext as security service of the TSF.
- The SFR FPT_ISA.1/Cert requires import of certificates with security attributes and integrity protection according to FPT_TIT.1/Cert.
- The SFR FCS_CKM.4 requires the TSF to implement secure key destruction.
- The SFR FPT_TDC.1/Cert requires the TSF to interpret consistently the security attributes in certificates (including those used for data authentication).
- The SFR FPT_TDC.1/CK requires the TSF to interpret consistently the security attributes keys (including those used for data authentication).

The security objective for the TOE O.RBGS "Random bit generation service" is met directly by the SFR FCS_RNG.1 as providing random bits for the service to the user.

The security objective for the TOE O.TChann "Trusted channel" is met by the following SFR:

- The SFR FTP_ITC.1 requires different types of trusted channel depending on the capability of the other endpoint. The cases are defined in Table 4. The remote entity and the TOE may use mutual authentication and key agreement by means of PACE according to FCS_CKM.1/PACE, shall provide integrity protection according to FCS_COP.1/TCM and may support confidentiality of the communication data according to FCS_COP.1/TCE. The cases 3 requires support of

trusted channel with mutual authentication by FIA_API.1/CA, FIA_UAU.5, key agreement TCAP according to FCS_CKM.1/TCAP, encryption and MAC data authentication.

- The TOE authenticate themselves according to FIA_API.1/PACE in case of PACE. It authenticates themselves according to FIA_API.1/CA in case of TCAP as Proximity Integrated Circuit Card (PICC).
- The SFR FMT_MOF.1 limits the configuration of the trusted channel according to FTP_ITC.1.3 to an administrator.
- The SFR FMT_MSA.1/KM describe the requirements for management of key security attributes for these mechanisms.

The security objective for the TOE O.AccCtrl “Access control” is met by the following SFR:

- The SFR FIA_ATD.1 defines the security attributes of individual users including *Role* which is used for access control according to FDP_ACF.1/Oper.
- The SFR FDP_ACC.1/Oper describes the subset access control for the *Cryptographic Operation* SFP.
- The SFR FDP_ACF.1/Oper defines the access control rules of the *Cryptographic Operation* SFP.
- The *Cryptographic Operation* SFP is defined by means of security attributes managed according to the SFR FMT_MSA.1/KM, FMT_MSA.2 and FMT_MSA.3/KM.

The security objective for the TOE O.SecMan “Security management” is met by the following SFR:

- The SFR FIA_ATD.1 defines the security attributes of individual users including *Role* which is used to enforce the *Key Management SFP*.
- The SFR FDP_ACC.1/KM defines subjects, objects and operations of the *Key Management SFP*.
- The SFR FMT_SMF.1 lists the security management functions provided by the TSF.
- The SFR FMT_SMR.1 lists the security role supported by the TOE especially the administrator and – if supported - Crypto-Officer responsible for key management.
- The SFR FCS_CKM.1/AES, FCS_CKM.1/ECC, FCS_CKM.1/ECKA-EG. FCS_CKM.1/PACE, FCS_CKM.1/RSA, FCS_CKM.1/AES_RSA, FCS_CKM.1/TCAP require the TSF to implement key generation function according to the assigned standards.
- The SFR FCS_CKM.5/ECDHE require the TSF to implement key agreement function according to the assigned standards.
- The SFR FCS_CKM.5/AES and FCS_CKM.5/ECKA-EG require the TSF to implement key derivation function according to the assigned standards.
- The SFR FCS_CKM.1/AES_RSA and FCS_CKM.5/AES_RSA require the TSF to implement AES session key generation function with RSA key encryption respective RSA key decryption and AES key derivation according to the assigned standards.
- The SFR FCS_RNG.1 requires the TSF to implement a random number generator for key generation, key agreement functions and cryptographic operations.
- The SFR FCS_COP.1/ED requires the TSF to provide encryption and decryption according to AES which may be used for key management.
- The SFR FCS_COP.1/Hash requires the TSF to implement cryptographic primitive hash function for key derivation, cf. FCS_CKM.5.
- The SFR FPT_ISA.1/CK requires import and FPT_ESA.1/CK the export of cryptographic keys with security attributes and protection of confidentiality according to SFR FPT_TCT.1/CK and integrity protection according to FPT_TIT.1/CK.

- The SFR FPT_ISA.1/Cert requires import of certificates with security attributes and integrity protection according to FPT_TIT.1/Cert.
- The SFR FPT_TDC.1/Cert requires consistent interpretation of certificate's content. The SFR FPT_TDC.1/CK requires consistent interpretation of security attributes imported with the key.
- The SFR FCS_COP.1/KW and FCS_COP.1/KU require the TSF key wrapping and unwrapping for key management.
- The SFR FCS_CKM.4 requires the TSF to implement secure key destruction.
- The SFR FMT_MSA.1/KM and FMT_MSA3/KM limit the setting of default values and specification of alternative initial values for security attributes of cryptographic keys to administrators. The SFR FMT_MSA.1/KM prevents modification or deletion of security attributes of keys.
- FMT_MSA.2 enforce secure values for security attributes.
- The SFR FMT_MTD.1/KM and FMT_MTD.1/RK restricts the management of cryptographic keys espacially the import of root public keys to specifically authorized users.

TOE O.TST "Self-test" is directly met by the SFR FPT_TST.1 and FPT_FLS.1. The TSF shall preserve a secure state if self test fails.

The security objective for the TOE O.PhysProt "Physical protection" is met by the directly met by the SFR FPT_PHP.3. The memory encryption required by FDP_SDC.1, FCS_CKM.1/SDEK and FCS_COP.1/SDE provides additional protection against compromise of information in the stored data. The SFR FPT_FLS.1 requires the TSF to preserve a secure state if exposure to operating conditions occurs which may not be tolerated according to the requirement Limited fault tolerance (FRU_FLT.2) or manipulation and physical probing is detected and secure state is reached as response.

The security objective for the TOE O.SecUpCP "Secure import of Update Code Package" is met by the following SFR:

- The SFR FDP_ACC.1/UCP and FDP_ACF.1/UCP requires the TSF to provide access control to enforce SFP *Update*. Note the verification of the authenticity of UCP and decryption of authentic UCP are performed under control of the TSF.
- The SFR FCS_COP.1/VDSUCP requires the verification of digital signature of the Issuer and FCS_COP.1/DecUCP requires decryption of authentic of UCP.
- The SFR FDP_ITC.2/UCP requires the TSF to import UCP as user data with security attributes if the authenticity of UCP is successful verified.
- The SFR FPT_TDC.1/UCP requires the TSF to import consistently the security attributes of the UCP.
- The SFR FMT_MSA.3 requires to provide restrictive initial security attributes to enforce the SFP *Update*.
- The SFR FDP_RIP.1/UCP requires the TSF to remove the received UCP after unsuccessful verification of its authenticity.
- The UCP signature verification key may be updated according to FPT_ISA.1/Cert with integrity protection according to FPT_TIT.1/Cert.
- The UCP decryption key may be updated with confidentiality protection according to FPT_TCT.1/CK with FCS_COP.1/KU.

7.3.3 Security assurance requirements rationale

The EAL4 was chosen to permit a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line. EAL4 is applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur sensitive security specific engineering costs.

The augmentation of the component AVA_VAN.5 provides a higher assurance of the security by vulnerability analysis to assess the resistance to penetration attacks performed by an attacker possessing a high attack potential.

Development security is concerned with physical, procedural, personnel and other technical measures that may be used in the development environment to protect the TOE. In the particular case of a cryptographic module the TOE implements security mechanisms in hardware which details about the implementation, (e. g., from design, test and development tools) may make such attacks easier. Therefore, in the case of a cryptographic module, maintaining the confidentiality of the design and protected manufacturing is very important and the strength of the corresponding protection measures shall be balanced with respect to the assumed moderate attack potential. Therefore ALC_DVS.2 was augmented.

7.3.4 Compatibility between SFR of [ST-CSP] and [ST-PLTF]

Table 11 below lists the SFRs that are declared in the security target [ST-PLTF], and separates them in 3 groups, as requested in [CCDB]:

- **IP-SFR**: Irrelevant Platform-SFRs not being used by the Composite-ST
- **RP-SFR-SERV**: Relevant Platform-SFRs being used by the Composite-ST to implement a security service with associated TSFI
- **RP-SFR-MECH**: Relevant Platform-SFRs being used by the Composite-ST because of its security properties providing protection against attacks to the TOE as a whole and are addressed in ADV_ARC. These required security properties are a result of the security mechanisms and services that are implemented in the Platform TOE.

Platform SFR	Platform-SFR content	IP_SFR	RP-SFR-SERV	RP-SFR-MECH	Comments
FDP_ACC.2/FIREWALL	Complete access control			x	
FDP_ACF.1/FIREWALL	Security attribute based access control			x	
FDP_IFC.1/JCVM	Subset information flow control			x	
FDP_IFF.1/JCVM	Simple security attributes			x	
FDP_RIP.1/OBJECTS	Subset residual information protection			x	
FMT_MSA.1/JCRE	Management of security attributes		x		
FMT_MSA.1/JCVM	Management of security attributes		x		
FMT_MSA.2/FIREWALL_JCVM	Secure security attributes		x		
FMT_MSA.3/FIREWALL	Static attribute initialization		x		
FMT_MSA.3/JCVM	Static attribute initialization		x		
FMT_SMF.1	Specification of Management Functions		x		
FMT_SMR.1	Security roles		x		
FCS_CKM.1/RSA	Cryptographic key generation		x		
FCS_CKM.1/ECDSA	Cryptographic key generation		x		
FCS_CKM.1/HMAC	Cryptographic key generation		x		
FCS_CKM.1/TDES	Cryptographic key generation	x			Not used
FCS_CKM.1/AES	Cryptographic key generation		x		
FCS_CKM.1/ECPF	Cryptographic key generation	x			Not used
FCS_CKM.1/ECDH	Cryptographic key generation		x		
FCS_CKM.1/DHGen	Cryptographic key generation	x			Not used
FCS_CKM.4	Cryptographic key destruction		x		
FCS_COP.1	Cryptographic operation		x		
FCS_RNG.1	Random number generation		x		
FDP_RIP.1/ABORT	Subset residual information protection		x		

Platform SFR	Platform-SFR content	IP_SFR	RP-SFR-SERV	RP-SFR-MECH	Comments
FDP_RIP.1/APDU	Subset residual information protection		x		
FDP_RIP.1/GlobalArray	Subset residual information protection		x		
FDP_RIP.1/bArray	Subset residual information protection		x		
FDP_RIP.1/KEYS	Subset residual information protection			x	
FDP_RIP.1/TRANSIENT	Subset residual information protection		x		
FDP_ROL.1/FIREWALL	Basic rollback			x	
FAU_ARP.1	Security alarms			x	
FDP_SDI.2/DATA	Stored data integrity monitoring and action			x	
FPR_UNO.1	Unobservability			x	
FPT_FLS.1/JCS	Failure with preservation of secure state			x	
FPT_TDC.1	Inter-TSF basic TSF data consistency		x		
FIA_ATD.1/AID	User attribute definition		x		
FIA_UID.2/AID	User identification before any action		x		
FIA_USB.1/AID	User-subject binding		x		
FMT_MTD.1/JCRE	Management of TSF data		x		
FMT_MTD.3/JCRE	Secure TSF data		x		
FDP_ITC.2/Installer	Import of user data with security attributes		x		
FMT_SMR.1/Installer	Security roles		x		
FPT_FLS.1/Installer	Failure with preservation of secure state		x		
FPT_RCV.3/Installer	Automated recovery without undue loss		x		

Platform SFR	Platform-SFR content	IP_SFR	RP-SFR-SERV	RP-SFR-MECH	Comments
FDP_ACC.2/ADEL	Complete access control		x		
FDP_ACF.1/ADEL	Security attribute based access control		x		
FDP_RIP.1/ADEL	Subset residual information protection		x		
FMT_MSA.1/ADEL	Management of security attributes		x		
FMT_MSA.3/ADEL	Static attribute initialization		x		
FMT_SMF.1/ADEL	Specification of Management Functions		x		
FMT_SMR.1/ADEL	Security roles		x		
FPT_FLS.1/ADEL	Failure with preservation of secure state		x		
FDP_RIP.1/ODEL	Subset residual information protection		x		
FPT_FLS.1/ODEL	Failure with preservation of secure state		x		
FCO_NRO.2/CM	Enforced proof of origin		x		
FDP_IFC.2/CM	Complete information flow control		x		
FDP_IFF.1/CM	Simple security attributes		x		
FDP_UIT.1/CM	Data exchange integrity		x		
FIA_UID.1/CM	Timing of identification		x		
FMT_MSA.1/CM	Management of security attributes		x		
FMT_MSA.3/CM	Static attribute initialization		x		
FMT_SMF.1/CM	Specification of Management Functions		x		
FMT_SMR.1/CM	Security roles		x		
FTP_ITC.1/CM	Inter-TSF trusted channel		x		
FPT_TST.1/SCP	TSF Testing		x		
FPT_PHP.3/SCP	Resistance to physical attacks			x	

Platform SFR	Platform-SFR content	IP_SFR	RP-SFR-SERV	RP-SFR-MECH	Comments
FPT_RCV.3/SCP	Automated recovery without undue loss		x		
FPT_RCV.4/SCP	Function recovery		x		
FDP_UIT.1/CCM	Data exchange integrity		x		
FDP_ROL.1/CCM	Basic rollback		x		
FDP_ITC.2/CCM	Import of user data with security attributes		x		
FPT_FLS.1/CCM	Failure with preservation of secure state		x		
FCS_COP.1/DAP	Cryptographic operation		x		
FDP_ACC.1/SD	Subset access control		x		
FDP_ACF.1/SD	Security attribute based access control		x		
FMT_MSA.1/SD	Management of security attributes		x		
FMT_MSA.3/SD	Static attribute initialization		x		
FMT_SMF.1/SD	Specification of Management Functions		x		
FMT_SMR.1/SD	Security roles		x		
FTP_ITC.1/SC	Inter-TSF trusted channel		x		
FCO_NRO.2/SC	Enforced proof of origin		x		
FDP_IFC.2/SC	Complete information flow control		x		
FDP_IFF.1/SC	Simple security attributes		x		
FMT_MSA.1/SC	Management of security attributes		x		
FMT_MSA.3/SC	Static attribute initialization		x		
FMT_SMF.1/SC	Specification of Management Functions		x		
FIA_UID.1/SC	Timing of identification		x		
FIA_UAU.1/SC	Timing of authentication		x		

Platform SFR	Platform-SFR content	IP_SFR	RP-SFR-SERV	RP-SFR-MECH	Comments
FIA_UAU.4/SC	Single-use authentication mechanisms		x		
FMT_SMR.1/ GemActivate	Security roles	x			Not used
FMT_SMF.1/ GemActivate	Specification of Management Functions	x			Not used
FMT_MOF.1/GemActivate	Management of security functions behavior	x			Not used
FMT_MSA.1/GemActivate	Management of security attributes	x			Not used
FMT_MTD.1/GemActivate	Management of TSF data	x			Not used
FIA_ATD.1/OS-UPDATE	User attribute definition	x			Not used
FDP_ACC.1/GemActivate	Subset access control	x			Not used
FDP_ACF.1/GemActivate		x			Not used
FMT_MSA.3/GemActivate	Static attribute initialization	x			Not used
FTP_TRP.1/OS-UPDATE		x			Not used
FPT_FLS.1/SecureAPI	Failure with preservation of secure state			x	
FPT_ITT.1/SecureAPI	Basic internal TSF data transfer protection			x	
FPR_UNO.1/SecureAPI	Unobservability			x	
FCS_CKM.1/DH_PACE	Cryptographic key generation – Diffie-Hellman for PACE session keys		x		
FCS_CKM.4/PACE	Cryptographic key destruction		x		
FCS_COP.1/PACE_ENC	Cryptographic operation – Encryption / Decryption AES / 3DES		x		
FCS_COP.1/PACE_MAC	Cryptographic operation – MAC		x		
FCS_COP.1/PACE_CAM	Cryptographic operation – Modular Multiplication		x		
FCS_RND.1/PACE	Quality metric for random numbers		x		

Platform SFR	Platform-SFR content	IP_SFR	RP-SFR-SERV	RP-SFR-MECH	Comments
FIA_AFL.1/PACE	Authentication failure handling – PACE authentication using non-blocking authorisation data		x		
FIA_UID.1/PACE	Timing of identification		x		
FIA_UAU.1/PACE	Timing of authentication		x		
FIA_UAU.4/PACE	Single-use authentication mechanisms - Single-use authentication of the Terminal by the TOE		x		
FIA_UAU.5/PACE	Multiple authentication mechanisms		x		
FIA_UAU.6/PACE	Re-authenticating – Re-authenticating of Terminal by the TOE		x		
FDP_RIP.1/PACE	Subset residual information protection			x	
FTP_ITC.1/PACE	Inter-TSF trusted channel after PACE		x		
FMT_SMF.1/PACE	Specification of Management Functions		x		
FMT_SMR.1/PACE	Security roles		x		
FMT_LIM.1/PERSO	Limited capabilities		x		
FMT_LIM.2/PERSO	Limited availability		x		
FMT_MTD.1/INI_ENA	Management of TSF data – Writing of Initialization Data and Pre-personalization Data		x		
FMT_MTD.1/INI_DIS	Management of TSF data – Disabling of Read Access to Initialization Data and Pre-personalization Data		x		
FMT_MTD.1/KEY_READ	Management of TSF data – Key Read		x		
FPT_EMS.1	TOE Emanation			x	

Platform SFR	Platform-SFR content	IP_SFR	RP-SFR-SERV	RP-SFR-MECH	Comments
FPT_FLS.1	Failure with preservation of secure state			x	
FPT_TST.1	TSF testing			x	
FPT_PHP.3	Resistance to physical attack			x	
FCS_COP.1/SHA	Cryptographic operation – Hash for key derivation		x		
FCS_COP.1/SIG_VER	Cryptographic operation – Signature verification		x		
FIA_API.1/CA	Authentication Proof of Identity		x		
FIA_UID.1/EAC2_Terminal	Timing of identification		x		
FIA_UAU.1/EAC2_Terminal	Timing of authentication		x		
FIA_UAU.6/CA	Re-authenticating of Terminal by the TOE		x		
FTP_ITC.1/CA2	Inter-TSF trusted channel after CA2		x		
FMT_MTD.1/Initialize_PIN	Management of TSF data – Initialize PIN	x			

Table 11 Compatibility between SFR of [ST-CSP] and [ST-PLTF]

8 TOE SUMMARY SPECIFICATION

This section provides a summary of the security functions implemented by the TOE in order to fulfil the security functional requirements. The summary is structured in security functions.

The security functionalities concerning the IC and the JC Platform are described in [ST-IC], [ST-PLTF] and are not redefined in this security target, although they must be considered for the TOE.

8.1 TOE SECURITY FUNCTIONS PROVIDED BY THE CSP

8.1.1 Authentication management

This security function provides authentication mechanisms such as:

1. Authentication of human users to the TOE
2. Authentication of the TOE to external entity
3. Authentication of external entity to the TOE
4. Authentication failure detection and reaction

8.1.2 Cryptography management

This security function provides cryptographic mechanisms such as:

1. Creation, derivation, deletion, import and export of cryptographic keys
2. import of certificates
3. Keys Security attributes modifications
4. Generation of random bits which may be used for security services outside the platform.
5. Cryptographic operations (encryption, decryption, authentication, data integrity and confidentiality)

8.1.3 Access control and imports/export management

This security function provides access control mechanisms and imports/export mechanisms on following operations:

1. Import of user data with security attributes including Update Code Package
2. Export of user data with security attributes
3. Export of user data without security attributes
4. Cryptographic operations

8.1.4 Security management

This security function provides security mechanisms such as:

1. Management of security functions behaviour
2. Management of Authentication reference data
3. Management of security attributes of cryptographic keys
4. Maintaining roles: Unidentified User, Unauthenticated User, Key Owner, Application component, Administrator
5. Ensuring that only secure values are accepted for security attributes
6. Restricting the ability to manage security functions such as password authentication and trusted channel to the Administrator
7. Management of trusted channel

8.1.5 Protection management

This security function provides protection mechanisms such as:

1. Management of the integrity or confidentiality of data and TSF data that required integrity or confidentiality
2. Management of the residual information protection
3. Management of failures
4. Management of physical attack
5. Management of self-tests

8.2 TOE SECURITY FUNCTIONS RATIONALE

Security Functional Requirements	TOE Summary Specification
FCS_CKM.1/AES	Cryptography management
FCS_CKM.1/AES_RSA	Cryptography management
FCS_CKM.1/ECC	Cryptography management
FCS_CKM.1/ECKA-EG	Cryptography management
FCS_CKM.1/PACE	Cryptography management, Authentication management
FCS_CKM.1/RSA	Cryptography management
FCS_CKM.1/SDEK	Cryptography management, Protection management
FCS_CKM.1/TCAP	Cryptography management, Authentication management
FCS_CKM.4	Cryptography management
FCS_CKM.5/AES	Cryptography management
FCS_CKM.5/AES_RSA	Cryptography management
FCS_CKM.5/ECC	Cryptography management
FCS_CKM.5/ECDHE	Cryptography management
FCS_CKM.5/ECKA-EG	Cryptography management
FCS_COP.1/CDS-ECDSA	Cryptography management, Authentication management
FCS_COP.1/CDS-RSA	Cryptography management, Authentication management
FCS_COP.1/DecUCP	Cryptography management, Authentication management
FCS_COP.1/ED	Cryptography management, Authentication management
FCS_COP.1/Hash	Cryptography management, Authentication management
FCS_COP.1/HDM	Cryptography management, Authentication management
FCS_COP.1/HEM	Cryptography management, Authentication management
FCS_COP.1/HMAC	Cryptography management, Authentication management
FCS_COP.1/KU	Cryptography management, Authentication management
FCS_COP.1/KW	Cryptography management, Authentication management
FCS_COP.1/MAC	Cryptography management, Authentication management
FCS_COP.1/SDE	Cryptography management, Protection management

Security Functional Requirements	TOE Summary Specification
FCS_COP.1/TCE	Cryptography management, Protection management
FCS_COP.1/TCM	Cryptography management, Protection management
FCS_COP.1/VDS-ECDSA	Cryptography management, Authentication management
FCS_COP.1/VDS-RSA	Cryptography management, Authentication management
FCS_COP.1/VDSUCP	Cryptography management, Authentication management
FCS_RNG.1	Cryptography management
FDP_ACC.1/KM	Access control and imports/export management
FDP_ACC.1/Oper	Access control and imports/export management
FDP_ACC.1/UCP	Access control and imports/export management
FDP_ACF.1/Oper	Access control and imports/export management
FDP_ACF.1/UCP	Access control and imports/export management
FDP_DAU.2/Att	Protection management, Authentication management
FDP_DAU.2/Sig	Protection management, Authentication management
FDP_ETC.1	Access control and imports/export management
FDP_ETC.2	Access control and imports/export management
FDP_ITC.2/UCP	Access control and imports/export management
FDP_ITC.2/UD	Access control and imports/export management
FDP_RIP.1/UCP	Protection management
FDP_SDC.1	Protection management
FIA_AFL.1	Authentication management
FIA_API.1/CA	Authentication management
FIA_API.1/PACE	Authentication management
FIA_ATD.1	Authentication management
FIA_UAU.1	Authentication management
FIA_UAU.5	Authentication management
FIA_UAU.6	Authentication management
FIA_UID.1	Authentication management
FIA_USB.1	Authentication management
FMT_MOF.1	Security management
FMT_MSA.1/KM	Cryptography management
FMT_MSA.2	Security management
FMT_MSA.3/KM	Cryptography management, Security management
FMT_MTD.1/KM	Cryptography management
FMT_MTD.1/RAD	Security management
FMT_MTD.1/RK	Security management
FMT_MTD.3	Security management

Security Functional Requirements	TOE Summary Specification
FMT_SAE.1	Security management
FMT_SMF.1	Security management
FMT_SMR.1	Security management
FPT_ESA.1/CK	Access control and imports/export management
FPT_FLS.1	Protection management
FPT_ISA.1/Cert	Access control and imports/export management
FPT_ISA.1/CK	Access control and imports/export management
FPT_PHP.3	Protection management
FPT_TCT.1/CK	Access control and imports/export management
FPT_TDC.1/CK	Access control and imports/export management
FPT_TDC.1/Cert	Access control and imports/export management
FPT_TDC.1/UCP	Access control and imports/export management
FPT_TIT.1/Cert	Protection management
FPT_TIT.1/CK	Protection management
FPT_TST.1	Protection management
FRU_FLT.2	Protection management
FTP_ITC.1	Security management

Table 12 TOE SECURITY FUNCTIONS RATIONALE

END OF DOCUMENT