Specification of the Security Target TCOS CSP Module Version 1.0 Release 1/P6022y

Version: 1.0.1/20200227

Dokumentenkennung:	CD.TCOS.ASE
Dateiname:	ASE TCOS CSP Module Version 1.0.1.docx
Stand:	2020-02-27
Version:	1.0.1
Hardware Basis:	P6022y
Autor:	Ernst-G. Giessmann, Markus Blick
Geltungsbereich:	T-Sec
Vertraulichkeitsstufe:	**Öffentlich**

History

Version	Date	Remark
1.0.1	2020-02-27	Final document

Contents

1 ST Introduction

1 This section provides document management and overview information that are required a potential user of the TOE to determine, whether the TOE fulfils her requirements.

1.1 ST Reference

2 Title:	Specification of the Security Target TCOS CSP Module Version 1.0 Release 1/P6022y
TOE:	TCOS CSP Module Version 1.0 Release 1/P6022y
Sponsor:	T-Systems International GmbH
Editor(s):	T-Systems International GmbH, T-Sec
CC Version:	3.1 (Revision 5)
Assurance Level:	EAL4 augmented with ALC_DVS.2 and AVA_VAN.5.
General Status:	Final Document
Version Number:	1.0.1
Date:	2020-02-27
Certification ID:	BSI-DSZ-CC-1118
Keywords:	Cryptographic Service Provider, TCOS

1.2 TOE Reference

3 This Security Target refers to the Product “TCOS CSP Module Version 1.0 Release 1/P6022y” (TOE) of T-Systems International GmbH for CC evaluation.

1.3 TOE Overview

4 The Target of Evaluation (TOE) addressed by this Security Target is a chip with contact-based interfaces programmed according to [ISO7816]. The TOE is dedicated to providing cryptographic services for the protection of the confidentiality and the integrity of user data, and for entity authentication. In this ST the TOE as a whole is called *Security Component*.

5 The TOE is prepared to be used in composed IT products comprising the TOE and one or more application components. The TOE provides the security services for these applications.

6 The TOE is defined as a device consisting of hardware, firmware and software and is implemented as a security integrated circuit.

7 The TOE security functionality (TSF) is logically defined by a common set of cryptographic and non-cryptographic security services for users and mechanisms for internal use. The cryptographic services for users comprise

- authentication of users,
- authentication and attestation of the TOE 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 TOE.

8 The TSF provides a non-cryptographic real time service.

- The time service allows the user to query the internal time of the TSF.
- The time stamp service provides evidence that user data were presented to the TSF and exported audit data, were generated at certain point in time and in a verifiable sequence.

9 The audit functionality generates audit records on selected user activities controlled by the TSF and security events of the TOE.

10 The TOE uses memory encryption for protection of internally stored data.

11 The TOE provides its services in a Client-Server architecture, where the TOE (Security Component) and the Application Component are physically separated interacting through a trusted channel. The Application component (in client role) uses the security services of the TOE (in server role).

12 The communication between the TOE and the application is protected by means of secure channel according to [CC]. The TOE supports cryptographically protected trusted channels between the TOE and the external entities.

13 The internal cryptographic TSF is used for

- TSF data import including certificates and cryptographic keys,
- confidentiality protection of stored user data and TSF data.

14 The TOE implements means to prove its own identity. The authentication keys are managed by the TOE manufacturer, the vendor or another trusted identity depending on the life cycle phase.

15 The non-cryptographic TSF provides human user authentication, access control on cryptographic TSF and cryptographic keys and TSF protection.

16 The TOE provides a time service, time stamp service and security audit.

17 The TOE supports download, authenticity verification and decryption of Update Code Packages for the CSP.

18 This version of the TOE does not support clustering of TOE samples.

19 The hardware may be relevant in some context, and if so, the TOE will be identified in more detail as “TCOS CSP Module Version 1.0 Release 1/P6022y”, otherwise the short-

er notion “TCOS CSP Module Version 1.0 Release 1” will be used, indicating that this context may be applicable to any realization regardless which hardware base is used. The TOE follows the composite evaluation aspects ([AIS36]). The Security Target of the underlying platform ([HWST]) claims conformance to Smartcard IC Platform Protection Profile ([ICPP]).

20 This composite ST is based on the ST of the underlying platform ([HWST]). The compatibility of the Life Cycle Model of the Protection Profile [CSPPP] and the Life Cycle Model required by [ICPP] will be shown in chap. 1.3.4, as required by [JIL].

21 The TOE comprises of

- the circuitry of the chip including all IC Dedicated Software being active in the Operational Phase of the TOE (the integrated circuit, IC),
- the IC Embedded Software (ES, Card Operating System, OS) including configuration and initialization data related to the security functionality of the chip,
- the Application Software (AS) providing the implemented services, and
- the associated guidance documentation including the more detailed description of the file system.

22 The Guidance documentation ([TCOSGD]) provides further requirements for the manufacturer and security measures required for protection of the TOE until reception by the end-user. In addition, the guidance contains in chapter 9.9 a detailed description of the delivery items and their protection.

1.3.1 TOE security features for operational use

23 The TOE security services are logically separated and provided through well-defined external interfaces. The TSF is self-contained, i.e. it is provided by the TOE itself. The operational environment cannot affect the security and correctness of the TSF, but it supports the availability of the TSF.

1.3.2 TOE Type

24 The TOE’s type addressed by this ST is according to [CSPPP] an integrated circuit (IC) providing different cryptographic services.

25 The typical life cycle phases for the current TOE type are development, manufacturing, combining with the intended Application Component and operational use. The life cycle phase development includes development of the IC itself and IC embedded software. Manufacturing includes IC manufacturing and smart card manufacturing, and installation of a card operating system. Installing includes completion of the operating system, installation of the smart card applications and their electronic personalization, i.e. tying the application data up to the Application Component.

26 Operational use of the TOE is explicitly in the focus of the Protection Profile [CSPPP]. Nevertheless, some TOE functionality is already available in the manufacturing and the card issuing life cycle phases. Therefore, it is also considered in this ST.

1.3.3 File System of the TOE

27 The TOE is configured with a dedicated file system during life cycle phase 2 “Manufacturing”. It is described in more detail in the Admin Guidance [TCOSGD].

1.3.4 Life Cycle Phases Mapping

28 Following the JIL Guidance for Smart Card Evaluation [JIL] the life cycle phases of a smart card can be divided into the following seven phases:

Phase 1: Smartcard Embedded Software Development
Phase 2: IC Development
Phase 3: IC Manufacturing and Testing
Phase 4: IC Packaging and Testing
Phase 5: Smartcard Product Finishing Process
Phase 6: Smart Card Personalization
Phase 7: Operational Use

29 This is the base for the TOE life cycle. It is described in terms of the following four life cycle phases, subdivided in 7 steps, with respect to [JIL].

Life cycle phase 1 “Development”

30 *Step 1*: The TOE is developed in phase 1. The IC developer develops the integrated circuit, the IC dedicated software and the guidance documentation associated with these TOE components.

31 *Step 2:* The software developer uses the guidance documentation for the integrated circuit and the guidance documentation for relevant parts of the IC dedicated software, and develops the IC embedded software (operating system), the application(s) and the guidance documentation associated with these TOE components.

32 The manufacturing documentation of the IC including the IC dedicated software and the embedded software in the non-volatile non-programmable memories is securely delivered to the IC manufacturer. The IC embedded software in the non-volatile programmable memories and the application(s) is securely delivered to the IC manufacturer.

33 This life cycle phase steps cover exactly phase 1 and phase 2 of [JIL]].

Life cycle phase 2 “Manufacturing and Pre-Personalization”

34 *Step 3*: In a first step, the TOE integrated circuit is produced. The circuit contains IC dedicated software, and the parts of the TOE’s embedded software (ES) in the non-volatile non-programmable memory (ROM). The IC manufacturer writes IC identification data onto the chip to track and control the IC during manufacturing, and during delivery to Application Component manufacturer. The IC manufacturer adds parts of the IC embedded software, the object system and keys in the non-volatile programmable memory, e.g. EEPROM.

35 *Step 4*: The IC may be delivered as a wafer, module or a packaged component, possibly combined with hardware for the contact-based interface.

36 *Step 5*: The IC manufacturer

- adds the IC embedded software, or parts of it in the non-volatile programmable memories, e.g. EEPROM or FLASH,
- creates the application(s), and

- equips the TOE's chip with pre-personalization data.

37 The first step in this phase, also named phase 5.1, is called *Completion,* and the one and only user of the TOE in this stage is the *Completion Agent* acting as manufacturer. After Completion the operating system cannot be changed anymore, the access protocols and the TSF are ready to use.

38 The other two steps, also known as phase 5.2 and phase 6, are called *Installation.* The one and only one user of the TOE in this stage is the *Installation Agent*. This step is sometimes also called *Pre-Personalization*. Creation of the application(s) implies the creation of the master file (MF), dedicated files (DFs), and elementary files (EFs) according to [ISO7816].

39 During Pre-Personalization the Installation agent installs keys used for key derivation and update-in-field procedure. Further the TOE is delivered with an attestation key for attestation as genuine sample of the certified product, cf. chapter 6.1.5.

40 Note that step 5 and step 6 is implemented technically as part of step 3.

After *Installation,* the TOE is prepared for the pairing with the Application Component and the import and generation of individual data.

41 **TOE delivery appears after Pre-Personalization. The TOE is delivered as a chip with a completed Operating System and a ready to personalization object system.**

42 *Application Note 1:* The IC personalization phase should not be confused with the TOE's personalization after integration in the Application Component, which takes place only in the next life cycle phase of the TOE.

43 The security environment for the TOE and the ST of the underlying platform match, the IC life cycle phases up to 6 are covered by a controlled environment as required in [HWCR, p. 41]. In IC life cycle phase 7 no restrictions apply.

Life cycle phase 3 "Personalization of the CSP"

44 *Step 7.* This life cycle phase corresponds to the first step of Phase 7 of [JIL].

45 The pre-personalized TOE together with the IC identifier is securely delivered from the TOE manufacturer to the Application Component manufacturer. The TOE is personalized in this phase and bound to the dedicated component. The authentication data for *Personalization* is delivered securely to the Application Component manufacturer.

46 The personalization of TOE includes

1. the check of the authenticity of the TOE using the attestation key of the TOE,
2. the check that the TOE is in the original state using the user administrator's password,
3. the generation of application depending keys, and
4. configuration of the TSF, if necessary.

47 Configuration of the TSF is performed by the *Personalization Agent*.

48 This cycle phase is already an operational use of the composite product and not a personalization of the hardware. The hardware's "Personalization" (cf. [HWST]) ends with the *Installation* of the TOE (installation of the object system).

Life cycle phase 4 "Operational Use"

49 *Step 7*: The security functions of the TOE are used by the Application Component.

50 This life cycle phase corresponds to the rest of Phase 7 of [JIL].

51 The life cycle of the TOE ends with implementation of any update code package changing the TOE to a new IT product.

1.3.5 Non-TOE hardware/software/firmware

52 There is no explicit non-TOE hardware, software or firmware required by the TOE to perform its claimed security features.

1.3.6 TOE Boundaries

1.3.6.1 TOE Physical Boundaries

53 Smartcard as used in this ST means an integrated circuit containing a microprocessor, (CPU), a coprocessor for special (cryptographic) operations, a random number generator, volatile and non-volatile memory, and associated software, packaged and embedded in a carrier. The integrated circuit is a single chip incorporating CPU and memory, which include RAM, ROM, and EEPROM.

54 The chip is embedded in a module, which provides the capability for standardized connection to systems separate from the chip through TOE's interfaces in accordance with ISO standards.

55 The physical constituent of the TOE is the initialized chip with an operating system in ROM and EEPROM and an installed object system.

1.3.6.2 TOE Logical Boundaries

56 All card accepting devices (Host Applications) will communicate through the I/O interface of the operating system by sending and receiving octet strings. The logical boundaries of the TOE are given by the complete set of commands of the TCOS operating system for access, reading, writing, updating or erasing data.

57 The input to the TOE is transmitted over the physical interface as an octet string that has the structure of Command Application Protocol Data Unit (CAPDU). The output octet string from the TOE has the structure of a Response Application Protocol Data Unit (RAPDU).

58 The Application Protocol Data Units or TCOS commands that can be used in the operating systems are described in more detail in another document.

1.3.7 Evaluated package types

59 The TOE can be delivered in several package types as defined in [*HWST*]:

- Wafer, Ux
- Sawn Wafer, Ux
- HVQFN32 SMD, HN
- HX2QFN14 SMD, HQ
- Module, Xx

2 Conformance Claims

2.1 CC Conformance Claims

60 This Security Target claims conformance to Common Criteria for Information Technology Security Evaluation [CC],

Part 1: Introduction and general model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017,

Part 2: Security functional components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017,

Part 3: Security assurance components; CCMB-2017-04-003, Version 3.1, Revision 5, April 2017

as follows:

Part 2 extended, Part 3 conformant.

61 The Common Methodology for Information Technology Security Evaluation, Evaluation methodology; CCMB-2012-09-004, Version 3.1, Revision 5, April 2017, [CC] has to be taken into account.

2.2 PP Claims

62 This ST claims *strict* conformance to the Base-PP

Common Criteria Protection Profile ‘Cryptographic Service Provider’, Version 0.9.8, Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik under BSI-CC-PP-0104-2019, 2019-02

63 This ST claims *strict* conformance to the PP-Module

Common Criteria Protection Profile Module ‘Cryptographic Service Provider Time Stamp and Audit’, Version 0.9.5, Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik under BSI-CC-PP-0107-2019, 2019-05

2.3 Package Claims

64 The evaluation of the TOE is a composite evaluation and uses the results of the CC evaluation provided by [HWCR]. The IC hardware platform and its primary embedded software are evaluated at level EAL 6+.

65 The evaluation assurance level of the TOE is EAL4 augmented with ALC_DVS.2 and AVA_VAN.5 as defined in [CC][1].

[1] In this ST the backslash provides line breaks for CC conformant identifiers. It should not be considered as a part of the identifier. Identifiers containing natural words are hyphenated as usual.

2.4 Conformance Claim Rationale

66 The TOE type is a chip consistent with the TOE type of the claimed PP ([CSPPP]).

3 Security Problem Definition

3.1 Assets and External Entities

Assets

67 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).

68 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.

Users and subjects

69 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.

70 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.

71 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.

Objects

72 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.

Security attributes

73 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.

74 Passwords as Authentication Reference Data have the security attributes

- status: values initial password, operational password,
- number of unsuccessful authentication attempts.

75 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.

76 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.

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

78 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.

79 The Administrator role is 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.
- Auditor: role that is allowed to configure the audit functionality, review audit data and export audit trails.
- Timekeeper: role that is allowed to adjust the internal clock.
- Update Agent: authorized user for import and verification of Update Code Package.
- Personalization Agent: role that is allowed to access the TOE in order to configure it while personalization phase.

80 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).

81 The TOE is delivered with initial Authentication Data Records for Unidentified User, Unauthenticated User and administrator roles. 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 than 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 be associated with.

82 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.1 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 “Signature Service[2]”, or time stamp service (cf. FDP_DAU.2/TS) by key usage type “TimeStamp”, 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,

[2] In the Protection Profile [**CSPPP**] this service is called “DigSign”, whereas in the corresponding SFR the same service is called “Signature Service”. Therefore, the last term used also here.

83 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 signatures created with a private signature key.

84 The UCP have at least the security attributes

- Issuer of the UCP,
- Version Number of the UCP.

3.2 Threats

85 This section describes the threats to be averted by the TOE independently or in collaboration with its IT environment. These threats result from the assets stored in or protected by the TOE and the method of TOE's use in the operational environment.

T.DataCompr **Compromise of communication data**

86 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**

87 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**

88 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**

89 A attacker gets as TOE user unauthorized access to security services of the TOE.

T.PhysAttack **Physical attacks**

90 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**

91 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.

3.3 Organizational Security Policies

92 The TOE and/or its environment shall comply with the following Organizational Security Policies (OSP) as security rules, procedures, practices, or guidelines imposed by an organization upon its operations (see CC part 1, sec. 3.2).

OSP.SecCryM Secure cryptographic mechanisms

93 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

94 The TOE provides cryptographic and non-cryptographic security services to the authorized user for encryption and decryption of user data, authentication prove and verification of user data, entity authentication to external entities including attestation, trusted channel, random bit generation and time services.

OSP.KeyMan Key Management

95 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 according to OSP Secure cryptographic mechanisms only 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

96 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

97 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.

98 The PP-Module [CSPMOD] adds new organizational security policies OSP.TimeService and OSP.Audit.

OSP.TimeService Audit for key management and cryptographic operations

99 The TOE provides non-cryptographic time service and cryptographic time stamp service for user data and TSF data. The time stamp service provides evidence that user data were presented to the TSF and exported audit data were generated at certain point in time and in a verifiable sequence.

OSP.Audit Audit for key management and cryptographic operations

100 The TOE provides security auditing related to activities controlled by the TSF and security critical events. The security auditing provides evidence to make users responsible for

actions they are authorized for and to protect users against unwarranted accusation. The administrator is allowed to select auditable events.

3.4 Assumptions

101 The assumptions describe the security aspects of the environment in which the TOE will be used or is intended to be used.

A.SecComm **Secure communication**

102 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.

4 Security Objectives

103 This chapter describes the security objectives for the TOE and for the TOE environment.

4.1 Security Objectives for the TOE

104 The following TOE security objectives address the protection provided by the TOE *independent* of the TOE environment.

O.AuthentTOE Authentication of the TOE to external entities

105 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

106 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

107 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 number generation service

108 The TOE provides cryptographically secure random number generation service for the users.

O.TChann Trusted channel

109 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.

110 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

111 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

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

O.SecMan Security management

113 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

114 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

115 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

116 The TSF verifies the authenticity of received encrypted Update Code Package, decrypts authentic Update Code Package and stores decrypted Update Code Package.

117

118 The PP-Module [CSPMOD] adds the following security objectives for the TOE.

O.TimeServices Time services

119 The TOE provides an internal time service and time stamp service for the user.

O.Audit Audit for cryptographic TSF

120 The TSF provides security auditing of selected user activities controlled by the TSF and security critical events. The Administrator is allowed to select auditable events, to manage the audit functionality and the export of audit records.

4.2 Security Objectives for the Operational Environment

OE.CommInf Communication infrastructure

121 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

122 The Application component supports the TOE for communication with users and trust centers.

OE.SecManag Security management

123 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

124 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

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

126 The PP-Module [CSPMOD] adds the following security objectives for the operational environment of the TOE.

OE.Audit Review and availability of audit records

127 The administrator shall ensure the regular audit review and the availability of exported audit records.

OE.TimeSource External time source

128 The operational environment provides reliable external time source for the adjustment of the TOE internal time source.

4.3 Security Objective Rationale

129 The following table provides an overview for security objectives coverage (TOE and its environment). It shows that all threats and OSPs are addressed by the security objectives. It also shows that all assumptions are addressed by the security objectives for the TOE environment.

	T.DataCompr	T.DataMani	T.Masqu	T.ServAcc	T.PhysAttack	T.FaUpD	OSP.SecCryM	OSP.SecService	OSP.KeyMa	OSP.Audit	OSP.TC	OSP.TimeService	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		x				
O.PhysProt					x									
O.RBGS							x	x						
O.SecMan			x				x		x		x			
O.SecUpCP						x							x	

	T.DataCompr	T.DataMani	T.Masqu	T.ServAcc	T.PhysAttack	T.FaUpD	OSP.SecCryM	OSP.SecService	OSP.KeyMa	OSP.Audit	OSP.TC	OSP.TimeService	OSP.Update	A.SecComm
O.TChann	x	x	x	x			x	x						
O.TST					x									
O.Audit										x				
O.TimeService												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	
OE.Audit										x				
OE.TimeService												x		

Table 1:Security Objective Rationale for the TOE

The corresponding complete rationale is given in the claimed by this ST Protection Profiles [CSPPP] and [CSPMOD]. Hence, it will not be repeated here.

5 Extended Components Definition

130 This Security Target includes all extended components from the claimed PPs. This includes families FCS_RNG, FCS_CKM.5, FIA_API, FPT_TCT, FPT_TIT, FPT_ISA, FPT_ESA and FPT_SDC from [CSPPP].

5.1 FCS_RNG Generation of random numbers

131 The family "Generation of random numbers (FCS_RNG)" is specified as follows.

Family behavior

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

Component levelling:

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 a mechanism to generate random numbers that meet [assignment: *a defined quality metric*].

5.2 FCS_CKM.5 Cryptographic key derivation

132 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.

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

FCS_CKM.5 Cryptographic key derivation requires the TOE to provide key derivation which can be based on an assigned standard.

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*].

5.3 FIA_API Authentication Proof of Identity

134 The family “Authentication Proof of Identity (FIA_API)” is specified as follows.

Family behavior

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

Component levelling:

FIA_API Authentication Proof of Identity
1

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 actions defined to be auditable.

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.

5.4 FPT_TCT Inter-TSF TSF data confidentiality transfer protection

135 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.

136 The family “TSF data confidentiality transfer protection (FPT_TCT)” is specified as follows.

Family behavior

This family requires confidentiality protection of exchanged TSF data.

Component levelling:

FPT_TCT.1 TSF data confidentiality transfer protection 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 actions defined to be auditable.

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 unauthorized disclosure.

5.5 FPT_TIT Inter-TSF TSF data integrity transfer protection

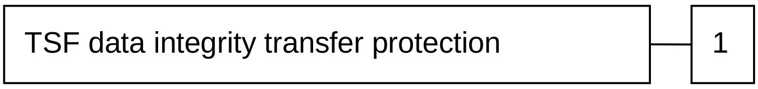
137 his section describes the functional requirements for integrity protection of TSF data exchanged with another trusted IT product. The family is similar to the family Inter-TSF user data integrity transfer protection (FDP_UIT) which defines functional requirements for integrity protection of exchanged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

138 The family “TSF data confidentiality transfer protection (FPT_TCT)” is specified as follows.

Family behavior

This family requires confidentiality protection of exchanged TSF data.

Component levelling:



FPT_TIT.1 TSF data integrity transfer protection requires the TOE to protect the integrity of information in exchanged TSF data.

Management: FPT_TIT.1

There are no management activities foreseen.

Audit: FPT_TIT.1

There are no actions defined to be auditable.

FPT_TIT.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_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.

5.6 FPT_ISA TSF data import with security attributes

139 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.

140 The family “TSF data import with security attributes (FPT_ISA)” is specified as follows.

Family behavior

This family requires TSF data import with security attributes.

Component levelling:

TSF data import with security attributes
1

FPT_ISA.1 Import of TSF data with security attributes 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 actions defined to be auditable.

FPT_ISA.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 orFMT_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*].

5.7 FPT_ESA TSF data export with security attributes

141 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.

142 The family “TSF data export with security attributes (FPT_ESA)” is specified as follows.

Family behavior

This family requires TSF data export with security attributes.

Component levelling:

TSF data export with security attributes
1

FPT_ESA.1 Export of TSF data with security attributes 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 actions defined to be auditable.

FPT_ESA.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 orFMT_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*].

5.8 FDP_SDC Stored data confidentiality

143 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.

144 The family “Stored data confidentiality (FDP_SDC)” is specified as follows.

Family behavior

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.1 Stored data confidentiality requires 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 actions defined to be auditable.

FDP_SDC.1 Stored data confidentiality

Hierarchical to: No other components.

Dependencies: No other components.

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*].

6 Security Requirements

145 This part of the ST defines the detailed security requirements that shall be satisfied by the TOE. The statement of **TOE security requirements** shall define the *functional* and *assurance* security requirements that the TOE needs to satisfy in order to meet the security objectives for the TOE.

146 The CC allows several operations to be performed on functional requirements; *refinement*, *Selection*, *assignment*, and *iteration* are defined in section 8.1 of Part 1 of the Common Criteria [CC]. Each of these operations is used in this ST.

147 The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinements of security requirements are denoted in such a way that added words are in **bold text** and removed are ~~crossed out~~. Refinements made by the ST author appear ***slanted, bold and underlined***.

148 The **Selection** operation is used to Select one or more options provided by the CC in stating a requirement. Selections having been made by the PP author are denoted as underlined text. Selections made by the ST author appear *slanted and underlined*.

149 The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments having been made by the PP author are denoted by showing as underlined text. Assignments made by the ST author appear *slanted and underlined*.

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

6.1 Security Functional Requirements for the TOE

151 The statements of security requirements must be internally consistent. As several different PPs with similar SFRs are claimed, great care must be taken to ensure that these several iterated SFRs do not lead to inconsistency. Following the Protection Profile [CSPPP] the SFR are not listed according to their classes but their functionalities.

6.1.0 Overview

152 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.

153 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.

154 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, FCS_CKM.5/KED-RSA, calculates the MAC for the cipher text and compares it with the received MAC. If the integrity of the cipher text is determined then the receiver decrypts the cipher text with the data decryption key, cf. FCS_COP.1/HDM.

155 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 5.3 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. 6.1. The authentication may be mutual as required for trusted channels in chapter 6.1.

156 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).

157 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.

158 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.

159 The TOE enforces the Key Management SFP to protect the cryptographic keys (as data objects of TSF data) and the key management services (as operation, cf. to SFR of the FMT class) provided for Administrators, Crypto-Officers and Key Owners (as subjects), cf. FDP_ACC.1/KM. Note the cryptographic keys will be used for cryptographic operations under Cryptographic Operation SFP as well.

160 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 (bits)	Standard
brainpoolP192r1	192	RFC5639, TR-03111, section 4.1.3 [ECCTR]
brainpoolP224r1	224	RFC5639, TR-03111, section 4.1.3 [ECCTR]

brainpoolP256r1	256	RFC5639, TR-03111, section 4.1.3 [ECCTR]
brainpoolP320r1	384	RFC5639, TR-03111, section 4.1.3 [ECCTR]
brainpoolP384r1	384	RFC5639, TR-03111, section 4.1.3 [ECCTR]
brainpoolP512r1	512	RFC5639, TR-03111, section 4.1.3 [ECCTR]
brainpoolP192t1	192	RFC5639, TR-03111, section 4.1.3 [ECCTR]
brainpoolP224t1	224	RFC5639, TR-03111, section 4.1.3 [ECCTR]
brainpoolP256t1	256	RFC5639, TR-03111, section 4.1.3 [ECCTR]
brainpoolP320t1	320	RFC5639, TR-03111, section 4.1.3 [ECCTR]
brainpoolP384t1	384	RFC5639, TR-03111, section 4.1.3 [ECCTR]
brainpoolP512t1	512	RFC5639, TR-03111, section 4.1.3 [ECCTR]
Curve P-192	192	FIPS PUB 186-4 B.4 and D.1.2.3 [FIPS186]
Curve P-256	256	FIPS PUB 186-4 B.4 and D.1.2.3 [FIPS186]
Curve P-384	384	FIPS PUB 186-4 B.4 and D.1.2.3 [FIPS186]

161 *Application Note 2:* Note that for security reasons the Curve P-521 is not supported by the TOE.

162 For Diffie-Hellman key exchange refer to the following groups:

Name	IANA number	Standard
256-bit random ECP group	19	RFC5903
384-bit random ECP group	20	RFC5903
brainpoolP256r1	28	RFC6954
brainpoolP384r1	29	RFC6954
brainpoolP512r1	30	RFC6954

163 *Application Note 3:* Note that for security reasons the 521-bit ECP group is not supported by the TOE.

164 The Module-PP adds for time stamps and audit mechanism the following new SFRs compared to the Base-PP:

FAU_GEN.1, FAU_STG.1, FAU_STG.3, FDP_ACF.1/TS, FDP_DAU.2/TS, FDP_\ETC.2/TS, FDP_ITC.2/TS, FMT_MTD.1/Audit, FMT_MOF.1/TSA, FMT_SMF.1/TSA, FMT_SMR.1/TSA, FPT_STM.1, FPT_TIT.1/Audit

6.1.1 Key management

6.1.1.1 Management of security attributes

165 **FDP_ACC.1/KM Subset access control – Cryptographic operation**

Hierarchical to: No other components

Dependencies: FDP_ACF.1 Security attribute based access control: not fulfilled but justified (the rules are specified by FMT_MTD.1/KM)

FDP_ACC.1.1/KM

The TSF shall enforce the Key Management SFP[3] on

1. subjects: *Crypto-Officer*[4], Key Owner
2. objects: operational cryptographic keys;
3. operations: key generation, key derivation, key import, key export, key destruction.

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

Hierarchical to: No other components

Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] fulfilled by FDP_ACC.1/KM
FMT_SMR.1 Security roles: fulfilled
FMT_SMF.1 Specification of Management: fulfilled

FMT_MSA.1.1/KM

The TSF shall enforce the Key Management SFP and Cryptographic Operation SFP[5] to restrict the ability to

1. change_default[6] 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[7] to *Crypto-Officer*[8],
2. **modify or delete**[6] **the security attributes Identity of the key, Key entity, Key type, Key usage type, Key validity time period of an existing key**[7] **to none**[9]**,**
3. **modify independent on key usage[6] the security attributes Key usage counter of an existing key[10] to none**[11].
4. **modify**[12] **the security attributes Key access control attribute of an existing key**[13] **to *Crypto-Officer*** [14],

[3] [assignment: *access control SFP, information flow control SFP*]

[4] [selection: Administrator, Crypto-Officer]

[5] [assignment: *access control SFP*]

[6] [selection: *change_default, query, modify, delete,* [assignment: *other operations*]]

[7] [assignment: *list of security attributes*]

[8] [selection: *Administrator, Crypto-Officer*]

[9] [assignment: *the authorized identified roles*]

[10] [assignment: *list of security attributes*]

[11] [assignment: *the authorized identified roles*]

[12] [selection: *change_default, query, modify, delete,* [assignment: *other operations*]]

[13] [assignment: *list of security attributes*]

[14] [selection: *Administrator, Crypto-Officer*]

5. **query[12] the security attributes Key type, Key usage type, Key access control attributes, Key validity time period and Key usage counter of an identified key[13] to *Crypto-Officer and Key Owner*[15].**

167 *Application Note 4:* The refinements repeat parts of the SFR component in order to avoid iteration of the component.

168 FMT_MSA.3/KM Static attribute initialisation

Hierarchical to: No other components

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

FMT_MSA.3.1/KM

The TSF shall enforce the Key Management SFP, Cryptographic Operation SFP and Update SFP[16] to provide restrictive[17] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/KM

The TSF shall allow the *Crypto-Officer* [18] to specify alternative initial values to override the default values when a **cryptographic key** ~~object or information~~ is created.

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

Hierarchical to: No other components

Dependencies: FMT_SMR.1 Security: fulfilled
FMT_SMF.1 Specification of Management Functions: fulfilled

FMT_MTD.1.1/KM

The TSF shall restrict the ability to

1. create according to FCS_CKM.1[19] the cryptographic keys[20] to *Crypto-Officerr*[21]
2. **import according to FPT_TCT.1/CK, FPT_TIT.1/CK and FPT_ISA.1/CK[22] the cryptographic keys[23] to *Crypto-Officer* [24]**
3. **export according to FPT_TCT.1/CK, FPT_TIT.1/CK and FPT_ESA.1/CK[25] the cryptographic keys[26] to *Crypto-Officer*[27] if security attribute of the key allows export,**

[15] [selection: *Administrator, Crypto-Officer, Key Owner*]
[16] [assignment: *access control SFP, information flow control SFP*]
[17] [selection: *choose one of: restrictive, permissive,* [assignment: *other property*]]
[18] [selection: *Administrator, Crypto-Officer*]
[19] [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]
[20] [assignment: *list of TSF data*]
[21] [selection: *Administrator, Crypto-Officer, Key Owner*]
[22] [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]
[23] [assignment: *list of TSF data*]
[24] [selection: *Administrator, Crypto-Officer*]
[25] [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]

4. **delete according to FCS_CKM4**[28] **the cryptographic keys**[29] **to *Crypto-Officer and Key Owner***[30]

170 *Application Note 5:* The bullets (2) to (4) are refinements to avoid an iteration of component and therefore printed in bold.

6.1.1.2 Hash based functions

171 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]: fulfilled
FCS_CKM.4 Cryptographic key destruction: fulfilled

FCS_COP.1.1/Hash

The TSF shall perform hash generation[31] in accordance with a specified cryptographic algorithm SHA-256, SHA-384, SHA-512[32] and cryptographic key sizes none[33] that meet the following: FIPS 180-4 [FIPS180][34].

172 *Application Note 6:* 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.

6.1.1.3 Management of Certificates

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

Hierarchical to: No other components

Dependencies: FMT_SMR.1 Security roles: fulfilled
FMT_SMF.1 Specification of Management Functions: fulfilled

FMT_MTD.1.1/RK

The TSF shall restrict the ability to

(1) create[35], modify, clear and delete[36] the root key pair[37] to *Crypto-Officer* [38],

(2) **import and delete**[39] **the known as authentic public key of a**

[26] [assignment: *list of TSF data*]

[27] [selection: *Administrator, Crypto-Officer, Key Owner*]

[28] [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]

[29] [assignment: *list of TSF data*]

[30] [selection: *Administrator, Crypto-Officer, Key Owner*]

[31] [assignment: *list of cryptographic operations*]

[32] [assignment: *cryptographic algorithm*]

[33] [assignment: *cryptographic key sizes*]

[34] [assignment: *list of standards*]

[35] "create” denotes initial setting a root key

[36] [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]

[37] [assignment: *list of TSF data*]

[38] [selection: *Administrator, Crypto-Officer*]

certification authority in a PKI[40] **to *Crypto-Officer*** [41]

174 *Application Note 7:* 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 a 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 and third bullets are a refinement to avoid an iteration of component and therefore printed in bold.

175 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]: fulfilled
[FMT_MTD.1 Management of TSF data orFMT_MTD.3 Secure TSF data]: fulfilled

FPT_TIT.1.1/Cert

The TSF shall enforce the Key Management SFP[42] to receive[43] **certificate** ~~TSF data~~ in a manner protected from modification and insertion[44] errors.

FPT_TIT.1.2/Cert

The TSF shall be able to determine on receipt of **certificate** ~~TSF data~~, whether modification or insertion[45] has occurred.

176 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]: fulfilled
[FMT_MTD.1 Management of TSF data or FMT_MTD.3 Secure TSF data]: fulfilled
[FMT_MSA.1 Management of security attributes, or FMT_MSA.4 Security attribute value inheritance]: fulfilled
FPT_TDC.1 Inter-TSF basic TSF data consistency: fulfilled

FPT_ISA.1.1/Cert

The TSF shall enforce the Key Management SFP[46] when importing **certificates** ~~TSF data~~, controlled under the SFP from outside the TOE.

FPT_ISA.1.2/Cert

The TSF shall use the security attributes associated with the imported

[39] [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]

[40] [assignment: *list of TSF data*]

[41] [selection: *Administrator, Crypto-Officer*]

[42] [assignment: *access control SFP, information flow control SFP*]

[43] [selection: *transmit, receive, transmit and receive*]

[44] [selection: *modification, deletion, insertion, replay*]

[45] [selection: *modification, deletion, insertion, replay*]

[46] [assignment: *access control SFP, information flow control SFP*]

certificate ~~TSF data~~.

FPT_ISA.1.3/Cert

The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the **certificate** ~~TSF data~~ received.

FPT_ISA.1.4/Cert

The TSF shall ensure that interpretation of the security attributes of the imported **certificates** ~~TSF data~~ is as intended by the source of the **certificates** ~~TSF data~~.

FPT_ISA.1.5/Cert

The TSF shall enforce the following rules when importing **certificates** ~~TSF data~~ 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 [47].

177 **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[48] 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 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.

(2) The identity of the certificate issuer shall meet the identity of the signer of the certificate.[49]

when interpreting the **certificate from a trust center** ~~TSF data from another trusted IT product~~.

178 *Application Note 8:* The security attributes assigned to certificate holder and the cryptographic key in the certificate are used as TSF data of the TOE. The certificate is import-

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

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

[49] [assignment: *list of TSF data types*]

ed 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).

6.1.1.4 Key generation, agreement and destruction

179 *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.

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

181 FCS_RNG.1 Random number generation

Hierarchical to:	No other components
Dependencies:	No dependencies

FCS_RNG.1.1

The TSF shall provide a *deterministic and physical* [50] random number generator that implements: *DRG.4 and PTG.2 according to [AIS31]*.[51]

FCS_RNG.1.2

The TSF shall provide random numbers that meet *requirements of a DRG.4*

(DRG.4.1) *The internal state of the RNG shall use PTRNG of class PTG.2 as random source.*

(DRG.4.2) *The RNG provides forward secrecy.*

(DRG.4.3) *The RNG provides backward secrecy even if the current internal state is known.*

(DRG.4.4) *The RNG provides enhanced forward secrecy on condition "session closed or aborted".*

(DRG.4.5) *The internal state of the RNG is seeded by a PTRNG of class PTG.2.*

(DRG.4.6) *The RNG generates output for which $k > 2^{34}$ strings of bit length 128 are mutually different with probability $1-\varepsilon$, with $\varepsilon < 2^{-16}$.*

(DRG.4.7) *Statistical test suites cannot practically distinguish the*

[50] [selection: *physical, non-physical true, deterministic, hybrid physical, hybrid deterministic*]

[51] [assignment: *list of security capabilities*]

random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A, the NIST and the diehardher[52] *tests*

and the quality requirements for a PTG.2 generator according to [AIS31].[53]

182 *Application Note 9:* The random bit generation of **DRG.4** 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/KW, FCS_COP.1/HEM and FCS_COP.1/TCE. The TOE provides the random number generation as security service for the user. **PTG.2** provides random bits for the Get Random command.

183 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]: fulfilled
FCS_CKM.4 Cryptographic key destruction: fulfilled

FCS_CKM.1.1/AES

The TSF shall generate cryptographic **AES** key in accordance with a specified cryptographic key generation algorithm AES[54] and key size 128 bits, *256 bits*[55] that meet the following: [ISO18033-3][56].

184 *Application Note 10:* The cryptographic key may be used with FCS_COP.1/ED, e.g. for internal purposes.

185 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]: fulfilled
FCS_CKM.4 Cryptographic key destruction: fulfilled

FCS_CKM.5.1/AES

The TSF shall derive cryptographic AES key[57] from *random input parameters*[58] in accordance with a specified cryptographic key derivation algorithms AES key generation using bit string derived from input parameters with DKDF_NIST_800_108[59] and specified cryptographic key sizes 128 bits, *256 bits*[60] that meet the following: [NIST SP 800-108][61].

[52] The selected here test suites http://csrc.nist.gov/groups/ST/toolkit/rng/documents/sts-2.1.1.zip and http://www.phy.duke.edu/~rgb/General/dieharder/dieharder-3.31.0.tgz are available at NIST and Dieharder web sites. Note that the dieharder tests include Marsaglia's "Diehard battery of tests" and NIST tests.

[53] [assignment: *a defined quality metric*]

[54] [assignment: *cryptographic key generation algorithm*]

[55] [selection: *256 bits, no other key size*]

[56] [assignment: *list of standards*]

[57] [assignment: *key type*]

[58] [assignment: *input parameters*]

[59] [assignment: *cryptographic key derivation algorithm*]

[60] [selection: *256 bits, no other key size*]

186 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]: fulfilled FCS_CKM.4 Cryptographic key destruction: fulfilled

FCS_CKM.1.1/ECC

The TSF shall generate cryptographic **elliptic curve** keys **pairs** in accordance with a specified cryptographic key generation algorithm ECC key pair generation with *elliptic curves table 6.1.0*[62] and cryptographic key sizes *key size in the table 6.1.0* [63] that meet the following: *corresponding standard in the table 6.1.0* [64].

187 *Application Note 11:* 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.

188 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]: fulfilled FCS_CKM.4 Cryptographic key destruction: fulfilled

FCS_CKM.5.1/ECC

The TSF shall derive cryptographic elliptic curve key~~s~~ pair[65] from *seed given from external entity*[66] in accordance with a specified cryptographic key derivation algorithms *ECC key pair generation with elliptic curves table 6.1.0*[67] *using bit string derived from input parameters with DKDF_ECC_PRF* [68] and specified cryptographic key sizes *key size in the table 6.1.0*[69] that meet the following: *standards in the table 6.1.0,* [TR-03111], **[SP800-56C], [BIP32]**[70].

189 *Application Note 12:* The elliptic key pair derivation applies a key derivation function (KDF) 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 ([ECCTR, section 4.1.1, Algorithm 1 or 2]. The input 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.

[61] [assignment: *list of standards*]

[62] [selection: *elliptic curves in the table in para 160*]

[63] [selection: *key size in the table in para 160*]

[64] [assignment: *list of standards*]

[65] [assignment: *key type*]

[66] [assignment: *input parameters*]

[67] [selection: *elliptic curves in the table in para 160*]

[68] [assignment: *KDF*]

[69] [selection: *key size in the table in para 160*]

[70] [assignment: *list of standards*]

190 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]: fulfilled
FCS_CKM.4 Cryptographic key destruction: fulfilled

FCS_CKM.1.1/RSA

The TSF shall generate cryptographic **RSA** keys pairs in accordance with a specified cryptographic key generation algorithm RSA[71] and cryptographic key sizes *2048, 3072 bits*[72] that meet the following: PKCS #1 v2.2 [RFC8017][73].

191 *Application Note 13:* 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.

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

Hierarchical to: No other components

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

FCS_CKM.5.1/ECDHE

The TSF shall derive cryptographic *ephemeral* keys **for data encryption and MAC with AES-128, [selection: AES-256, none other]** [74] from an *agreed shared secret*[75] in accordance with a specified cryptographic key derivation algorithm *Elliptic Curve Diffie-Hellman ephemeral key agreement* with *elliptic curves table 6.1.0*[76] and *DH group in table 6.1.0*[77] with a key derivation from the shared secret [*assignment: key derivation function]* [78] and specified cryptographic key sizes 128 bits, *[selection:256 bits, none other]*[79] that meet the following: TR-03111 [TR-03111][80].

193 *Application Note 14:* The input parameter for key derivation is an agreed shared secret established by means of Elliptic Curve Diffie-Hellman. The tables in 6.1.0 list elliptic curves and the Diffie-Hellman Groups for agreement of the shared secret. The SHA-1

[71] [assignment: *cryptographic key generation algorithm*]

[72] [assignment: *cryptographic key sizes*]

[73] [assignment: *list of standards*]

[74] [selection: *AES-256, none other*]

[75] [assignment: *input parameters*]

[76] [selection: *elliptic curves in table 2*]

[77] [selection: *DH group in table 3*]

[78] [selection: *SHA-256, none other*]

[79] [selection: *256 bits, none other*]

[80] [assignment: *list of standards*]

shall be supported for generation of 128 bits AES keys. The SHA-256 shall be selected and used to generate 256 bits AES keys.

194 *Application Note 15:* This TSFR is not implemented in the TOE because it is neither selected in FCS_COP.1/HEM nor in FCS_COP.1/HDM. The functionality of **FCS_CKM.5/ECDHE** is therefore not needed in the scope of the TOE and would not be reachable over any TSFI. For that reason, the TSFR-operation from the Base-PP was not concretized in this ST.

195 FCS_CKM.1/ECKA-EG Cryptographic key generation – ECKA-EG key generation

Hierarchical to:	No other components
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation]: fulfilled FCS_CKM.4 Cryptographic key destruction: fulfilled

FCS_CKM.1.1/ECKA-EG

The TSF shall generate **an ephemeral** cryptographic **elliptic curve** key **pair for ECKGA-EG** ([ECCTR], sender role) in accordance with a specified cryptographic key generation algorithms ECC key pair generation with *elliptic curves in 6.1.0*[81] and specified cryptographic key sizes *key sizes in 6.1.0*[82] that meet the following: *standards in 6.1.0*[83].

196 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]: fulfilled FCS_CKM.4 Cryptographic key destruction: fulfilled

FCS_CKM.5.1/ECKA-EG

The TSF shall derive cryptographic data encryption key and MAC keys for AES-128, *AES-256*[84] from a private and a public ECC key[85] in accordance with a specified cryptographic key derivation algorithm ECKGA-EG [ECCTR] *elliptic curves in 6.1.0*[86] and X9.6 3 Key Derivation Function[87] and specified cryptographic **symmetric** key sizes 128 bits, *256 bits*[88] that meet the following: TR-03111 [ECCTR, chap. 4.3.2.2][89].

197 *Application Note 16:* FCS_CKM.5/ECKA-EG is used by both the sender (encryption) and the recipient (decryption) to compute a secret point S_{AB} on an elliptic curve and the derived shared secret Z_{AB}. The shared secret is then used as input to the key derivation

[81] [selection: *elliptic curves in table 2*]

[82] [selection: *key size in the table 2*]

[83] [assignment: *list of standards*]

[84] [selection: *AES-256, none other*]

[85] [assignment: *input parameters*]

[86] [selection: *elliptic curves in table 2*]

[87] [assignment: *cryptographic key derivation algorithm*]

[88] [selection: *256 bits, none other*]

[89] [assignment: *list of standards*]

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 6.1.3).

198 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]: fulfilled FCS_CKM.4 Cryptographic key destruction: fulfilled

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, *AES-256*** [90] in accordance with a specified cryptographic key algorithm X9.6 3 Key Derivation Function [ANSI-X9.63] and RSA EME-OAEP [PKCS#1] [91] and specified cryptographic **symmetric** key sizes 128 bits, *256 bits*[92] that meet the following [ISO18033-3], PKCS #1 v2.2 [RFC8017, chapter 3.5][93].

199 *Application Note 17:* 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 6.1.3).

200 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]: fulfilled FCS_CKM.4 Cryptographic key destruction: fulfilled

FCS_CKM.5.1/AES_RSA

The TSF shall derive cryptographic data encryption key and MAC key for AES-128, *AES-256*[94] from **decrypted** RSA encrypted seed[95] in

[90] [selection: *AES-256, none other*]

[91] [assignment: *cryptographic key generation algorithm*]

[92] [selection: *256 bits, none other*]

[93] [assignment: *list of standards*]

[94] [selection: *AES-256, none other*]

accordance with a specified cryptographic key derivation algorithm RSA-EME-OAEP [PKCS#1] and X9.63 [ANSI-X9.63] Key Derivation Function[96] and specified cryptographic **symmetric** key sizes 128 bits, *256 bits*[97] that meet the following: [ISO14888-2, chap. 3.5][98].

201 FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components

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

FCS_CKM.4.1

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *physical deletion by overwriting the memory data with zeros, random numbers or the new key*[99] that meets the following: *none*[100].

202 **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.**

6.1.1.5 Key import and export

203 FCS_COP.1/KW Cryptographic operation – Key wrap

Hierarchical to: No other components

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

FCS_COP.1.1/KW

The TSF shall perform key wrap[101] in accordance with a specified cryptographic algorithm AES-Keywrap *KW* [102] and cryptographic key sizes **of the key encryption key** 128 bits, *256 bits*[103] that meet the following: [SP800-38F][104].

204 *Application Note 18:* The selection of the length of the key encryption key shall be equal or greater than the security bits of the wrapped key.

205 FCS_COP.1/KU Cryptographic operation – Key unwrap

[95] [assignment: *input parameters*]

[96] [assignment: *cryptographic key derivation algorithm*]

[97] [selection: *256 bits, none other*]

[98] [assignment: *list of standards*]

[99] [assignment: *cryptographic key destruction method*]

[100] [assignment: *list of standards*]

[101] [assignment: *list of cryptographic operations*]

[102] [selection: *KW, KWP*]

[103] [selection: *256 bits, none other*]

[104] [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, or
FCS_CKM.1 Cryptographic key generation]: fulfilled

FCS_COP.1.1/KU

The TSF shall perform key unwrap[105] in accordance with a specified cryptographic algorithm AES-Keywrap *KW*[106] and cryptographic key sizes **of the key encryption key** 128 bits, *256 bits*[107] that meet the following: [SP800-38F][108].

206 *Application Note 19:* The selection of the length of the key encryption key shall be equal or greater than the security bits of the wrapped key.

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

FPT_TCT.1.1/CK

The TSF shall enforce the Key Management SFP[109] by providing the ability to transmit and receive[110] **cryptographic key** ~~TSF data~~ in a manner protected from unauthorized disclosure **according to FCS_COP.1/KW and FCS_COP.1/KU**.

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

FPT_TIT.1.1/CK

The TSF shall enforce the Key Management SFP[111] to transmit and receive[112] **cryptographic key** ~~TSF data~~ in a manner protected from modification and insertion[113] errors **according to FCS_COP.1/KW and FCS_COP.1/KU**.

FPT_TIT.1.2/CK

[105] [assignment: *list of cryptographic operations*]

[106] [selection: *KW, KWP*]

[107] [selection: *256 bits, none other*]

[108] [assignment: *list of standards*]

[109] [assignment: *access control SFP, information flow control SFP*]

[110] [selection: *transmit, receive, transmit and receive*]

[111] [assignment: *access control SFP, information flow control SFP*]

[112] [selection: *transmit, receive, transmit and receive*]

[113] [selection: *modification, deletion, insertion, replay*]

The TSF shall be able to determine on receipt of **cryptographic key** ~~TSF data~~, whether modification and insertion[114] has occurred **according to FCS_COP.1/KU**.[115].

209 **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]: fulfilled [FMT_MTD.1 Management of TSF data or FMT_MTD.3 Secure TSF data]: fulfilled [FMT_MSA.1 Management of security attributes or FMT_MSA.4 Security attribute value inheritance]: fulfilled FPT_TDC.1 Inter-TSF basic TSF data consistency: fulfilled

FPT_ISA.1.1/CK

The TSF shall enforce the Key Management SFP[116] when importing **cryptographic key** ~~TSF data~~, 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** ~~TSF data~~.

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** ~~TSF data~~ received.

FPT_ISA.1.4/CK

The TSF shall ensure that interpretation of the security attributes of the imported ~~TSF data~~ is as intended by the source of the **cryptographic key** ~~TSF data~~.

FPT_ISA.1.5/CK

The TSF shall enforce the following rules when importing **cryptographic key** ~~TSF data~~ controlled under the SFP from outside the TOE[117]:

(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) *none*[118].

210 *Application Note 20:* The operational environment is obligated to provide trust center services for secure key management, cf. OE.SecManag.

[114] [selection: *modification, deletion, insertion, replay*]

[115] [assignment: *list of standards*]

[116] [assignment: *access control SFP, information flow control SFP*]

[117] [assignment: *importation control rules*]

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

211 FPT_TDC.1/CK Inter-TSF basic TSF data consistency – Keys

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[119] 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[120]

when interpreting the **imported key data object** ~~TSF data from another trusted IT product~~.

212 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]: fulfilled
[FMT_MTD.1 Management of TSF data or FMT_MTD.3 Secure TSF data]: fulfilled
[FMT_MSA.1 Management of security attributes or FMT_MSA.4 Security attribute value inheritance]: fulfilled
FPT_TDC.1 Inter-TSF basic TSF data consistency: fulfilled

FPT_ESA.1.1/CK

The TSF shall enforce the Key Management SFP[121] when exporting **cryptographic key** ~~TSF data~~, controlled under the SFP(s), outside of the TOE.

FPT_ESA.1.2/CK

The TSF shall export the **cryptographic key** ~~TSF data~~ with the **cryptographic key's** ~~TSF data~~ 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** ~~TSF data~~.

FPT_ESA.1.4/CK

[119] [assignment: *list of TSF data types*]

[120] [assignment: *list of interpretation rules to be applied by the TSF*]

[121] [assignment: *access control SFP, information flow control SFP*]

The TSF shall enforce the following rules when cryptographic key TSF data is exported from the TOE: *none*[122].

213 *Application Note 21:* 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. In this ST are no rules for inter-TSF key exchange foreseen.

6.1.2 Data encryption

214 **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]: fulfilled

FCS_COP.1.1/ED

The TSF shall perform data encryption and decryption[123] in accordance with a specified cryptographic algorithm symmetric data encryption according to AES-128 and *AES-256*[124] in CBC and *no other* mode [125] and cryptographic key size 128 bits, *256 bits*[126], that meet the following: [SP800-38A], [ISO18033-3], [ISO10116][127].

215 *Application Note 22:* 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.

6.1.3 Hybrid encryption with MAC for user data

216 **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]: fulfilled

FCS_COP.1.1/HEM

[122] [assignment: *exportation control rules*]

[123] [assignment: *list of cryptographic operations*]

[124] [selection: *AES-256, no other algorithm*]

[125] [selection: *CRT mode, OFB mode, CFB mode, no other mode*]

[126] [selection: *256 bits, no other key size*]

[127] [assignment: *list of standards*]

The TSF shall perform hybrid data encryption and MAC calculation[128] in accordance with a specified cryptographic algorithm asymmetric key encryption according to *FCS_CKM.1/ECKA-EG, FCS_CKM.1/AES_RSA*[129], symmetric data encryption according to AES-128, *AES-256*[130] *[FIPS197]* in *CBC* *[NIST-SP800-38A]* [131] mode with *CMAC[NIST-SP800-38B],* calculation[132] and cryptographic **symmetric** key sizes 128 bits, *256 bits*[133] that meet the following: [ISO18033-3], [ISO10116], [FIPS197][134].

217 *Application Note 23:* Hybrid data encryption and MAC calculation is a self-contained security service 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 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.

218 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]: fulfilled

FCS_COP.1.1/HDM

The TSF shall perform MAC verification and hybrid data decryption[135] in accordance with a specified cryptographic algorithm asymmetric key decryption according to *FCS_CKM.5/ECKA-EG, FCS_CKM.5/AES_RSA*[136], verification of *CMAC[NIST-SP800-38B],* [137] and symmetric data decryption according to AES with *AES-128, AES-256*[138] *[FIPS197]* in mode *CBC* *[NIST-SP800-38A]* [139] and cryptographic **symmetric** key sizes 128 bits, *256 bits*[140] *[FIPS197]* that meet the following: [ISO18033-3], [ISO10116], [FIPS197][141].

219 *Application Note 24:* Hybrid data decryption and MAC verification is a self-contained security service 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 steps of this service. The used symmetric key shall meet the AES CMAC and the AES algorithm for decryption of the cipher text for MAC, e.g. verification-then-decrypt for CMAC.

[128] [assignment: *list of cryptographic operations*]

[129] [selection: *FCS_CKM.1/ECKA-EG, FCS_CKM.1/AES_RSA*]

[130] [selection: *AES-256, none other*]

[131] [selection: *CBC, CCM, GCM*]

[132] [selection: *CMAC, GMAC, HMAC*]

[133] [selection: *256 bits, none other*]

[134] [assignment: *list of standards*]

[135] [assignment: *list of cryptographic operations*]

[136] [selection: *FCS_CKM.1/ECKA-EG, FCS_CKM.1/AES_RSA*]

[137] [selection: *CMAC, GMAC, HMAC*]

[138] [selection: *AES-256, none other*]

[139] [selection: *CBC, CCM, GCM*]

[140] [selection: *256 bits, none other*]

[141] [assignment: *list of standards*]

6.1.4 Data integrity mechanisms

220 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 cipher texts in Encrypt-then-MAC order.

221 **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]: fulfilled

FCS_COP.1.1/MAC

The TSF shall perform MAC generation and verification[142] in accordance with a specified cryptographic algorithm AES-128 and *AES-256*[143] *[FIPS197]* CMAC [NIST-SP800-38B] and *no other* [144] and cryptographic key sizes 128 bits, *256 bits*[145] that meet the following: [SP800-38B], [ISO9797-1], [SP800-38D], [FIPS197][146].

222 *Application Note 25:* 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.

223 **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]: fulfilled

FCS_COP.1.1/HMAC

The TSF shall perform HMAC generation and verification[147] in accordance with a specified cryptographic algorithm HMAC-SHA256 and *no other*[148] and cryptographic key sizes *128, 256 bits*[149] that meet the following: [RFC2104], [ISO9797-2][150].

224 *Application Note 26:* 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.

[142] [assignment: *list of cryptographic operations*]

[143] [selection: *AES-256, none other*]

[144] [selection: *GMAC, no other*]

[145] [selection: *256 bits, none other*]

[146] [assignment: *list of standards*]

[147] [assignment: *list of cryptographic operations*]

[148] [selection: *HMAC-SHA-1, HMAC- SHA384, no other*]

[149] [assignment: *cryptographic key sizes*]

[150] [assignment: *list of standards*]

225 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]: fulfilled

FCS_COP.1.1/CDS-ECDSA

The TSF shall perform signature-creation[151] in accordance with a specified cryptographic algorithm EC-DSA with *elliptic curves in the table 6.1.0*[152] and specified cryptographic key sizes *corresponding key sizes in the table 6.1.0* [153] that meet the following: *corresponding standard in the table,* [ANSX9.63], [SP800-56C][154].

226 *Application Note 27:* The selection of elliptic curve and cryptographic key sizes shall correspond to each other, e.g. elliptic curve brainpoolP256r1 and key size 256 bits.

227 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]: fulfilled

FCS_COP.1.1/VDS-ECDSA

The TSF shall perform signature-verification[155] in accordance with a specified cryptographic algorithm EC-DSA with *elliptic curves in the table 6.1.0*[156] and specified cryptographic key sizes *corresponding key sizes in the table 6.1.0*[157] that meet the following: *corresponding standard in the table,* [ANSX9.63], [SP800-56C][158].

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

Hierarchical to: No other components

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

FCS_COP.1.1/CDS-RSA

The TSF shall perform signature-creation[159] in accordance with a specified cryptographic algorithm RSA and EMSA-PSS[160] and cryp-

[151] [assignment: *list of cryptographic operations*]

[152] [selection: *elliptic curves in the table in para 160*]

[153] [selection: *key size in the table in para 160*]

[154] [assignment: *list of standards*]

[155] [assignment: *list of cryptographic operations*]

[156] [selection: *elliptic curves in the table in para 160*]

[157] [selection: *key size in the table in para 160*]

[158] [assignment: *list of standards*]

[159] [assignment: *list of cryptographic operations*]

tographic key sizes *2048, 3072 bits*[161] that meet the following: [ISO14888-2], PKCS #1, v2.2 [RFC8017][162].

229 *Application Note 28:* 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.

230 **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]: fulfilled

FCS_COP.1.1/VDS-RSA

The TSF shall perform signature-verification[163] in accordance with a specified cryptographic algorithm RSA and EMSA-PSS[164] and cryptographic key sizes *2048, 3072 bits*[165] that meet the following: [ISO14888-2], PKCS #1, v2.2 [RFC8017][166].

231 *Application Note 29:* 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.

232 **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: fulfilled

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[167] **imported according to FDP_ITC.2/UD by means of *FCS_COP.1/CDS-RSA, FCS_COP.1/CDS-ECDSA*[168] 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[169] with the ability to verify evidence of the validity of the indicated information and the identity of the user that generated the evidence.

233 *Application Note 30:* 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

[160] [assignment: *cryptographic algorithm*]

[161] [assignment: *cryptographic key sizes*]

[162] [assignment: *list of standards*]

[163] [assignment: *list of cryptographic operations*]

[164] [assignment: *cryptographic algorithm*]

[165] [assignment: *cryptographic key sizes*]

[166] [assignment: *list of standards*]

[167] [assignment: *list of objects or information types*]

[168] [selection: *FCS_COP.1/CDS-RSA, FCS_COP.1/CDS-ECDSA*]

[169] [assignment: *list of subjects*]

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.

234 FDP_DAU.2/TS Data Authentication with Identity of Guarantor – Signature with time stamp and optional key usage counter

Hierarchical to: FDP_DAU.1 Basic Data Authentication

Dependencies: FIA_UID.1 Timing of identification: fulfilled

FDP_DAU.2.1/TS

The TSF shall provide a capability to generate evidence that can be used as a guarantee of **the existence at certain point in time, sequence and** validity of

(a) *user data imported according to FDP_ITC.2/UD,*
(b) *exported audit trails according to FMT_MTD.1/Audit clause (1) and FAU_STG.3 clause (1)*[170]

with

(1) **time stamp of the evidence generation according to FPT_STM.1**,
(2) **and optionally the key usage counter of the signature key**

by means of digital signature generated according to *FCS_COP.1/CDS-RSA, FCS_COP.1/CDS-ECDSA*[171] and keys holding the dedicated values of the security attributes Key identity that indicate key ownership of the TOE and Key usage type “Time stamp service” [172].

FDP_DAU.2.2/TS

The TSF shall provide *external entities*[173] with the ability to verify evidence of the validity of the indicated information and the identity of the user that generated the evidence.

235 *Application Note 31:* The TSF according to FDP_DAU.2/TS is intended for time stamp service of the TOE for any provided user data and exported audit records. The user data source shall select the security attribute Key usage type “TimeStamp” of the signature key of the time stamp service. The signature key of exported audit records shall be defined according to FMT_MOF.1.1 clause (9). The Key usage counter allows to verify the sequence of signed data e.g. in an audit trail. The verification of the evidence requires a certificate showing the identity of the TOE sample and the key usage type of time stamp service. The format of input data and output data shall meet the BSI TR-03151 [SE API].

[170] [assignment: *list of objects or information types*]

[171] [selection: *FCS_COP.1/CDS-RSA, FCS_COP.1/CDS-ECDSA*]

[172] Der hier "Time stamp service" genannte Key Usage Type wird außerhalb der SFR generell als "TimeStamp" bezeichnet.

[173] [assignment: *list of subjects*]

6.1.5 Authentication and attestation of the TOE, trusted channel

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

Hierarchical to: No other components

Dependencies: No dependencies

FIA_API.1.1/PACE

The TSF shall provide a PACE in ICC role[174] to prove the identity of the TOE[175] to an external entity **and establishing a trusted channel according to FTP_ITC.1 case 1 or 2**.

237 **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 [EACTR, part 2, section 3.4][176] to prove the identity of the TOE[177] to an external entity **and establishing a trusted channel according to FTP_ITC.1 case 3.**

238 **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: fulfilled

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[178] **by means of** *FCS_COP.1/CDS-ECDSA*[179] **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*[180] with the ability to verify evidence of the validity of the indicated information and the identity of the user that generated the evidence.

239 *Application Note 32:* 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-

[174] [assignment: *authentication mechanism*]

[175] [assignment: *object, authorized user or role*]

[176] [assignment: *authentication mechanism*]

[177] [assignment: *object, authorized user or role*]

[178] [assignment: *list of objects or information types*]

[179] [selection: *FCS_COP.1/CDS-RSA, FCS_COP.1/CDS-ECDSA, ECDAA according to* [selection: [*TPM*], [*FIDO*]]

[180] [assignment: *list of subjects*]

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 [TPM] or FIDO U2F Authenticators [FIDO].

240 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 ~~logically distinct from other communication channels~~ *logically separated from other communication channels*[181] and provides assured identification of its end points ***Authentication of TOE and remote entity according to the case in the following table***[182] and protection of the channel data from modification or disclosure ***according to the case in the following table***[183] **as required by** ***cryptographic operation according to the case in the table***[184].

FTP_ITC.1.2

The TSF shall permit the remote trusted IT product[185] **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.1.1 clause (4)[186].

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: Operation in SFR for trusted channel

[181] [selection: *logically separated from other communication channels, using physical separated ports*]

[182] [selection: *Authentication of TOE and remote entity according to the case in the table*]

[183] [assignment: *according to the case in the table*]

[184] [selection: *cryptographic operation according to the case in the table*]

[185] [selection: *the TSF, the remote trusted IT product*]

[186] [assignment: *list of functions for which a trusted channel is required*]

241 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]: fulfilled
FCS_CKM.4 Cryptographic key destruction: fulfilled

FCS_CKM.1.1/PACE

The TSF shall generate cryptographic keys for **MAC with FCS_COP.1/TCM and if selected encryption keys for FCS_COP.1/TCE** in accordance with a specified cryptographic key ~~generation~~ **agreement** algorithm PACE with *elliptic curves in the table 6.1.0*[187] and Generic Mapping in ICC role[188] and specified cryptographic key sizes *256 bits*[189] that meet the following: [ICAO9303, Part 11, section 4.4][190].

242 *Application Note 33:* 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.

243 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]: fulfilled
FCS_CKM.4 Cryptographic key destruction: fulfilled

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 ~~generation~~ **agreement** algorithm Terminal Authentication version 2 and Chip Authentication Version 2 [191] and specified cryptographic key sizes *256 bits*[192] that meet the following: [EACTR, section 3.3 and 3.4][193].

244 *Application Note 34:* 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.

245 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

[187] [selection: *elliptic curves in para 160*]

[188] [assignment: *cryptographic algorithm*]

[189] [selection: *128 bits, 192 bits, 256 bits*]

[190] [assignment: *list of standards*]

[191] [assignment: *cryptographic algorithm*]

[192] [selection: *128 bits, 192 bits, 256 bits*]

[193] [assignment: *list of standards*]

FCS_CKM.1 Cryptographic key generation]: fulfilled

FCS_COP.1.1/TCE

The TSF shall perform encryption and decryption[194] in accordance with a specified cryptographic algorithm AES in *CBC [NIST-SP800-38A]* mode[195] and cryptographic key sizes *256 bits* [196] that meet the following: [FIPS197] [197].

246 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]: fulfilled

FCS_COP.1.1/TCM

The TSF shall perform MAC calculation and MAC verification[198] in accordance with a specified cryptographic algorithm AES in *CMAC[NIST-SP800-38B],* mode[199] and cryptographic key sizes *256 bits* [200] that meet the following: *[FIPS197]* [201].

6.1.6 User identification and authentication

247 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[202]:

(1) Identity,
(2) Authentication reference data,
(3) Role.

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

Hierarchical to: No other components

Dependencies: FMT_SMR.1 Security roles: fulfilled
FMT_SMF.1 Specification of Management Functions: fulfilled

FMT_MTD.1.1/RAD

[194] [assignment: *list of cryptographic operations*]

[195] [selection: *CBC, CCM, GCM*]

[196] [selection: *128 bits, 192 bits, 256 bits*]

[197] [assignment: *list of standards*]

[198] [assignment: *list of cryptographic operations*]

[199] [selection: CMAC[NIST-SP800-38B], GMAC[NIST-SP800-38D]]]

[200] [selection: *128 bits, 192 bits, 256 bits*]

[201] [assignment: *list of standards*]

[202] [assignment: *list of security attributes*]

The TSF shall restrict the ability to

(1) create[203] the initial Authentication reference data of all authorized users[204] to *User Administrator*[205] [206],

(2) **delete**[203] **the Authentication reference data of an authorized user**[204] **to *User Administrator*** [206],

(3) **modify**[203] **the Authentication reference data**[204] **to the corresponding authorized user**[206]

(4) **create**[203] **the permanently stored session key of trusted channel as Authentication reference data**[204] **to *User Administrator*** [206]

(5) **define**[203] **the time in range *[0..6553.5, infinity seconds]***[207] **after which the user security attribute Role is reset according to FMT_SAE.1** [204] **to *User Administrator*** [206],

(6) **define**[203] **the value *Unidentified user***[208] **to which the security attribute Role shall be reset according to FMT_SAE.1** [204] **to *User Administrator*** [206].

249 *Application Note 35:* 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 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). The bullets (2) to (6) are refinements in order to avoid an iteration of component and therefore printed in bold.

250 FMT_MTD.3 Secure TSF data

Hierarchical to:	No other components
Dependencies:	FMT_MTD.1 Management of TSF data: fulfilled

FMT_MTD.3.1

The TSF shall ensure that only secure values are accepted for passwords[209] **by enforcing change of initial passwords after first successful authentication of the user to different operational password**.

251 FIA_AFL.1 Authentication failure handling

Hierarchical to:	No other components

[203] [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]

[204] [assignment: *list of TSF data*]

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

[206] [assignment: *the authorized identified roles*]

[207] [assignment: *time frame*]

[208] [selection: *Unidentified user, Unauthenticated user*]

[209] [assignment: *list of TSF data*]

Dependencies: FIA_UAU.1 Timing of authentication: fulfilled

FIA_AFL.1.1

The TSF shall detect when *a positive integer number as shown in the rows of the following Table* [210]unsuccessful authentication attempts occur related to *user authentication*[211].

FIA_AFL.1.2

When the defined number of unsuccessful authentication attempts has been *met*[212], the TSF shall *block the corresponding user authentication*[213].

ADR	Role	Retry Counter	Minimum password length
PWD.TimeAdmin	Timekeeper	None, i.e. infinite	16 bytes
PWD.Auditor	Auditor	None, i.e. infinite	16 bytes
PWD.UpdateAgent	Update Agent	8	10 Bytes
PWD.CryptoOfficer	Crypto Officer	None, i.e. infinite	16 bytes
PWD.UserAdmin	User Administrator	5	16 bytes

252 *Application Note 36:* All password ADRs are configured to use the transmission format ASCII, i.e. each digit has a value range from 0 to 255. A minimum password length of e.g. 10 Bytes means therefore that the probability of acceptance of an authentication failure is about 2^{-80}.

253 FIA_USB.1 User-subject binding

Hierarchical to: No other components

Dependencies: FIA_ATD.1 User attribute definition: fulfilled

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[214].

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[215].

FIA_USB.1.3

[210] [selection: [assignment: *positive integer number*], *an* [selection: *Administrator, User Administrator] configurable positive* integer within [assignment: *range of acceptable values*]]

[211] [assignment: *list of authentication events*]

[212] [selection: *met, surpassed*]

[213] [assignment: *list of actions*]

[214] [assignment: *list of user security attributes*]

[215] [assignment: *rules for the initial association of attributes*]

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[216].

254 FMT_SAE.1 Time-limited authorization

Hierarchical to: No other components

Dependencies: FMT_SMR.1 Security roles: fulfilled
FPT_STM.1 Reliable time stamps: fulfilled

FMT_SAE.1.1

The TSF shall restrict the capability to specify an expiration time for Role[217] to *User Administrator*[218].

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)[219] after the expiration time for the indicated security attribute has passed.

255 *Application Note 37:* The TSF implement means to handle expiration time for the roles within 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. Since this ST requires FPT_STM.1 this time stamp is used to meet FMT_SAE.1.

256 FIA_UID.1 Timing of identification

Hierarchical to: No other components

Dependencies: No dependencies

FIA_UID.1.1

The TSF shall allow[220]

(1) self test according to FPT_TST.1,
(2) identification of the TOE to the user,
(3) *none*[221]

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

FIA_UID.1.2

[216] [assignment: *rules for the changing of attributes*]

[217] [assignment: *list of security attributes for which expiration is to be supported*]

[218] [selection: *Administrator, User Administrator]* [assignment: *the authorized identified roles*]

[219] [assignment: *list of actions to be taken for each security attribute*]

[220] [assignment: *list of TSF mediated actions*]

[221] [assignment: *list of other TSF-mediated actions*]

The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of ~~that user~~ **the Unauthenticated User**.

257 **FIA_UAU.1 Timing of authentication**

Hierarchical to: No other components

Dependencies: FIA_UID.1 Timing of identification: fulfilled

FIA_UAU.1.1

The TSF shall allow[222]

(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 *a role*[223] for authentication,
(4) *none*[224]

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.

258 *Application Note 38:* Clause (2) and (3) in FIA_UAU.1.1 allows mutual identification for mutual authentication, e.g. by exchange of certificates.

259 **FIA_UAU.5 Multiple authentication mechanisms**

Hierarchical to: No other components

Dependencies: No dependencies

FIA_UAU.5.1

The TSF shall provide[225]

(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 [EACTR-2] 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 according to [EACTR-2],
(5) certificate based Chip Authentication Version 2 with establishment of trusted channel according to FTP_ITC.1,
(6) message authentication by MAC verification of received mes-

[222] [assignment: *list of TSF mediated actions*]

[223] [selection: *a role, a set of role*]

[224] [assignment: *list of other TSF mediated actions*]

[225] [assignment: *list of multiple authentication mechanisms*]

sages

to support user authentication.

FIA_UAU.5.2

The TSF shall authenticate any user's claimed identity according to the **rules**[226]

(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 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) certificate based Chip Authentication Version 2 with establishment of trusted channel according to FTP_ITC.1 may be used for authentication of users which certificate imported as TSF data,
(7) message authentication by MAC verification of received messages shall be used after initial authentication of remote entity according to clauses (2), (3) or (6) for trusted channel according to FTP_ITC.1,
(8) *none* [227].

260 **FIA_UAU.6 Re-authenticating**

Hierarchical to: No other components

Dependencies: No dependencies

FIA_UAU.6.1

The TSF shall re-authenticate the user under the conditions[228]

(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) *none* [229].

[226] [assignment: *rules describing how the multiple authentication mechanisms provide authentication*]

[227] [assignment: *additional rules*]

[228] [assignment: *list of conditions under which re-authentication is required*]

[229] [assignment: *list of other conditions under which re-authentication is required*]

6.1.7 Access control

261 **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]: fulfilled
[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]: fulfilled
FPT_TDC.1 Inter-TSF basic TSF data consistency: fulfilled

FDP_ITC.2.1/UD

The TSF shall enforce the Cryptographic Operation SFP[230] 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.

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[231].

262 *Application Note 39:* Keys to be used for the cryptographic operation of the imported user data are identified by security attribute *Key identity*.

[230] [assignment: *access control SFP*]

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

263 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]: fulfilled

FDP_ETC.2.1

The TSF shall enforce the Cryptographic Operation SFP[232] 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[233].

264 *Application Note 40:* The TOE imports data to be signed by CSP 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.

265 FDP_ETC.1 Export of user data without security attributes

Hierarchical to: No other components

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

FDP_ETC.1.1

The TSF shall enforce the Cryptographic Operation SFP[234] when exporting user data **as plaintext according to FCS_COP.1/HDM**, controlled under the SFP(s), outside of the TOE.

[232] [assignment: *access control SFP*]

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

[234] [assignment: *access control SFP*]

FDP_ETC.1.2

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

266 **FDP_ACC.1/Oper Subset access control – Cryptographic operation**

Hierarchical to: No other components

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

FDP_ACC.1.1/Oper

The TSF shall enforce the Cryptographic Operation SFP[235] on

(1) subjects: *Crypto-Officer*[236], Key Owner, *none*[237];
(2) objects: operational cryptographic keys, user data;
(3) operations: cryptographic operation[238].

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

Hierarchical to: No other components

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

FDP_ACF.1.1/Oper

The TSF shall enforce the Cryptographic Operation SFP[239] to objects based on the following:

(1) subjects: subjects with security attribute Role *Crypto-Officer*[240], Key Owner, *none*[241];

(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[242].

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 *Crypto-Officer*[243] role is allowed to perform cryptographic operation on cryptographic keys in accordance with their security attributes.

[235] [assignment: *access control SFP*]

[236] [selection: *Administrator, Crypto-Officer*]

[237] [assignment: *other roles*]

[238] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]

[239] [assignment: *access control SFP*]

[240] [selection: *Administrator, Crypto-Officer*]

[241] [assignment: *other roles*]

[242] [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]

[243] [selection: *Administrator, Crypto-Officer*]

(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) *none*[244].

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 the following Table.

(2) *none*[245].

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) *none*[246].

Access control rules for cryptographic operation		
Crypto-Officer, Key Owner[247]	Key type: symmetric Key usage type: Key wrap Key validity time period	FCS_COP.1/KW
Crypto-Officer [247]	Key type: symmetric Key usage type: Key unwrap Key validity time period	FCS_COP.1/KU
(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	Key type: public	FCS_COP.1/HEM,

[244] [assignment: *other rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]

[245] [assignment: *additional rules, based on security attributes, that explicitly authorize access of subjects to objects*]

[246] [assignment: *additional rules, based on security attributes, that explicitly deny access of subjects to objects*]

[247] [selection: *Administrator, Crypto-Officer*]

user)	Key usage type: RSA_ENC Key validity time period: as in certificate	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/DS-ECDSA
(any authenticated user)	Key type: public Key usage type: DS-ECDSA Key validity time period:	FCS_COP.1/DS-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

268 **FDP_ITC.2/TS Import of user data with security attributes – User data for time stamping**

Hierarchical to: No other components

Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]: fulfilled
[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]: fulfilled
FPT_TDC.1 Inter-TSF basic TSF data consistency: fulfilled

FDP_ITC.2.1/TS

The TSF shall enforce the Cryptographic Operation SFP[248] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.2.2/TS

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

FDP_ITC.2.3/TS

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/TS

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/TS

[248] [assignment: *access control SFP*]

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

(1) user data imported for time stamp generation to FDP_\ DAU.2/TS shall be imported with security attributes Key identity of the signature key and Key usage type TimeStamp, and the identification of the requested cryptographic operation[249].

269 *Application Note 41:* Keys to be used for the cryptographic operation of the imported user data are identified by security attribute *Key identity*.

270 **FDP_ETC.2/TS** **Export of user data with security attributes – User data with time stamp**

Hierarchical to: No other components

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

FDP_ETC.2.1/TS

The TSF shall enforce the Cryptographic Operation SFP[250] when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.2.2/TS

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

FDP_ETC.2.3/TS

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/TS

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

(1) user data exported as time stamped data according to FDP_\ DAU.2/TS shall be exported with digital signature and Key identity of the used signature-creation key[251].

271 *Application Note 42:* 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 (e.g. audit records) 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.

272 **FDP_ACF.1/TS** **Security attribute based access control – Crypto graphic operations**

Hierarchical to: No other components

Dependencies: FDP_ACC.1 Subset access control: fulfilled

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

[250] [assignment: *access control SFP*]

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

FMT_MSA.3 Static attribute initialization: fulfilled

FDP_ACF.1.1/TS

The TSF shall enforce the Cryptographic Operation SFP[252] to objects based on the following:

(1) subjects: subjects with security attribute Role Application Component, *no other role*[253];

(2) objects: user data[254].

FDP_ACF.1.2/TS

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

(1) Application Component, *no other role*[255] is allowed to perform cryptographic operation according to FDP_DAU.2/TS on user data with cryptographic keys with Key usage type TimeStamp.

(2) *none*[256].

FDP_ACF.1.3/TS

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: *none*[257].

FDP_ACF.1.4/TS

The TSF shall explicitly deny access of subjects to objects based on 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) *none*[258].

6.1.8 Security Management

273 **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:

[252] [assignment: *access control SFP*]

[253] [assignment: *other roles*]

[254] [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]

[255] [assignment: *other roles*]

[256] [assignment: *other rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]

[257] [assignment: *additional rules, based on security attributes, that explicitly authorize access of subjects to objects*]

[258] [assignment: *additional rules, based on security attributes, that explicitly deny access of subjects to objects*]

(1) management of security functions behavior (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) *none*[259].

274 **FMT_SMR.1 Security roles**

Hierarchical to: No other components

Dependencies: FIA_UID.1 Timing of identification: fulfilled

FMT_SMR.1.1

The TSF shall maintain the roles[260]:

Unidentified User, Unauthenticated User, Key Owner, Application component, *Crypto-Officer, User Administrator, Update Agent*[261], *Personalization Agent, no other roles*[262].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

275 **FMT_SMR.1/TSA Security roles**

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1/TSA

The TSF shall maintain the roles **additional to those required by FMT_SMR.1 in the Base-PP**: *Auditor and Timekeeper*[263].

FMT_SMR.1.2/TSA

The TSF shall be able to associate users with roles.

276 **FMT_SMF.1/TSA Specification of Management Functions**

Hierarchical to: No other components

Dependencies: No dependencies

FMT_SMF.1.1/TSA

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

(1) management of security functions behavior MT_MOF.1/TSA[264].

277

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

[260] [assignment: *authorized identified roles*]

[261] [selection: *Administrator, Crypto-Officer, User Administrator, Update Agent*]

[262] [selection: [assignment: *other roles*], *no other roles*]

[263] [selection: *Auditor,Timekeeper, no other roles*]

[264] [assignment: list of management functions to be provided by the TSF]

278 FMT_MSA.2 Secure security

Hierarchical to: No other components

Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] : fulfilled
FMT_MSA.1 Management of security attributes: fulfilled
FMT_SMR.1 Security roles: fulfilled

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) none[265].

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**.

279 FMT_MOF.1 Management of security functions behavior

Hierarchical to: No other components

Dependencies: FMT_SMR.1 Security roles: fulfilled
FMT_SMF.1 Specification of Management Functions: fulfilled

FMT_MOF.1.1

The TSF shall restrict the ability to

(1) enable[266] the functions password authentication according to FIA_UAU.5.1, clause (1)[267] to *User Administrator*[268].
(2) **disable[266] the functions password authentication according to FIA_UAU.5.1, clause (1)[267] to *User Administrator*[268]**,
(3) **determine the behavior of[266] the functions trusted channel according to FDP_ITC.1.2[267] by defining the remote trusted IT products permitted to initiate communication via the trusted channel to *User Administrator*[268]**,
(4) **determine the behavior of[266] the functions trusted channel according to FDP_ITC.1.3[267] by by defining the entities for which the TSF shall enforce communication via the trusted channel to *User Administrator*[268]**.

280 *Application Note 43:* 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 be-

[265] [assignment: *additional security attributes*]

[266] [selection: *determine the behavior of, disable, enable, modify the behavior of*]

[267] [assignment: *list of functions*]

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

long to the entities for which the TSF shall enforce trusted channel according to FDP_ITC.1, cf. FMT_MOF.1.1 in bullet (4).

281 FMT_MOF.1/TSA Management of security functions behaviour

Hierarchical to: No other components

Dependencies: FMT_SMR.1 Security roles: fulfilled

FMT_SMF.1 Specification of Management Functions: fulfilled

FMT_MOF.1.1/TSA

The TSF shall restrict the ability to

(1) modify the behaviour of[269] the function~~s~~ adjustment of the internal clock according to FPT_STM.1 clause (1)[270] to *Timekeeper* [271],

(2) **modify the behaviour of[272] the function~~s~~ adjustment of the internal clock according to FPT_STM.1 clause (2)[273] to *Timekeeper* [274],,**

(3) determine the behaviour of and modify the behaviour of[275] the functions select the auditable events according to FAU_GEN.1[276] to *Auditor* [277],

(4) determine the behaviour of and modify the behaviour of[278] the functions automatic export of audit trails according to FAU_STG.3.1 clause (1) [279] to *Auditor* [280]

(5) determine the behaviour of and modify the behaviour of[281] the functions FDP_DAU.2/TS by selection of signature key used to sign exported audit trails[282] to *Auditor* [283].

282 Application note *44*: The SFR defines additional management of security functions behaviour for new SFR with respect to the Base-PP. The refinements of FMT_MOF.1.1/TSA in bullets (2) to (5) are made in order to avoid further iterations of the component.

[269] [assignment: *list of management functions to be provided by the TSF*]

[270] [assignment: *list of functions*]

[271] [selection: *Administrator, Timekeeper*]

[272] [selection: *determine the behaviour of, disable, enable, modify the behaviour of*]

[273] [assignment: *list of functions*]

[274] [selection: *Administrator, Timekeeper*]

[275] [selection: *determine the behaviour of, disable, enable, modify the behaviour of*]

[276] [assignment: *list of functions*]

[277] [selection: *Administrator, Auditor*]

[278] [selection: *determine the behaviour of, disable, enable, modify the behaviour of*]

[279] [assignment: *list of functions*]

[280] [selection: *Administrator, Auditor*]

[281] [selection: *determine the behaviour of, disable, enable, modify the behaviour of*]

[282] [assignment: *list of functions*]

[283] [selection: *Administrator, Auditor*]

6.1.9 Security audit

283 **FAU_GEN.1 Audit data generation**

Hierarchical to: No other components

Dependencies: FPT_STM.1 Reliable time stamps: fulfilled

FAU_GEN.1.1

The TSF shall be able to generate an audit record of the following auditable events:

(a) Start-up and shutdown of the audit functions;

(b) All auditable events for the not specified[284] level of audit; and

(c) Discrete adjustment of the real time clock

(1) by automatic adjustment of the clock according to FPT_STM.1.1 clause (2) if selected as auditable event,

(2) by Administrator according to FPT_STM.1.1 clause (1) or(2),

(3) failure of adjustment according to FPT_STM.1.1

(d) other auditable events

(1) Start-up after power-up,

(2) Import of UCP (FDP_ITC.2/UCP),

(3) Authentication failure handling (FIA_AFL.1): the reaching of the threshold for the unsuccessful authentication attempts with claimed Identity of the user,

(4) *no other event*[285]

FAU_GEN.1.2

The TSF shall record within each audit record at least the following information:

(a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

(b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, *none*[286].

284 *Application Note 45:* The SFR FDP_ITC.2/UCP, FIA_AFL.1, FCS_CKM.1, FCS_COP.1, FCS_CKM.4, FPT_FLS.1 and FMT_MOF.1 are defined in the Base-PP. The SFR FPT_\ STM.1, FMT_MOF.1/TSA and FMT_MTD.1/AUDIT are defined in the PP-Module.

285 **FMT_MTD.1/Audit Management of TSF data**

Hierarchical to: No other components

Dependencies: FMT_SMR.1 Security roles: fulfilled
MT_SMF.1 Specification of Management Functions: fulfilled

[284] [selection: *choose one of: minimum, basic, detailed, not specified*]

[285] [selection: …] cf. the list of other events in the Protection Profile CSPPP

[286] [assignment: *other audit relevant information*]

FMT_MTD.1.1/Audit

The TSF shall restrict the ability to

(1) manual export,

(2) clear after manual export,

(3) select audited events in FAU_GEN.1,

(4) define the number of audit records causing automatic export and clearing of exported audit records according to FAU_STG.3.1 clause (1),

(5) define the percentage of storage capacity of audit records if actions are assigned in FAU_STG.3.1 clause (2)[287]

the audit records[288] to *Auditor*[289].

286 *Application Note 46:* The selection of auditable events according to FMT_MTD.1.1/Audit, clause (3) enables or disables or specifies the generation of audit records as defined in FAU_GEN.1. For security reasons the selection of auditable events according to clause (3) can only be done once and the functionality is then blocked for the remaining life cycle of the TOE. Clause (2) requires that the TOE only allow the deletion of the audit records after the current status of the audit records has been read out.

287 *Application Note 47:* Automatic export as defined in clause (4) is not possible on a typical smartcard or secure element hardware. The Auditor defines the maximum number of records to store. The threshold for automatic export of audit trails is therefore defined to be always higher than the number of records to store.

288 FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components

Dependencies: FAU_GEN.1 Audit data generation: fulfilled

FAU_STG.1.1

The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.1.2

The TSF shall be able to prevent[290] unauthorized modifications to the stored audit records in the audit trail.

289 FAU_STG.3 Action in Case of Possible Audit Data Loss

Hierarchical to: No other components

Dependencies: FAU_STG.1 Protected audit trail storage: fulfilled

FAU_STG.3.1

The TSF shall

(1) automatically export audit trails and clear automatically exported audit records[291] if the audit trail exceeds an *Auditor*[292] de-

[287] [selection: *change_default, query, modify, delete, clear,*[assignment: *other operations*]]

[288] [assignment: *list of TSF data*]

[289] [selection: *Auditor, Administrator*]

[290] [selection: *choose one of: prevent, detect*]

[291] [assignment: *actions to be taken in case of possible audit storage failure*]

fined number of audit records within [*maximum number of audit records+1.. maximum number of audit records+1*][293]

(2) ***blocks all TSF which possibly trigger an audit event*[294] if the audit trail exceeds an *Auditor*[295] settable percentage of storage capacity.**

290 **FPT_STM.1** **Reliable time stamps**

Hierarchical to: No other components

Dependencies: No dependencies

FPT_STM.1.1

The TSF shall be able to provide reliable time stamps **by means of** [296] ***internal clock with accuracy 10 percent*** [297] ***with the ability of adjustment of the clock by the TimeKeeper*** [298].

291 *Application Note 48:* The external trustable source (e.g. signed Network Time Protocol) provides a reliable time source for adjustment of the internal clock. The time intervals of adjustments in clause (2) may be configured by the administrator. Any adjustment or failure of adjustment of the internal clock is an auditable event according to FAU_GEN.1.1.The refinement with selection defines different cases for internal clocks and are therefore printed in bold.

292 **FPT_TIT.1/Audit** **TSF data integrity transfer protection – Audit functionality**

Hierarchical to: No other components

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

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

FPT_TIT.1.1/Audit

The TSF shall enforce the Update SFP, *Cryptographic Operation SFP* [299] to transmit[300] TSF data **audit records** in a manner protected from modification, deletion, insertion and replay[301] errors.

FPT_TIT.1.2/Audit

The TSF shall be able to determine on receipt of TSF data **time**, whether modification[302] has occurred.

[292] [selection: *Administrator, Auditor*]

[293] [assignment: *pre-defined range*]

[294] [assignment: *actions to be taken in case of possible audit storage failure*]

[295] [selection: *Administrator, Auditor*]

[296] [selection: *(1) internal clock with accuracy* [assignment: *approximate deviation*] *with the ability of adjustment of the clock by the* [selection: *Administrator, Timekeeper*], *(2) internal clock with accuracy* [assignment: *approximate deviation*] *with automatic adjustment of the clock by an externally trustable source in a cryptographically verifiable manner (e.g. by signed Network Time Protocol) and the ability of adjustment of the clock by the* [selection: *administrator, timekeeper*]]

[297] [assignment: *approximate deviation*]

[298] [selection: *administrator, timekeeper*]

[299] [selection: *Key Management SFP, Cryptographic Operation SFP*]

[300] [selection: *transmit, receive, transmit and receive*]

[301] [selection: *modification, deletion, insertion, replay*]

[302] [selection: *modification, deletion, insertion, replay*]

293 *Application Note 49:* The Update SFP is enforced by the export of audit records about import of UCP, cf. FAU_GEN.1.1 clause c) (2). The selection of the Key Management SFP or Cryptographic Operation SFP depends of the selection of auditable events of key management, cryptographic operations and adjustment of the internal clock (e. g. used for verification of validity time period) in FAU_GEN.1.1 clause c). The TSF transmits audit records and receives time as TSF data for security audit. The TSF protects the audit records by means of digital signature against modification and by means of time stamps and key usage counter of the signature key as part of the signature against deletion, insertion and replay as required in FPT_TIT.1.1.

6.1.10 Protection of the TSF

294 **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 *memory protected by PUF of the hardware*[303] **by encryption according to FCS_COP.1/SDE**.

295 *Application Note 50:* 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.

296 **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]: fulfilled
FCS_CKM.4 Cryptographic key destruction: fulfilled

FCS_CKM.1.1/SDEK

The TSF shall generate cryptographic **stored data encryption** key in accordance with a specified cryptographic generation key algorithm *PUF*[304] **using random bit generation according to FCS_RNG.1** and specified cryptographic key sizes *128 bit*[305] that meet the following: *[HWST]* [306].

297 **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

[303] [assignment: *memory area*]

[304] [assignment: *cryptographic key generation algorithm*]

[305] [assignment: *cryptographic key sizes*]

[306] [assignment: *list of standards*]

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

FCS_COP.1.1/SDE

The TSF shall perform stored data encryption and decryption[307] in accordance with a specified cryptographic algorithm *PUF*[308] and cryptographic key sizes *128 bit* [309] that meet the following: *[HWST]*[310].

298 *Application Note 51:* 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 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.

299 **FRU_FLT.2 Limited fault tolerance**

Hierarchical to: FRU_FLT.1 Degraded fault tolerance

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

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)[311].

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

301 *Application Note 52:* Environmental conditions include but are not limited to power supply, clock, and other external signals (e.g., reset signal) necessary for the TOE operation.

302 **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).

[307] [assignment: *list of cryptographic operations*]

[308] [assignment: *cryptographic algorithm*]

[309] [assignment: *cryptographic key sizes*]

[310] [assignment: *list of standards*]

[311] [assignment: *list of types of failures*]

303 **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.**

304 **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[312] to demonstrate the correct operation of *the Random Number Generator PTG.2 provided by the hardware*[313].

FPT_TST.1.2

The TSF shall provide authorized users with the capability to verify the integrity of TSF data[314].

FPT_TST.1.3

The TSF shall provide authorized users with the capability to verify the integrity of TSF **implementation**[315].

305 *Application Note 53:* Note that beside the Random Number Generator other parts of the TSF are tested periodically during normal operation as well. Nevertheless, this cannot be requested by the authorized user, except by a power reset. Due to this restriction only the RNG is included in FPT_TST.

306 **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[316] to the TSF implementation[317]

(2) perturbation and environmental stress[316] to the TSF[317] by responding automatically such that the SFRs are always enforced.

307 **Refinement: The TSF will implement appropriate mechanisms continuously to counter physical probing and manipulation.**

308 *Application Note 54:* “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

[312] [selection: *during initial start-up, periodically during normal operation, at the request of the authorized user, at the conditions*[assignment: *conditions under which self test should occur*]]

[313] [selection: [assignment: *parts of TSF*], *the TSF*]

[314] [selection: [assignment: *parts of TSF data*], *TSF data*]

[315] [selection: [assignment: *parts of TSF*], *TSF*]

[316] [assignment: *physical tampering scenarios*]

[317] [assignment: *list of TSF devices/elements*]

are 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.

6.1.11 Import and verification of Update Code Package

309 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.

310 Note that update packages can only be built by the developer of the TOE and not by the customer. The customer must coordinate the update strategy with the developer of the TOE in case of necessary updates.

311 **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]: fulfilled
[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]: fulfilled
FPT_TDC.1 Inter-TSF basic TSF data consistency: fulfilled

FDP_ITC.2.1/UCP

The TSF shall enforce the Update SFP [318] 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

[318] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]

FCS_COP.1/DecUCP[319].

312 **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[320] 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.

313 **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]: fulfilled
FCS_CKM.4 Cryptographic key destruction: fulfilled

FCS_COP.1.1/VDSUCP

The TSF shall perform verification of the digital signature of the authorized Issuer[321] in accordance with a specified cryptographic algorithm *ECDSA with brainpoolP512t1*[322] and cryptographic key sizes *512 bit* [323] that meet the following: [TCOSGD].[324].

314 *Application Note 55:* 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.

315 **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
FCS_CKM.1 Cryptographic key generation]: fulfilled

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

[320] [assignment: *list of TSF data types*]

[321] [assignment: *list of cryptographic operations*]

[322] [assignment: *cryptographic algorithm*]

[323] [assignment: *cryptographic key sizes*]

[324] [assignment: *list of standards*]

FCS_CKM.4 Cryptographic key destruction: fulfilled

FCS_COP.1.1/DecUCP

The TSF shall perform decryption of authentic encrypted Update Code Package[325] in accordance with a specified cryptographic algorithm *AES-256 in OFB mode*[326] and cryptographic key sizes *256 bit*[327] that meet the following: [*FIPS197*][328].

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

Hierarchical to: No other components

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

FDP_ACC.1.1/UCP

The TSF shall enforce the Update SFP[329] on

(1) subjects: *Update Agent*[330];
(2) objects: Update Code Package;
(3) operations: import, store[331].

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

Hierarchical to: No other components

Dependencies: FDP_ACC.1 Security attribute based access control: fulfilled
FMT_MSA.3 Static attribute initialization: not fulfilled, the security attributes of the UCP are imported according to FDP_ITC.2/UCP without default values

FDP_ACF.1.1/UCP

The TSF shall enforce the Update SFP[332] to objects based on the following:

(1) subjects: *Update Agent*[333]
(2) objects: Update Code Package with security attributes Issuer and Version Number[334].

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) *Update Agent*[333] is allowed to import Update Code Package according to FDP_ITC.2/UCP.
(2) *Update Agent*[333] is allowed to store Update Code Package if

[325] [assignment: *list of cryptographic operations*]

[326] [assignment: *cryptographic algorithm*]

[327] [assignment: *cryptographic key sizes*]

[328] [assignment: *list of standards*]

[329] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]

[330] [selection: *Administrator, Update Agent*]

[331] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]

[332] [assignment: access control SFP]

[333] [selection: *Administrator, Update Agent*]

[334] [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]

(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 the Version Number of the TSF[335].

FDP_ACF.1.3/UCP

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: *none* [336].

FDP_ACF.1.4/UCP

The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *none*[337].

318 **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**[338] the following objects: received Update Code Package[339].

6.2 Security Assurance Requirements for the TOE

319 The assurance requirements for the evaluation of the TOE, its development and operating environment are to choose as the predefined assurance package EAL4 augmented by the following components:

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

320 The Protection Profiles BSI-CC-PP0035 [ICPP] and BSI-CC-PP0104 [CSPPP] define refinements to the TOE Assurance Requirements, which are considered by the TOE Developer under the corresponding assurance packages.

6.3 Security Requirements Rationale

321 A detailed justification required for suitability of the security functional requirements to achieve the security objectives is given in the PP [CSPPP] and is therefore not repeated here.

[335] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]

[336] [assignment: *rules, based on security attributes, that explicitly authorize access of subjects to objects*]

[337] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]

[338] [selection: *allocation of the resource to, deallocation of the resource from*]

[339] [assignment: *list of objects*]

6.3.1 Rationale for SFR’s Dependencies

322 The following table provides an overview for security functional requirements coverage also giving an evidence for sufficiency and necessity of the SFRs chosen. It refers the corresponding Table of the Protection Profile [CSPPP]. Note that the SFRs and objectives related to the hardware ST are not considered here.

	O.I&A	OT.AuthentTOE	O.Enc	O.DataAuth	O.RBGS	O.TChann	O.AccCtrl	O.SecMan	O.PhysProt	O.TST	O.SecUpCP	O.Audit	O.TimeService
FAU_GEN.1												x	
FAU_STG.1												x	
FAU_STG.3												x	
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													
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							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		
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/TS													x
FDP_ACF.1/UCP											x		
FDP_DAU.2/Att	x												

	O.I&A	OT.AuthentTOE	O.Enc	O.DataAuth	O.RBGS	O.TChann	O.AccCtrl	O.SecMan	O.PhysProt	O.TST	O.SecUpCP	O.Audit	O.TimeService
FDP_DAU.2/Sig				X									
FDP_DAU.2/TS												X	x
FDP_ETC.1				x									
FDP_ETC.2			x	x									
FDP_ETC.2/TS													x
FDP_ITC.2/TS													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								x				
FIA_UAU.5	x					x							
FIA_UAU.6	x												
FIA_UID.1	x												
FIA_USB.1	x												
FMT_MOF.1	x					x							
FMT_MOF.1/TSA													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/Audit												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					
FMT_SMF.1/TSA												x	x
FMT_SMR.1/TSA												x	x
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_STM.1												x	x
FPT_TCT.1/CK								x			x		
FPT_TDC.1/Cert	x		x	x				X					
FPT_TDC.1/CK								X					
FPT_TDC.1/UCP											x		
FPT_TIT.1/Audit								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 2: SFR coverage

323 The dependency analysis for the security functional requirements given in the corresponding Table of the Protection Profile [CSPPP] shows that the mutual support and internal consistency between all defined functional requirements is satisfied or justified.

6.3.2 Security Assurance Requirements Rationale

324 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.

325 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.

326 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.

327 The set of *assurance* components being part of EAL4 fulfils all dependencies a priori.

328 The component AVA_VAN.5 has the following dependencies: ADV_ARC.1, ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, AGD_OPE.1, AGD_PRE.1, and ATE_DPT.1. All of these are met or exceeded in the EAL4 assurance package.

329 The component ALC_DVS.2 has no dependencies.

7 TOE Summary Specification

330 This section presents an overview of the security functionalities implemented by the TOE and the assurance measures applied to ensure their correct implementation.

331 According to the SFRs the TOE provides the following functionalities

- Key Management
- Data Encryption
- Hybrid Encryption with User Data Authentication
- Data Integrity Mechanisms
- Authentication and Attestation of the TOE, Trusted Channel
- User Identification and Authentication
- Access Control
- Security Management
- Security Audit
- Protection of the TSF
- Import and Verification of Update Code Package

332 According to the Protection Profiles [CSPPP] and [CSPMOD] all security function are supported by the coordinated and matching SFRs. In the following the SFRs are associated to security functions implemented by the TOE.

7.1 Key Management

333 The TSFRs FDP_ACC.1/KM, FMT_MSA.1/KM, FMT_MSA.3/KM and FMT_MTD.1/KM require the TOE to implement several management functions on/with the cryptographic keys and enforce the access control security functional policies of subject on the objects (cryptographic keys). The TOE implements the functionality via the Export Key, Import Key and key management commands.

334 The TOE implements the cryptographic algorithm SHA-256, SHA-384, SHA-512 (FCS_COP.1/Hash). 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. Additionally the Hash-function is directly usable via the PSO:Hash – command.

335 The root key of a public key infrastructure (PKI)s imported via a link certificate using the Verify Certificate command. While verifying the command assures the requirements of FPT_TIT.1/Cert, FPT_ISA.1/Cert and FPT_TDC.1/Cert.

336 The TOE provides a hybrid deterministic random number generator of class DRG.4 and PTG.2 according to [AIS31] (FCS_RNG.1).

337 The TOE implements cryptographic checksum functions, including hash functions used for signature verification and key generation and derivation and message authentication codes (MACs) addressed by FCS_COP.1.

338 The TOE provides the symmetric encryption algorithm AES with standardized key lengths of 128 and 256 bits (FCS_COP.1).

339 The TOE implements asymmetric crypto algorithms used for encryption/decryption, key agreement and digital signatures based elliptic curves.

340 Cryptographic functions are necessary for different security protocols implemented by the TOE, e.g. PACE, Chip and Terminal Authentication, key derivation or the Update procedure.

341 Cryptographic keys are explicitly deleted by overwriting the memory data with zeros or random numbers, e.g. the new key according to FCS_CKM.4.

342 SFRs supporting cryptographic functions are listed below:

- FCS_RNG.1
- FCS_CKM.1/AES
- FCS_CKM.5/AES
- FCS_CKM.1/ECC
- FCS_CKM.5/ECC
- FCS_CKM.1/RSA
- FCS_CKM.5/ECDHE
- FCS_CKM.1/ECKA-EG
- FCS_CKM.5/ECKA-EG
- FCS_CKM.1/AES_RSA
- FCS_CKM.5/AES_RSA
- FCS_CKM.4

343 The TOE implements function to securely export and import cryptographic keys keeping integrity, authenticity and confidentiality. Exported key (via Export Key – command) can only be imported by the TOE sample which has exported the key because every sample maintains its own key-wrap key.

344 SFRs supporting export/import are listed below:

- FCS_COP.1/KW
- FCS_COP.1/KU
- FPT_TCT.1/CK
- FPT_TIT.1/CK
- FPT_ISA.1/CK
- FPT_TDC.1/CK
- FPT_ESA.1/CK

7.2 Data Encryption

345 The TOE provides the symmetric encryption algorithm AES with standardized key lengths of 128 and 256 bits (FCS_COP.1/ED). The functionality is available via a self-contained command PSO:Encipher/Decipher.

7.3 Hybrid Encryption with MAC for User Data

346 The TOE provides hybrid data encryption/decryption and MAC calculation/verification of user data as required in AES FCS_COP.1/HEM and FCS_COP.1/HDM. The functionality is available over the TSFI PSO:Encipher and PSO:Decipher.

7.4 Data Integrity Mechanisms

347 The TOE implements cryptographic checksum functions, including hash functions used for message authentication codes (MACs) addressed by FCS_COP.1/MAC and FCS_COP.1/HMAC. The functionality is available via the TSFI PSO:Verify Cryptographic Checksum and PSO:Compute Cryptographic Checksum.

348 Digital signature generation and verifications as required by FCS_COP.1/CDS-ECDSA, FCS_COP.1/VDS-ECDSA, FCS_COP.1/CDS-RSA, FCS_COP.1/VDS-RSA, FDP_DAU.2/Sig and FDP_DAU.2/TS is implemented by the TOE and reachable via the commands PSO:Compute Digital Signature and PSO:Verify Digital Signature.

7.5 Authentication and Attestation of the TOE, Trusted Channel

349 The secure data exchange in a trusted channel is required by FTP_ITC.1. It is supported by cryptographic operations. The TOE enforces a protected communication by means of the PACE or Chip Authentication protocol. The trusted channel supports confidential information exchange which integrity is assured.

350 The randomness of the parameters of the PACE protocol is guaranteed by the RNG class DRG.4 (FCS_RNG).

351 The strength of algorithms for ensuring confidentiality and integrity is supplied by FCS_COP.1.

352 The TOE supports attestation to ensure that the sample is a genuine sample of the certified product via the command Compute Attestation.

353 The SFRs supporting Authentication and Attestation are listed below:

- FIA_API.1/PACE
- FIA_API.1/CA
- FDP_DAU.2/Att
- FTP_ITC.1
- FCS_CKM.1/PACE
- FCS_CKM.1/TCAP
- FCS_COP.1/TCE
- FCS_COP.1/TCM

7.6 User Identification and Authentication

354 The protocols for identification and authentication of users and devices are described in the TCOS Guidance [TCOSGD]. The roles assigned after successful authentication are listed in FMT_SMR.1 and its iterations.

355 The security and the reliability of the identification and authentication are supported by the correct key agreement (FIA_UAU.1, FIA_UAU.5 and FIA_UAU.6) and the quality of random numbers (FCS_RNG.1). As soon the authentication state is left, the session keys cannot be used anymore (FCS_CKM.4).

356 User is authenticated with means of PACE passwords and PINs represented on the TOE by ADRs, which are bound by corresponding failure or usage counters (FIA_AFL.1). A Terminal is authenticated by using a correct key derived from the provided certificate and the authentication context.

357 Before a user or device is identified only dedicated commands can be executed. This is supported by the iterated SFRs FIA_UID.1.

358 The SFRs supporting identification and authentication are listed below:

- FIA_ATD.1
- FMT_MTD.1/RAD
- FMT_MTD.3
- FIA_USB.1
- FMT_SAE.1
- FIA_UID.1
- FIA_UAU.1
- FIA_UAU.5
- FIA_UAU.6

7.7 Security Management

359 The TOE supports the management of security functions and its behavior. Password can be changed and modified via Change Reference Data and Reset Retry Counter command. Cryptographic keys are managed by using the command Manage Key.

360 The internal clock can be adjusted via the command ManageTime. The behavior of the audit functions can be changed using the command Manage Audit Functions.

361 The SFRs supporting security management are listed below:

- FMT_SMF.1
- FMT_SMR.1
- FMT_MSA.2
- FMT_MOF.1
- FMT_SMF.1/TSA
- FMT_SMR.1/TSA

- FMT_MOF.1/TSA

7.8 Access Control

362 The access to User Data is restricted according to the different iterations of the SFRs FDP_ACC.1 and FDP_ACF.1.

363 The access to the TOE security functions and the TSF data is controlled by the functionality of the class FMT.

364 User data are imported as required by FDP_ITC.2/UD via the command PSO:Encipher/Decipher and PSO:CDS respective PSO:VDS.

365 User data are exported as required by FDP_ETC.1 and FDP_ETC.2 via the command PSO:Encipher/Decipher and PSO:CDS respective PSO:VDS.

366 The SFRs supporting identification and authentication are listed below:

- FDP_ITC.2/UD
- FDP_ITC.2/TS
- FDP_ETC.2
- FDP_ETC.2/TS
- FDP_ETC.1
- FDP_ACC.1/Oper
- FDP_ACF.1/Oper
- FDP_ACF.1/TS

7.9 Security Audit

367 The TOE supports audit data generation on occurrence of several auditable events. Event data are stored in an audit trail and can be exported later via the command GetAuditData. Exported audit trails are digitally signed. Therefore modification, deletion, insertion and replay can be easily determined. Events can be activated and deactivated by using the command ManageAuditFunctions.

368 The SFRs supporting identification and authentication are listed below:

- FAU_GEN.1
- FMT_MTD.1/Audit
- FAU_STG.1
- FAU_STG.3
- FPT_STM.1
- FPT_TIT.1/Audit

7.10 Protection of the TSF

369 According to the SFRs FDP_ACC.1 and FDP_ACF.1 and their iterations the access to cryptographic keys is restricted by defined rules laid down in the certified object system. The details can be found in the corresponding SFPs. Note that the TOE enforces these access rules based on roles taken by authentication against the corresponding ADR, but there is no a priori protection of a said object. Some of the roles can also be taken by verifying certificates followed by authentication to the corresponding imported public key ADR. The TOE is able to interpret these certificates accordingly.

370 Data stored on the TOE is protected by FDP_SDC.1, FCS_COP.1/SDE and FCS_CKM.1/SDEK which is implemented by using the hardware features of the chip.

371 Residual information of sensitive data in previously used resources will not be available after its usage (FDP_RIP.1/UCP). Session keys and message authentication keys will be destroyed after reset or termination of the secure messaging channel (FCS_CKM.4). The TOE hides the correlation of power or timing variations and the command execution accessing sensitive user data as different keys and passwords (FPT_EMS.1). In case of a malfunction, operating errors or integrity check failures the TOE enters a secure state (FPT_FLS.1). This is supported by the functional services of the hardware.

372 The TOE executes self-tests (FPT_TST.1) to demonstrate the correct operation of the TSF and its confidentiality protection capabilities. In case of failures, FPT_FLS.1 requires the preservation of a secure state in order to protect the user data, TSF data and security services. FRU_FLT.2 ensures the operation of all the TOE's capabilities when an exposure to operating conditions which are not detected according to the previous requirement occurs.

373 The SFRs supporting protection of the TOE are listed below:

- FDP_DAU.2/Sig
- FMT_MSA.1/KM
- FMT_MSA.2
- FMT_MSA.3/KM
- FMT_MTD.1/KM
- FMT_MTD.1/RAD
- FMT_MTD.1/RK
- FMT_MTD.3

7.11 Import and Verification of Update Code Package

374 The TSFR in this group require the functionality to load update code packages in the TOE in operational phase. The TOE implements this via the commands Application Management Request and Load Application.

375 The SFRs supporting Import and Verification of Update Code Package are listed below:

- FDP_ITC.2/UCP
- FPT_TDC.1/UCP
- FCS_COP.1/VDSUCP
- FCS_COP.1/DecUCP

- FDP_ACC.1/UCP
- FDP_ACF.1/UCP
- FDP_RIP.1/UCP

7.12 Statement of Compatibility

376 This is the statement of compatibility between this Composite Security Target and the Security Target Chip of the underlying hardware [HWST].

7.12.1 Relevance of Hardware TSFs

377 In the following lists the relevance of the hardware security services (SS) and functions (SF) for the composite security target is considered.

Relevant:

- SS.RNG: Random Number Generator
- SS.AES: AES Co-processor
- SS.CRC: Cyclic Redundancy Check
- SF.OPC: Control of Operating Conditions
- SF.PHY: Protection against Physical Manipulation
- SF.PUF: User Data Protection using PUF
- SF.LOG: Logical Protection
- SF.MEM_ACC: Memory Access Control
- SF.SFR_ACC: Special Function Register Access Control

Not relevant:

- SS.TDES: Triple-DES (TDES) Co-processor
- SS.RECONFIG: Customer Reconfiguration
- SF.COMP: Protection of Mode Control
- SF.FFW: Firmware Firewall
- SF.FIRMWARE: Firmware Support

7.12.2 Security Requirements

Security Functional Requirements

378 The relevant Security Requirements of the TOE and the hardware can be mapped or are not relevant. They show no conflict between each other.

Security Requirements of the TOE related to the Composite ST:

379 The Security Requirements of the TOE of the classes FAU, FCS, FIA, FDP, FMT and FTP are specific for the Operating System and have no conflicts with the underlying hardware.

380 The Security Requirements of the TOE of the classes FPT, FRU are supported by the Security Feature SF.PHY and SF.OPC of the hardware ([HWST]). The requirements FPT_FLS and FPT_PHP are also not conflicting with the requirements for the hardware. They support each other. The requirements for test (FPT_TST) in the operating system

are supported by various tests of the hardware, and there are no conflicts with the underlying hardware.

Security Requirements of the hardware

381 The Security Requirements of the TOE's hardware based on PP-0084 [ICPP, sec.6.1] can be mapped to Security Requirements of the TOE. They show no conflict between each other.

- FAU_SAS.1[HW] is not relevant because it concerns internal audit data handling for initialization- and pre-personalization-data
- FDP_IFC.1 is not relevant because it concerns information flow policy between parts of the hardware
- FDP_SDC.1, FDP_SDI.2 concerns low level stored data protection (confidentiality, integrity) and is covered by FDP_SDC.1, FCS_CKM.1/SDEK and FCS_COP.1/SDE of the composite ST.
- FDP_ITT.1 is not relevant because it concerns basic internal transfer protection of the hardware
- FMT_LIM.1[HW] and FMT_LIM.2[HW] is not relevant because it concerns limited capabilities and availability of Deploying Test Features of the hardware
- FRU_FLT.2 is covered by FRU_FLT.2 of the composite ST
- FPT_FLS.1 is covered by FPT_FLS.1 of the composite ST
- FPT_ITT.1 is not relevant because it concerns basic hardware internal TSF data transfer protection
- FPT_PHP.3 concerns the resistance to physical attacks and is covered by FPT_PHP.3 of the composite ST

382 The additional Security Requirements of the TOE's hardware defined in [HWST] can be mapped to Security Requirements of the TOE too. They show no conflict between each other.

- FCS_CKM.1[PUF], FCS_CKM.4[PUF], FCS_COP.1[PUF_AES], FCS_COP.1\[PUF_MAC]: concerns internal data protection and is covered by FDP_SDC.1, FCS_CKM.1/SDEK and FCS_COP.1/SDE of the composite ST.
- FCS_COP.1[AES]: covered by FCS_CKM.1/AES.
- FCS_CKM.4[TDES]: is not used in this TOE.
- FCS_COP.1[TDES]: is not used in this TOE.
- FCS_RNG.1[HW]: matches FCS_RNG.1 of the Composite ST
- FDP_ACC.1 concerns the Memory Access Control Policy on software tasks accessing assigned data in memories, this is covered by FDP_ACC.1 and its iterations of the Composite TOE
- FDP_ACF.1 concerns the Memory Access Control Policy on software tasks accessing assigned data in memories, this is covered by FDP_ACC.1 and its iterations of the Composite TOE.
- FDP_SDI.2[HW, FW, EEPROM, RAM, ROM] concerns low level stored data protection and monitoring and does not conflict with the requirements of this ST.
- FMT_MSA.1 concerns the management of security attributes on hardware's level, does not conflict with the SFRs of the TOE
- FMT_MSA.3 concerns the management of security attributes on hardware's level, does not conflict with the SFRs of the TOE
- FMT_SMF.1 concerns the access of the configuration registers of the Memory Management Unit, does not conflict with the SFRs of the TOE

Security Assurance Requirements

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

384 The chosen level of assurance of the hardware is EAL 6 augmented with ALC_FLR.1 and ASE_TSS.2. This includes ALC_DVS.2 and AVA_VAN.5.

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

7.12.3 Security Objectives

386 The Security Objectives of the TOE and the hardware can be mapped or are not relevant. They show no conflict between each other.

387 The following Security Objectives of the TOE are related to the Composite ST and are not relevant for the hardware:

- O.AccCtrl
- O.AuthentTOE
- O.DataAuth
- O.SecMan
- O.SecUpCP
- O.TChann
- O.Audit
- O.TimeService

388 Security Objectives of the TOE related to the Composite ST, that can be mapped to Objectives of the hardware:

- O.PhysProt
- O.RBGS
- O.TST
- O.Enc
- O.I&A

389 The following Security Objectives of the Hardware are covered by objectives of the TOE

- O.Leak-Forced, O.Leak-Inherent and O.PUF are covered by O.PhysProt
- O.Abuse-Func, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation are covered by O.TST
- O.RND is covered by O.RBGS
- O.AES is covered by O.Enc
- O.Identification is covered by O.I&A

390 The remaining objectives of the hardware concern the internal processing of the hardware and are not related to specific objectives of the TOE. They do not conflict to each other:

- O.CUST_RECONF_PLAIN
- O.EEPROM_INTEGRITY

- O.FM_FW
- O.MEM_ACCESS
- O.SFR_ACCESS
- O.TDES

391 The Security Objectives for the Environment of the TOE are related to the life cycle phase “Operational Use” and do not conflict with the Security Objectives for the hardware which are related to the manufacturing process. Therefore, they do not conflict to each other.

392 Security Objective for the environment of TOE’s hardware:

- OE.Resp-Appl
- OE.Process-Sec-IC

393 Security Objective for the environment of composite TOE:

- OE.CommInf
- OE.AppComp
- OE.SecComm
- OE.SUCP
- OE.Audit
- OE.TimeSource

7.12.4 Conclusion

394 No contradictions between the Security Targets of the TOE and the underlying hardware can be found.

7.13 Assurance Measures

395 The documentation is produced compliant to the Common Criteria Version 3.1. The following documents provide the necessary information to fulfil the assurance requirements listed in section 6.2 Security Assurance Requirements for the TOE.

Development
ADV_ARC.1 Security Architecture Description TCOS CSP 1.0 Release 1
ADV_FSP.4 Functional Specification TCOS CSP 1.0 Release 1
ADV_IMP.1 Implementation of the TSF TCOS CSP 1.0 Release 1
ADV_TDS.3 Modular Design of TCOS CSP 2.0 Release 1

Guidance documents
AGD_OPE.1 User Guidance TCOS CSP 2.0 Release 1
AGD_PRE.1 Administrator Guidance TCOS CSP 2.0 Release 1

Life-cycle support
ALC_CMC.4, ALC_CMS.4 Documentation for Configuration Management
ALC_DEL.1 Documentation for Delivery and Operation
ALC_LCD.1 Life Cycle Model Documentation TCOS CSP 2.0 Release 1
ALC_TAT.1, ALC_DVS.2 Development Tools and Development Security for TCOS CSP 2.0 Release 1

Tests
ATE_COV.2, ATE_DPT.2 Test Documentation for TCOS CSP 2.0 Release 1

ATE_FUN.1 Test Documentation of the Functional Testing

Vulnerability assessment

AVA_VAN.5 Independent Vulnerability Analysis TCOS CSP 2.0 Release 1

396 The developer team uses a configuration management system that supports the generation of the TOE. The configuration management system is well documented and identifies all different configuration items. The configuration management tracks the implementation representation, design documentation, test documentation, user documentation, administrator documentation, and security flaws. The security of the configuration management is described in detail in a separate document.

397 The delivery process of the TOE is well defined and follows strict procedures. Several measures prevent the modification of the TOE based on the developer's master copy and the user's version. The Administrator and the User are provided with necessary documentation for installation, personalization and start-up of the TOE.

398 The implementation is based on an informal high-level and low-level design of the components of the TOE. The description is sufficient to generate the TOE without other design requirements.

399 The tools used in the development environment are appropriate to protect the confidentiality and integrity of the TOE design and implementation. The development is controlled by a life-cycle model of the TOE. The development tools are well-defined and use semiformal methods, i.e. a security model.

400 The development department is equipped with organizational and personnel means that are necessary to develop the TOE. The testing and the vulnerability analysis require technical and theoretical know-how available at T-Systems International GmbH.

401 As the evaluation is identified as a composite evaluation based on the CC evaluation of the hardware, the assurance measures related to the hardware (IC) will be provided by documents of the IC manufacturer.

Appendix: Keywords and Abbreviations

402 The terminology and abbreviations of Common Criteria version 3.1 [CC], Revision 5 apply to this ST. The following table is taken over from the PP [CSPPP]

Term	Description
authentication reference data	data used by the TOE to verify the authentication attempt of a user
authentication verification data	data used by the user to authenticate themselves to the TOE
authenticity	the property that ensures that the identity of a subject or resource is the one claimed (cf. ISO/IEC 7498-2:1989)
cluster	a system of TOE samples initialized by an administrator and communication through trusted channels in order to manage known users and to share the cryptographic keys
cryptographic key	a variable parameter which is used in a cryptographic algorithm or protocol
data integrity	the property that data has not been altered or destroyed in an unauthorized manner (cf. ISO/IEC 7498-2:1989)
firmware	executable code that is stored in hardware and cannot be dynamically written or modified during execution while operating on a non-modifiable or limited execution platform, cf. ISO/IEC 19790
hardware	physical equipment or comprises the physical components used to process programs and data or to protect physically the processing components, cf. ISO/IEC 19790
Issuer of update code package	Trusted authority issuing an update code package (UCP) and holding the signature private key for signing the UCP and corresponding to the public key implemented in the TOE for verification of the UCP. The issuer is typically the TOE manufacturer. The issuer of an UCP is identified by the security attribute Issuer of the UCP.
private key	confidential key used for asymmetric cryptographic mechanisms like decryption of cipher text, signature-creation or authentication proof, where it is difficult for the adversary to derive the confidential private key from the known public key
public key	public known used for asymmetric cryptographic mechanisms like encryption of cipher text, signature-verification or authentication verification, where it is difficult for the adversary to derive the confidential private key from the known public key
secret key	key of symmetric cryptographic mechanisms, using two identical keys with the same secret value or two different values, where one may be easy calculated from the other one, for complementary operations like encryption / decryption, signature-creation / signature-verification, or authentication proof / authentication verification.
secure channel	a trusted channel which is physically protected and logical separated communication channel between the TOE and the user, or is protected by means of cryptographic mechanisms
software	executable code that is stored on erasable media which can be dynamically written and modified during execution while operating on a modifiable execution platform, cf. ISO/IEC 19790
trusted channel	a means by which a TSF and another trusted IT product can communicate with necessary confidence (cf. CC part 1 [1], paragraph 97)
update code package	code if implemented changing the TOE implementation at the end of the TOE life time

Acronym	Term
A.xxx	Assumption
CC	Common Criteria
CSP	Cryptographic Service Provider
ECC	Elliptic curve cryptography
HMAC	Keyed-Hash Message Authentication Code
KDF	Key derivation function
MAC	Message Authentication Code
n. a.	not applicable
O.xxx	Security objective for the TOE
OE.xxx	Security objective for the TOE environment
OSP.xxx	Organizational security policy
PACE	Password Authenticated Connection Establishment
PKI	Public Key Infrastructure
PP	Protection Profile
SAR	Security Assurance Requirements
SFR	Security Functional Requirement
T.xxx	Threat
TOE	Target of Evaluation
TSF	TOE Security Functionality
UCP	Update Code Package

References

[AIS31]

Bundesamt für Sicherheit in der Informationstechnik, Anwendungshinweise und Interpretationen zum Schema (AIS), AIS 31, A proposal for Functionality classes for random number generators Version 2.0 vom 18.09.2011, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[AIS36]

Bundesamt für Sicherheit in der Informationstechnik, Anwendungshinweise und Interpretationen zum Schema (AIS), AIS 36, Version 2 vom 12.11.2007, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[ANSX9.63]

American National Standard X9.63-2001, Public Key Cryptography for the Financial Services Industry, Key Agreement and Key Transport Using Elliptic Curve Cryptography, 2005-11

[CC]

Common Criteria for Information Technology Security Evaluation, Version 3.1,

Part 1: Introduction and general model; Version 3.1, April 2017, CCMB-2017-04-001,
Part 2: Security functional components; Version 3.1, April 2017, CCMB-2017-04-002,
Part 3: Security assurance components; Version 3.1, April 2017, CCMB-2017-04-003

Common Methodology for Information Technology Security Evaluation, Evaluation methodology, Version 3.1, April 2017, CCMB-2017-04-004

[EACTR]

Technical Guideline TR-03110: Advanced Security Mechanisms for Machine Readable Travel Documents,

Part 1 – eMRTDs with BAC/PACEv2 and EACv1,

Part 2 – Extended Access Control Version 2 (EACv2), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI),

Part 3 – Common Specifications, Version 2.10, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2012-03

[ECCTR]

Technical Guideline TR-03111: Elliptic Curve Cryptography, Version 2.0, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2012-08

[SE API]

Technical Guideline TR-03151: Secure Element API (SE API) Version 1.0.0, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2018-06

[FIPS180]

Federal Information Processing Standards Publication FIPS PUB 180-4, Secure Hash Standard (SHS), 2012-03

[FIDO]

FIDO Alliance Proposed Standard FIDO ECDAA Algorithm, FIDO Alliance, 2017-04

[FIPS186]

Federal Information Processing Standards Publication FIPS PUB 186-4, Digital Signature Standard (DSS), 2013-07

[FIPS197]

Federal Information Processing Standards Publication 197, Advanced Encryption Standard (AES), U.S. Department of Commerce/National Institute of Standards and Technology, 2001-11-26

[ISO18033-3]

ISO/IEC 18033-3:2010 Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers, ISO, 2010-12

[HWCR]

Certification Report of the underlying hardware platform, BSI-DSZ-CC-1059-2018 for NXP Secure Smart Card Controller P6022y VB including IC Dedicated Software from NXP Semiconductors Germany GmbH, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2018-05

[HWST]

Security Target of the underlying hardware platform, NXP Secure Smart Card

Controller P6022y VB, Security Target Lite Version 2.1, BSI-DSZ-CC-1059-V2, NXP Semiconductors, 2018-11

[ICAO9303]

ICAO Doc 9303, Machine Readable Travel Documents, Seventh Edition, 2015

[ISO7816]

ISO 7816-4:2013, Identification cards – Integrated circuit cards with contacts, Part 4: Organization, security and commands for interchange, ISO, 2013-04

[ISO9796-2]

ISO/IEC 9796-2:2010 Information technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms, ISO, 2010-12

[ISO9797-1]

ISO/IEC 9797-1:1999, Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher, ISO, 2005-01-04

[ISO9797-2]

ISO/IEC 9797-2:2011, Information technology – Security techniques – Message Authentication Codes (MACs) – Part 2: Mechanisms using a dedicated hash-function, ISO, 2011-05

[ISO10116]

ISO/IEC 10116:2017, Information technology – Security techniques – Modes of operation for an n-bit block cipher, 2017-07

[ISO14888-2]

ISO/IEC 14888-2:2008, Information technology – Security techniques – Digital signatures with appendix – Part 2: Integer factorization based mechanisms, ISO, 2008-04

[CSPPP]

CC Protection Profile Cryptographic Service Provider, Version 0.9.8, Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik under BSI-CC-PP-0104-2019, 2019-02

[CSPMOD]

Protection Profile-Module CSP Time Stamp Service and Audit (PPM-TS-Au), Version 0.9.5, Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik under BSI-CC-PP-0107-2019, 2019-05

[JIL]

CC Joint Interpretation Library, Guidance for smartcard evaluation, Version 2.0, CCDB-2010-03-001, 2010-02

[ICPP]

Security IC Platform Protection Profile with Augmentation Packages Version 1.0, Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik under BSI-CC-PP-0084-2014, 2014-01

[RFC2104]

Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, IETF, 1997-02

[RFC5639]

M. Lochter, J. Merkle, Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, RFC 5639, IETF, 2010-03

[RFC5903]

D. Fu, J. Solinas, Elliptic Curve Groups modulo a Prime (ECP Groups) for IKE and IKEv2, RFC 5903, IETF, 2010-06

[RFC6954]

M. Lochter, J. Merkle, Using the Elliptic Curve Cryptography (ECC) Brainpool Curves for the Internet Key Exchange Protocol Version 2 (IKEv2), RFC 6954, IETF, 2013-07

[RFC8017]

K. Moriarty, B. Kaliski, J. Jonsson, A. Rusch, PKCS #1: RSA Cryptography Specifications Version 2.2, RFC 8017, IETF, 2016-11

[SP800-38A]

Recommendation for Block Cipher Modes of Operation: Methods and Techniques, NIST Special Publication 800-38A, National Institute of Standards and Technology, 2001-12

[SP800-38B]

Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, NIST Special Publication 800-38B, National Institute of Standards and Technology, 2005-05

[SP800-38D]

Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, NIST Special Publication 800-38D, National Institute of Standards and Technology, 2007-11

[SP800-56C]

Recommendation for Key-Derivation Methods in Key-Establishment Schemes Rev.1, NIST Special Publication 800-56C, National Institute of Standards and Technology, 2018-04

[TPM]

Trusted Platform Module Library, Part 1: Architecture, Family “2.0”, Level 00 Revision 01.38, TCG, 2016-09

[SP800-38F]

Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping, NIST Special Publication 800-38F, National Institute of Standards and Technology, 2012-12

[SP800-67]

Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, NIST Special Publication 800-67, Revised January 2012, National Institute of Standards and Technology, 2012-01

[TCOSGD]

Administrator’s Guidance TCOS CSP Version 1.0 Release 1, T-Systems International GmbH, Version 1.0, 2020-02

[TR02102]

Technische Richtlinie TR-02102-1 Kryptographische Verfahren Empfehlungen und Schlüssellängen, Version 2019-01, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2019-02

[BIP32]

Bitcoin Improvement Proposal number 32: “Hierarchical Deterministic Wallets”, 11. February 2012

https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki

[NIST SP 800-108]

NIST Special Publication 800-108: “Recommendation for Key Derivation Using Pseudorandom Functions”, October 2009