Rambus

Security IP
PKE Core Version 4.1

Common Criteria Security Target Lite

Document Revision: D
Document Date: 2023-12-08
Document Number: 001-029410-503/004
Document Status: Accepted

Rambus Inc. Corporate Headquarters
4453 North First Street, Suite 100
San Jose, CA 95134
USA
Phone: +1 408-462-8000
Website : https://www.rambus.com/
Contact : sipsupport@rambus.com

Table of Contents

List of Tables

List of Figures

Document Revision History

Doc Rev	Page(s) Section(s)	Date (Y-M-D)	Author	Purpose of Revision
A	All	2023-08-01	Rambus	Initial version derived from full ST
B	2.6	2023-12-01	Rambus	Update non-TOE components
C	1.2, 2.3, 2.4, 7.1, 7.3, 8.3	2023-12-04	Rambus	Correct USG reference, update SW delivery component from ST
D	1.2	2023-12-08	Rambus	USG date update

1 About this Document

1.1 Scope

This Security Target (ST) identifies the security properties of the TOE and defines the scope of the evaluation.

1.2 References

Document	Title
[CC]	Common Criteria for Information Technology Security Evaluation - Part 1: Security assurance components, CCMB-2017-04-001, Version 3.1 Revision 5
	Common Criteria for Information Technology Security Evaluation - Part 2: Security assurance components, CCMB-2017-04-002, Version 3.1 Revision 5
	Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components, CCMB-2017-04-003, Version 3.1 Revision 5
	Common Criteria for Information Technology Security Evaluation – Evaluation methodology, CCMB-2017-04-0004, Version 3.1 Revision 5
[PP]	Security IC Platform Protection Profile with Augmentation Packages, BSI-CC-PP-0084-2014, Version 1.0
[ISO 14888-3]	ISO/IEC 14888-3-2013 Information technology – security techniques – Digital signatures with appendix – Part 2: Discrete logarithm based mechanisms, 2015
[FIPS 186-4]	FIPS PUB 186-4-2013: Digital Signature Standard, Federal Information Processing Standards publication, 2013, July, National Institute of Standards and Technology
[FIPS 140-2]	FIPS PUB 140-2, Security Requirements for Cryptographic Modules, National Institute of Standards and Technology (NIST), up to change notice December 3, 2002
[ANSI X9.62]	ANSI X9.62-2005: Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA) November 15, 2005, American National Standards Institute
[ANSSI]	Avis Relatif Aux Parametres de courbes elliptiques definis par lÉtat francais, Journal Officiel de la Republique Francaise, 2011, JORF n 0241 du 16 Octobre 2011, page 17533
[SM2]	"GB/T 32918: Information Security Technology – Public Key cryptographic algorithm SM2 based on elliptic curves" • Part 1: General, August 2016 (GBT 32918.1-2016) • Part 2: Digital signature algorithm, August 2016 (GBT 32918.2-2016) • Part 3: Key exchange protocol, August 2016 (GBT 32918.3-2016) • Part 4: Public key encryption algorithm, August 2016 (GBT 32918.4-2016) • Part 5: Parameter definition, May 2017 (GBT 32918.5-2017)
[SM2 TR]	Chinese Commercial Cryptography Administration office, SM2: A group of ECC public key algorithms. Technical report, CC-CAO, 2010
[RFC 5639]	Elliptic Curve Cryptography (ECC) Brainpool standard Curves and Curve generation, RFC 5639 (Informational), Manfred Lochter and Johannes Merkle, 2010
[ISO 11770-3]	ISO/IEC 11770-3-2021: Information security – key management – Part 3: Mechanisms using asymmetric techniques part3: October 2021
[ANSI X9.63]	ANSI X9.63 Public Key Cryptography for the financial services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography, December 2011, American National standards
[RFC 7748]	IETF RFC 7748, Elliptic curves for security, January 2016, Internet Research Task Force (IRTF)
[NIST SP 800-186]	NIST SP 800-186, Recommendations for Discrete Logarithm-Bases Cryptography: Elliptic Curve Domain parameters, October 2019

[Ed448]	Ed448-Goldilocks, A new elliptic curve, M. Hamburg, NIST ECC workshop 2015, Cryptology ePrint Archive : Report 2015/625
[Curve 25519]	Curve 25519 : New Diffie-Hellman speed records, D.J. Bernstein, Proceedings of PKC2006, 2006/02/09
[RFC 8032]	IETF RFC 8032: Edwards-Curve digital Signature algorithm (EDDSA), January 2017, Internet Research Task Force (IRTF)
[PKCS#1]	PKCS#1 v2.2 RSA cryptography standards, October 2021, RSA Laboratories
[KS2011]	A proposal for Functionality classes for random number generators (Version 2.0, 18 September 2011, part of AIS 20 / 31)
[ERS]	Rambus, PKE v4.1 External Reference Specification, Document Number 007-029410-222, Revision A, Date 2021-01-12
[ITG]	Rambus, PKE v4.1 Integration and Testing Guide, Document Number 007-029410-228, Revision A, Date 2021-01-12
[USG]	Rambus, PKE v4.1 User Security Guidance, Document Number 007-029410-424, Revision G, Document Status: Accepted, Date 2023-01-13
[SEC_DHR]	Secure Data Handling Requirements for Intellectual Property and Information, Spec No 000425, Version: D
[DPASL_MAN]	DPA Resistant Software Libraries, Version 2.0

1.3 Terms and Abbreviations

Term or abbreviation	Meaning
CC	Common Criteria
EAL	Evaluation Assurance Level
DPA	Differential Power Analysis
SCA	Side Channel Analysis
FIA	Fault Injection Attack
IC	Integrated Circuit
PP	Protection Profile
PRNG	Pseudo-Random Number Generator
TRNG	True Random Number Generator
SAR	Security Assurance Requirement
Security IC	A system, into which the TOE is integrated
SFP	Security Functional Policy
SFR	Security Functional Requirement
ST	Security Target
PKE	Public Key Engine
MAU	Modulo Arithmetic Unit
MCG	MAU Command Generator
AHB	Advanced High-Performance Bus
SRAM	Static Random-Access Memory
CIC	Command and Interrupt Controller
GF(p)	Prime field
EC	Elliptic Curve

ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman protocol
ECDSA	Elliptic Curve Digital Signature Algorithm
EdDSA	Edwards-curve Digital Signature Algorithm
SM2	Chinese public-key standard based on elliptic curves
SM2DSA	Elliptic Curve Digital Signature Algorithm from SM2 standard

2 Introduction

2.1 ST Lite Reference

The title of this ST is *Rambus PKE4 Core version 4.1 Security Target Lite*, Revision D. The date is 08/Dec/2023.

2.2 TOE Reference

The TOE is titled as *PKE4 Core version 4.1*.

2.3 TOE Overview

Rambus' PK engine is a cryptographic hardware block designed to perform public-key cryptographic operations. It has the following major components.

1. Public Key Engine (PKE):
    a. The Modular Arithmetic Unit (MAU) core performs multi-precision modular arithmetic.
    b. The MAU Command Generator (MCG) core sends sequences of commands to the MAU. For example, an elliptic curve scalar multiply operation requires a sequence of several thousand arithmetic computations.
    c. The Advanced High-performance Bus (AHB) shell interfaces the rest of the system to an external bus.
    d. The interface to the SRAM (SRAM arbiter).

High level block diagram of PK engine is shown in Figure 1.

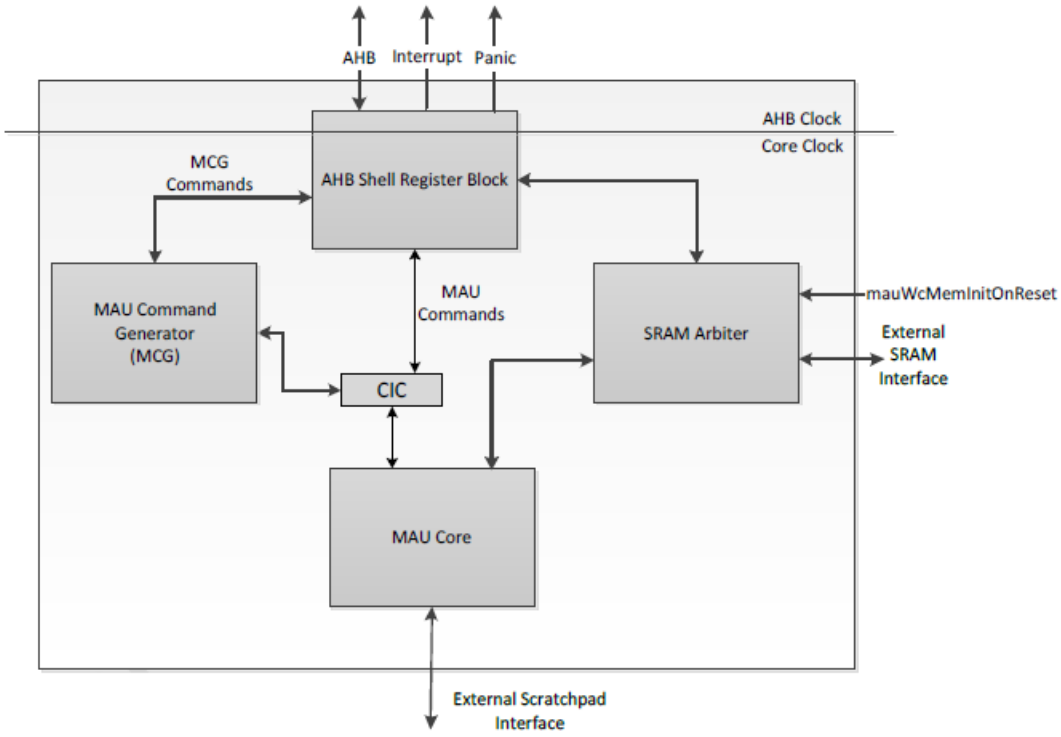

Figure 1 High level block diagram of the PKE

Here AHB stands for Advanced High-Performance Bus, CIC stands for Command and Interrupt Controller and SRAM stands for Static Random-Access Memory.

The PKEv4 core family is available in the following configurations.

Core name	Multiplier	Countermeasures	Maximum RSA key size
PKEv4_64x64_8K_DPA_FIA	64x64	FIA, SCA	8192

Here SCA stands for side channel analysis and FIA stands for fault injection attacks.

PK Engine accepts commands in two formats – MCG command format and MAU command format.

MCG commands are high level commands e.g. ECDH, ECDSA, EdDSA, SM2DSA, RSA, etc. while MAU commands are low level commands e.g. commands for modular arithmetic, memory-related commands, etc.

The TOE is delivered to the integrator as synthesizable Verilog RTL description, a software library in C and the corresponding guidance documents. The integrator is responsible for integrating the TOE into their system, which is referred to as the Security IC throughout this document.

2.4 TOE Description

2.4.1 Physical Scope

Rambus Inc. provides a delivery package to the integrator containing the following components:

1. HW package (source code and test bench), Part Number 950-029004-410
    - Synthesizable Verilog RTL description of PKE Engine.
    - Test bench C files and SystemVerilog files
    - Test bench scripts and file lists
    - Simulation vectors with self-checks
2. SW package (source code and documentation), Part Number 951-029004-410
    - Software library source in C
    - Software reference manual [DPASL_MAN]
    - Software unit tests
3. External reference specification [ERS], Part Number 007-029410-222
4. Integration guide [ITG], Part Number 007-029410-228
5. User security guidance [USG], Part Number 007-029410-424

This list represents the physical scope of the TOE. The Verilog RTL description, functional test bench and test vectors are in one TAR package (Part Number 950-029004-410) and the software library, software reference manual, and software unit tests are in another TAR package (Part Number 951-029004-410) which are delivered to the user PGP encrypted.

A total of four user guidance documents are delivered to the user: External reference specification [ERS], Integration guide [ITG], User security guidance [USG] and Software reference manual [DPASL_MAN]. The Software reference manual [DPASL_MAN] is delivered within the SW package.

It should be noted that a secure delivery process [SEC_DHR] is implemented to ensure the security and integrity of the delivery package. The documentation describing this process is delivered to the customer in plaintext (unencrypted) ahead of receipt of the delivery package.

The integrator is responsible for integrating the TOE into their Security IC. This involves implementing the PKE4 Core interface logic and connecting it to the PKE4 Core. The integrator is expected to fully verify the interface logic and test for proper connectivity. Features internal to the PKE4 Core have been verified by Rambus Inc.

The Security IC is not a part of the TOE and is therefore out of the scope of the evaluation.

2.4.2 Logical scope

PK Engine accepts commands in two formats – MCG command format and MAU command format.

MCG commands are high level commands such as

- ECDH calculation using NIST P-192, NIST P-224, NIST P-256, NIST P-384, NIST P-521, Brainpool-224, Brainpool 256, Brainpool 320, Brainpool 384, Brainpool 512 and ANSSI frp256v1;
- ECDH calculation using the Montgomery X-coordinates X25519 and X448 based on Curve25519 and Curve448;
- ECDSA key generation, signature generation and signature verification using NIST P-192, NIST P-224, NIST P-256, NIST P-384, NIST P-521, Brainpool-224, Brainpool 256, Brainpool 320, Brainpool 384, Brainpool 512, ANSSI frp256v1;
- EdDSA key generation, signature generation and signature verification using Ed448 and Ed25519;
- SM2DSA key generation, signature generation and signature verification using SM2(256);
- Auxiliary elliptic-curve functionality e.g. verification of the curve equation,
- RSA public-key and private key operations for non-CRT implementations;
- Modular exponentiation.

Full description of the TOE interfaces is presented in [ERS].

The TOE is designed to be resistant against state-of-the-art SPA, DPA, template attacks, FIA as well as their combinations. Transient faults as well as permanent faults are in scope.

2.5 TOE Lifecycle and Delivery

As explained in Section 2.3, the integrator is responsible for integrating the TOE into their Security IC. The Security IC must be certified according to the IC Platform Protection Profile [PP], which defines seven lifecycle phases:

1. IC embedded software development,
2. IC development,
3. IC manufacturing,
4. IC packaging,
5. composite product integration,
6. personalization,
7. operational usage.

The whole lifecycle of the TOE can be seen as a part of Phase 2 for the Security IC. Details of the components included in the delivery package are described in Section 2.4.1.

2.6 Non-TOE Hardware/Software/Firmware

The non-TOE hardware/software/firmware required by the TOE includes the

- Working Context Memory for TOE inputs, outputs, computations
  - 1024x78 single-ported SRAM with half-word enables, single-cycle latency
- Scratchpad Memory for TOE computations
  - 128x72 1R/1W memory as register file or SRAM macro, single-cycle latency
- Security IC, i.e., a system into which the TOE is integrated
  - Includes hardware or software to drive the TOE

3 Conformance Claims

3.1 CC Conformance Claim

This ST claims to be conformant to [CC]. Furthermore, it claims to be CC Part 2 conformant and CC Part 3 conformant.

3.2 PP Claim

This ST does not claim conformance to any PP.

The purpose of this ST is to enable the developer of a Security IC to certify their product according to the IC Platform Protection Profile [PP] in a composite evaluation reusing the certification results of this TOE.

3.3 Package Claim

This ST claims conformance to the assurance package EAL4 augmented with AVA_VAN.5, ATE_DPT.2 and ALC_DVS.2.

3.4 Information for Feature Composition [PP]

The TOE is a simple product in the sense that its functionality is limited to ECC and RSA operations. The IC Platform Protection Profile [PP] provides Packages for Cryptographic Services that can be used to describe this functionality. The ST author uses these packages as a stepping stone for the security problem definition, security objectives and the security functional requirements (SFRs).

The security problem definition does not include any threats. In particular, no threats from [PP] are included. Those threats shall be taken into account during composite evaluations. The organizational security policies and assumptions are the same as in [PP] except for:

- an additional organizational security policy is added in order to address ECC and RSA operations.
- an additional assumption A.RNG is added since the environment needs to provide a TRNG that provide an entropy source of sufficient quality to seed the PRNG of the TOE.

The ECC and RSA functionality is further mapped to the objective for the TOE. The ST also contains four objectives for the environment:

- OE.Process-Sec-IC and OE.Resp-Appl originate from [PP].
- OE.Identification results from a transformation of O.Identification from [PP] into an objective for the environment. The reason for such transformation is that the TOE depends on the Security IC when it comes to the identification.
- OE.RNG is added to map to the A.RNG assumption.

The SFRs used in this ST are a subset of the SFRs claimed in [PP] except for the FDP_ITC.1, which is defined in [CC] Part 2. The reason is that the TOE needs to import several parameters to perform cryptographic operations.

The ST uses exactly the same set of security assurance requirements as [PP] to ensure that the certification results of the TOE can be reused for the future composite evaluations.

4 Security Problem Definition

As explained above, the purpose of this ST is to enable the developer of a Security IC to certify their product according to the IC Platform Protection Profile [PP] in a composite evaluation reusing the certification results of this TOE. In order to simplify the composite evaluations, the security problem definition (SPD) for this ST is chosen to be a subset of the SPD in [PP] with one additional organizational security policy, which is copied from an augmentation package of [PP].

4.1 Assets

The list of the assets in this ST is the same as in [PP]. In particular, the list includes user data such as input, output data, intermediate values and cryptographic keys as well as the correct execution of the ECC and RSA operations.

4.2 Threats

No threats are included.

4.3 Organisational Security Policies

Policy Name	Policy Definition
P.Process-TOE	Identification during TOE Development and Production An accurate identification must be established for the TOE. This requires that each instantiation of the TOE carries this unique identification.
P.Crypto-Service	Cryptographic services of the TOE The TOE provides secure hardware based cryptographic services for the IC Embedded Software.

4.4 Assumptions

Assumption Name	Assumption Definition
A.Process-Sec-IC	Protection during Packaging, Finishing, and Personalisation It is assumed that security procedures are used after delivery of the TOE by the TOE Manufacturer up to delivery to the end-consumer to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorised use). This means that the Phases after TOE Delivery are assumed to be protected appropriately.
A.Resp-Appl	Treatment of user data of the Composite TOE All user data of the Composite TOE are owned by Security IC Embedded Software. Therefore, it must be assumed that security relevant user data of the Composite TOE (especially cryptographic keys) are treated by the Security IC Embedded Software as defined for its specific application context.
A.RNG	PRNG seed It is assumed that the security IC platform running the TOE has a TRNG that provide an entropy source of sufficient quality to seed the PRNG of the TOE (i.e., at least satisfying the requirements for PTG.2 as described in [KS2011]).

5 Security Objectives

5.1 Security Objectives for the TOE

Objective Name	Objective Definition
O.ECC	Cryptographic Service ECC The TOE provides secure hardware based cryptographic services for the ECC for ECDH, ECDSA, EdDSA and SM2DSA.
O.RSA	Cryptographic service RSA The TOE provides secure hardware based cryptographic services for the RSA for private-key and public-key operations.

5.2 Security Objectives for the Environment

Objective Name	Objective Definition
OE.Process-Sec-IC	Protection during composite product manufacturing Security procedures shall be used after TOE Delivery up to delivery to the end-consumer to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorised use). This means that Phases after TOE Delivery up to the end of Phase 6 (refer to Section 2.5) must be protected appropriately.
OE.Resp-Appl	Treatment of user data of the Composite TOE Security relevant user data of the Composite TOE (especially cryptographic keys) are treated by the Security IC Embedded Software as required by the security needs of the specific application context.
OE.Identification	Identification during TOE Development and Production The TOE environment must enable accurate identification of the TOE during TOE development and production.
OE.RNG	PRNG seed The security IC platform running the TOE shall have a TRNG that provide an entropy source of sufficient quality to seed the PRNG of the TOE (i.e., at least satisfying the requirements for PTG.2 as described in [KS2011]).

5.3 Security Objectives Rationale

The following table shows that the security objectives are suitable to cover the organizational security policies and assumptions.

Threats, OSP or Assumption	Security Objective	Rationale
P.Process-TOE	OE.Identification	P.Process-TOE states that an accurate identification must be established for the TOE during TOE development and production. The TOE implements no functionality for TOE identification and therefore this functionality must be provided by the TOE environment, which is exactly what OE.Identification claims. Thus the security objective is suitable to cover P.Process-TOE.
P.Crypto-Service	O.ECC, O.RSA	P.Crypto-Service states that TOE provides secure hardware based cryptographic services while O.ECC and O.RSA state that the TOE implements RSA and ECC. Therefore the O.ECC and O.RSA are suitable to cover P.Crypto-Service.

A.Process-Sec-IC	OE.Process-Sec-IC	Since OE.Process-Sec-IC requires the Composite Product Manufacturer to implement those measures assumed in A.Process-Sec-IC, the assumption is covered by this objective.
A.Resp-Appl	OE.Resp-Appl	Since OE.Resp-Appl requires the Security IC Embedded Software to implement measures as assumed in A.Resp-Appl, the assumption is covered by the objective.
A.RNG	OE.RNG	Since the OE.RNG requires the Security IC Platform to have a TRNG that provides an entropy source of sufficient quality to seed the PRNG of the TOE as assumed in A.RNG, the assumption is covered by the objective.

6 Extended Components Definition

This document contains no definitions for extended SFRs.

7 Security Requirements

7.1 Security Functional Requirements

In order to define the Security Functional Requirements (SFRs) Part 2 of the Common Criteria standard [CC] was used.

The operations are marked as follows.

- The selection operation is used to select one or more options provided by the CC in stating a requirement. Selections made by the ST author are denoted as ***bold and italicized***.
- The assignment operation is used to assign a specific value to an unspecified parameter. Assignments made by the ST author appear in **bold text**.
- In some cases, an interpretation refinement is given. In such a case an extra paragraph starting with "Refinement" may be given.
- 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.

The SFRs defined in this ST are a subset of the SFRs defined in [PP] except for the FDP_ITC.1 which is defined in [CC] Part 2.

7.1.1 FCS_COP.1 Cryptographic operation

FCS_COP.1.1 The TSF shall perform **cryptographic operations in** Table 1 in accordance with a specified cryptographic algorithm **defined in** Table 1 and cryptographic key sizes **defined in** Table 1 that meet the following: **see** Table 1.

Application note:

The TOE does not have a hardware hash core. The hash is provided by the environment.

Application note (ECDSA):

Supported curves are NIST P-192, NIST P-224, NIST P-256, NIST P-384, NIST P-521, Brainpool-224, Brainpool 256, Brainpool 320, Brainpool 384, Brainpool 512, ANSSI frp256v1.

Application note (ECDH):

- Supported curves are NIST P-192, NIST P-224, NIST P-256, NIST P-384, NIST P-521, Brainpool-224, Brainpool 256, Brainpool 320, Brainpool 384, Brainpool 512, ANSSI frp256v1, Montgomery curve25519
- The TOE implements two variants of the ECDH operation for long term and ephemeral keys.

Application note (EdDSA):

Supported curves are Edwards curves Ed448 and Ed25519.

Iteration of FCS_COP.1	Assignment: list of cryptographic operations	Assignment: cryptographic algorithm	Assignment: list of cryptographic key sizes	Assignment: list of standards
FCS_COP.1/ONCURVE	**Point on curve verification and x-coordinate on curve verification**	**ECC over GF(p)**	**192, 224, 256, 320, 384, 512, 521 bits**	**[ISO 14888-3] [FIPS 186-4] [ANSI X9.62] [ANSSI] [RFC 5639] [SM2] [SM2 TR]**

Iteration of FCS_COP.1	Assignment: list of cryptographic operations	Assignment: cryptographic algorithm	Assignment: list of cryptographic key sizes	Assignment: list of standards
FCS_COP.1/ECDSA	**signature generation and signature verification**	**Elliptic Curve Digital Signature Algorithm / ECC over GF(p)**	**192, 224, 256, 320, 384, 512, 521 bits**	**[ISO 14888-3] [FIPS 186-4] [ANSI X9.62] [ANSSI] [RFC 5639]**
FCS_COP.1/SM2DSA	**signature generation and signature verification**	**SM2DSA / ECC over GF(p)**	**256 bits**	**[SM2] [SM2 TR] [ISO 14888-3]**
FCS_COP.1/ECDH	**Diffie-Hellman key exchange**	**ECDH / ECC over GF(p)**	**192, 224, 256, 320, 384, 512, 521 bits**	**[ISO 11770-3] [ANSI X9.63]**
FCS_COP.1/EdDSA	**signature generation and signature verification**	**EdDSA / ECC over GF(p)**	**456, 256 bits**	**[RFC 8032]**
FCS_COP.1/RSA	**signature generation, signature verification, decryption**	**RSA (non-CRT)**	**1024 to 8192 bits**	**[PKCS#1]**

Table 1 FCS_COP.1 iterations

7.1.2 FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **detailed in** Table 2 and specified cryptographic key sizes **detailed in** Table 2 that meet the following: **see** Table 2.

Application Note (FCS_CKM.1/ECDSA):

Supported curves are NIST P-192, NIST P-224, NIST P-256, NIST P-384, NIST P-521, Brainpool-224, Brainpool 256, Brainpool 320, Brainpool 384, Brainpool 512, ANSSI frp256v1.

Application Note (FCS_CKM.1/ECDH):

- Supported curves are NIST P-192, NIST P-224, NIST P-256, NIST P-384, NIST P-521, Brainpool-224, Brainpool 256, Brainpool 320, Brainpool 384, Brainpool 512, ANSSI frp256v1, Montgomery curve25519.
- The TOE implements two variants of the ECDH operation for long term and ephemeral keys.
- Following papers were considered to support the implementation: [Ed448] and [Curve 25519].

Application Note (FCS_CKM.1/EdDSA):

Supported curves are Ed448 and Ed25519.

Iteration of FCS_CKM.1	Assignment: cryptographic key generation algorithms	Assignment: cryptographic key sizes	Assignment: list of standards
FCS_CKM.1/ECDSA	**ECDSA public key generation**	**192, 224, 256, 320, 384, 512, 521 bits**	**[ANSI X9.62] [ISO 14888-3] [FIPS 186-4]**

Iteration of FCS_CKM.1	Assignment: cryptographic key generation algorithms	Assignment: cryptographic key sizes	Assignment: list of standards
FCS_CKM.1/SM2DSA	**SM2DSA public key generation**	**256 bits**	**[SM2] Part 1**
FCS_CKM.1/ECDH	**ECDH public key generation (x-coordinate only) and ECDH public shared key generation**	**192, 224, 256, 320, 384, 512, 521 bits**	**[ISO 11770-3]** **[ANSI X9.63]** **[RFC 7748]** **[NIST SP 800-186]**
FCS_CKM.1/EdDSA	**EdDSA public key generation**	**456, 256 bits**	**[RFC 8032]**

Table 2 FCS_CKM.1 iterations

7.1.3 FCS_CKM. 4 Cryptographic key destruction

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

7.1.4 FRU_FLT.2 Limited fault tolerance

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)**.

Application note:
The assignment is done in the same way as in [PP].

7.1.5 FPT_FLS.1 Failure with preservation of secure state

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

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

Application note:
The assignment and the refinement are done in the same way as in [PP].

7.1.6 FDP_ITT.1 Basic internal transfer protection

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

Refinement: The MCG and other functional units of the TOE (e.g. the Modular Arithmetic Unit) are seen as physically-separated parts of the TOE.

Application note:
The assignment and the refinement are done in the same way as in [PP].

Application note:
The Data Processing Policy is defined as follows. “No user data such as input, output data, intermediate values and cryptographic keys shall be transferred or processed in plain. The data shall be protected by masking techniques”. The definition is different from the one given in [PP] the reason being that this ST needs a more concrete version.

Application note:
This ST does not claim full protection against SCA since the TOE is delivered as the Synthesizable Verilog RTL description and a number of critical decisions have to be made by the IC designer. If SCA is in scope the IC has to be designed in such a way that SCA attacks are infeasible

7.1.7 FPT_ITT.1 Basic internal TSF data transfer protection

FPT_ITT.1.1	The TSF shall protect TSF data from ***disclosure*** when it is transmitted between separate parts of the TOE. **Refinement: The MCG and other functional units of the TOE (e.g. the Modular Arithmetic Unit) are seen as physically-separated parts of the TOE.**

Application note:
The assignment and the refinement are done in the same way as in [PP].

Application note:
This ST does not claim full protection against SCA since the TOE is delivered as the Synthesizable Verilog RTL description and a number of critical decisions have to be made by the IC designer. If SCA is in scope the IC has to be designed in such a way that SCA attacks are infeasible.

7.1.8 FDP_IFC.1 Subset information flow control

FDP_IFC.1.1	The TSF shall enforce the **Data Processing Policy** on **all confidential data when they are processed or transferred by the TOE or by the Security IC Embedded Software**.

Application note:
The assignments are done in the same way as in [PP].

Application note:
The Data Processing Policy is defined as follows. “No user data such as input, output data, intermediate values and cryptographic keys shall be transferred or processed in plain. The data shall be protected by masking techniques”. The definition is different from the one given in [PP] the reason being that this ST needs a more concrete version.

Application note:
This ST does not claim full protection against SCA since the TOE is delivered as the Synthesizable Verilog RTL description and a number of critical decisions have to be made by the IC designer. If SCA is in scope the IC has to be designed in such a way that SCA attacks are infeasible

7.1.9 FDP_ITC.1 Import of user data without security attributes

FDP_ITC.1.1	The TSF shall enforce the **none** when importing user data, controlled under the SFP, from outside of the TOE.
FDP_ITC.1.2	The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE
FDP_ITC.1.3	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **improper commands are rejected**

Application note:
The TOE implements no access control SFP(s) and/or information flow control SFP(s). The commands sent to the TOE must comply with the TOE guidance [ERS], [USG] and [ITG].

7.2 Security Assurance Requirements

This Security Target claims conformance to EAL4 augmented with ATE_DPT.2, AVA_VAN.5 and ALC_DVS.2, which are the same assurance security requirements claimed in the IC Platform Protection Profile [PP].

The applicability to the TOE of all refinements defined in Section 6.2.1 of the Protection Profile [PP] has been also assessed in this section, as summarized in the last column in Table 3 and detailed in the subsections.

The following table lists the security assurance requirements for the TOE.

Assurance Class	Component	Component Title
ADV Development	ADV_ARC.1	Security architecture
	ADV_FSP.4	Complete functional specification
	ADV_IMP.1	Implementation representation of the TSF
	ADV_TDS.3	Basic modular design
AGD: Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
ALC_ Life-cycle support	ALC_CMC.4	Production support, acceptance procedures and automation
	ALC_CMS.4	Problem tracking CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.2	Sufficiency of security measures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
ASE: Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_TSS.1	TOE summary specification
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
ATE: Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.2	Testing: basic design
	ATE_FUN.1	Functional tests
	ATE_IND.2	Independent testing
AVA: Vulnerability assessment	AVA_VAN.5	Advanced methodical vulnerability analysis

Table 3 EAL4 requirements description extended with augmented with AVA_VAN.5 and ALC_DVS.2

Since this ST claims all assurance requirements from [PP] and since the objective of this ST is to provide a basis for certification of [PP] compliant Security ICs, this ST also claims all SAR refinements from [PP]. Some refinements, however, need to be adjusted as the TOE is only a part of the Security IC. All SAR refinements are listed in the table below.

SAR	Refinement	Description
ALC_DEL	188 in [PP]	This ST redefines this refinement as follows. **For delivery of the TOE to the "IC Designer as consumer", all the external interfaces of the composite TOE designer have to be taken into account.**
ALC_DVS	194 in [PP]	This ST redefines this refinement as follows. **"TOE design and implementation" must be understood as comprising all material and information related to the development and production of the TOE.**
ALC_CMS	199 in [PP]	This refinement is out of scope for the TOE because it relates to consumer software that can be part of manufacturing and delivery.
	205 in [PP]	This refinement is out of scope for the TOE because it refers to the CMS refinement.
	206 in [PP]	This refinement is out of scope for the TOE because it refers to tracking of production batches for wafers or dies.
ADV_ARC	209 in [PP]	This refinement is applicable without any adjustments. **The Security Architecture description of the TSF initialisation process shall include the procedures to establish full functionality after power-up, state transitions from the secure state as required by FPT_FLS.1, and any state transitions of power save modes if provided by the TOE.**
	210 in [PP]	This refinement in [PP] is out of scope for the TOE because it relates to test features used in wafer testing.
ADV_FSP	215 in [PP]	This refinement refers to test software delivered but not available in the operational phase. This refinement is regarded out of scope for the TOE.
	216 in [PP]	This refinement refers to features that do not provide functionality but nevertheless contribute to SFRs. This refinement is regarded out of scope for the TOE.
	217 in [PP]	The ST redefines this refinement as follows. **The Functional Specification is expected to refer to mechanisms.**
	218 in [PP]	This refinement refers to operating conditions. This refinement is regarded out of scope for the TOE.
ADV_IMP	223 in [PP]	This refinement is applicable without any adjustments. **It must be checked that the provided implementation representation is complete and sufficient to ensure that analysis activities are not curtailed due to lack of information.**
ATE_COV	226 in [PP]	This refinement specifies that the TOE must be tested under different operating conditions within the specified ranges. This refinement is out of scope for the TOE.
	227 in [PP]	This refinement relates to physical testing. This refinement is out of scope for the TOE.
AGD_OPE	233 in [PP]	This ST redefines this refinement as follows. **The role of the IC Designer is the main focus of the guidance.**
	234 in [PP]	This refinement relates to requirements concerting embedded software. This requirement is regarded out of scope for the TOE.
	235 in [PP]	This refinement is applicable without any adjustments. **Guidance documents must not contain security relevant details which are not necessary for the usage or administration of the security functionality of the TOE.**
AGD_PRE	239 in [PP]	The ST redefines this refinement as follows.

SAR	Refinement	Description
		The Family AGD_PRE addresses the activities of the delivery acceptance procedures.
	240 in [PP]	This refinement refers to configuration in Phase 2 or Phase 7. This refinement is out of scope for the TOE
	241 in [PP]	This refinement refers to downloading of embedded software. This refinement is out of scope for the TOE.
AVA_VAN	245 in [PP]	The ST redefines this refinement as follows. **The vulnerability analysis shall include a justification for the rating of information on the TOE available to the attacker.**

7.3 Security Requirements Rationale

7.3.1 Rationale for the Security Functional Requirements

This rationale shows that all security objectives for the TOE are upheld by the security functional requirements.

Objective	Rationale
O.ECC	FCS_COP.1 iterations request the TOE to implement the cryptographic service targeted in O.ECC according to approved public standards. FCS_CKM.1 iterations request the TOE to implement a key generation method to be used by the cryptographic service and FCS_CKM.4 request the TOE to implement secure destruction method for its cryptography key. FDP_ITC.1 makes also possible to load keys and data needed for the ECC operation. FRU_FLT.2 addresses the limited fault tolerance for the ECC functionality. FPT_FLS.1 preserves a secure state then a failure is detected during an ECC operation. FDP_IFC.1 ensures that no user data such as input, output data, intermediate values, keys are transferred or processed in plain. FDP_ITT.1 and FPT_ITT.1 preserve that no user data and TSF data are transferred or processed in plain between separated parts of the TOE. O.ECC is met by: • FCS_COP.1/ECDSA, FCS_COP.1/SM2DSA, FCS_COP.1/ECDH, FCS_COP.1/EdDSA, FCS_COP.1/ONCURVE • FCS_CKM.1/ECDSA, FCS_CKM.1/SM2DSA, FCS_CKM.1/ECDH, FCS_CKM.1/EdDSA • FCS_CKM.4 • FRU_FLT.2 • FPT_FLS.1 • FDP_IFC.1 • FDP_ITT.1 • FPT_ITT.1 • FDP_ITC.1
O.RSA	FCS_COP.1/RSA requests the TOE to implement the cryptographic service targeted in O.RSA according to approved public standards. FCS_CKM.4 requests the TOE to implement secure destruction method for its cryptography key. FRU_FLT.2 addresses the limited fault tolerance for the ECC functionality. FPT_FLS.1 preserves a secure state then a failure is detected during an ECC operation. FDP_IFC.1 ensures that no user data such as input, output data, intermediate values, keys are transferred or processed in plain. FDP_ITT.1 and FPT_ITT.1 preserve that no user data and TSF data are transferred or processed in plain between separated parts of the TOE. O.RSA is met by: • FCS_COP.1/RSA • FCS_CKM.4 • FRU_FLT.2 • FPT_FLS.1 • FDP_IFC.1 • FDP_ITT.1 • FPT_ITT.1 • FDP_ITC.1

Table 4 SFR to Security Objectives rationale

SFR	TOE Objectives	
	O.ECC	O.RSA
FCS_COP.1/ECDSA	X	
FCS_COP.1/SM2DSA	X	
FCS_COP.1/ECDH	X	
FCS_COP.1/EdDSA	X	
FCS_COP.1/ONCURVE	X	
FCS_COP.1 /RSA		X
FCS_CKM.1/ECDSA	X	
FCS_CKM.1/SM2DSA	X	
FCS_CKM.1/ECDH	X	
FCS_CKM.1/EdDSA	X	
FCS_CKM.4	X	X
FRU_FLT.2	X	X
FPT_FLS.1	X	X
FDP_IFC.1	X	X
FDP_ITT.1	X	X
FPT_ITT.1	X	X
FDP_ITC.1	X	X

Table 5 SFRs to Security Objectives for the TOE mapping

7.3.2 Dependencies of Security Functional Requirements

This rationale shows that all dependencies of all security requirements have been addressed:

Requirement	Dependency	Fulfilled?
FCS_COP.1/ECDSA	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1) and (FCS_CKM.4)	Yes, FCS_CKM.1/ECDSA, FCS_CKM.4 and FDP_ITC.1
FCS_COP.1/SM2DSA	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1) and (FCS_CKM.4)	Yes, FCS_CKM.1/SM2DSA, FCS_CKM.4 and FDP_ITC.1
FCS_COP.1/ECDH	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1) and (FCS_CKM.4)	Yes, FCS_CKM.1/ECDH, FCS_CKM.4 and FDP_ITC.1
FCS_COP.1/EdDSA	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1) and (FCS_CKM.4)	Yes, FCS_CKM.1/EdDSA, FCS_CKM.4 and FDP_ITC.1
FCS_COP.1/ONCURVE	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1) and (FCS_CKM.4)	Only FDP_ITC.1. See justification below.
FCS_COP.1/RSA	(FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	Yes, FCS_CKM.4 and FDP_ITC.1
FCS_CKM.1/ECDSA	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	Yes, FCS_COP.1/ECDSA, FCS_CKM.4 and FDP_ITC.1
FCS_CKM.1/SM2DSA	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	Yes, FCS_COP.1/SM2DSA, FCS_CKM.4 and FDP_ITC.1
FCS_CKM.1/ECDH	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	Yes, FCS_COP.1/ECDH, FCS_CKM.4 and FDP_ITC.1
FCS_CKM.1/EdDSA	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	Yes, FCS_COP.1/EdDSA, FCS_CKM.4 and FDP_ITC.1
FCS_CKM.4	(FDP_ITC.1 or FDP_ITC.1 or FCS_CKM.1)	Yes, FCS_CKM.1/ECDSA, FCS_CKM.1/ECDH, FCS_CKM.1/SM2DSA, and FCS_CKM.1/EdDSA
FRU_FLT.2	FPT_FLS.1	Yes, FPT_FLS.1
FPT_FLS.1	No dependencies	Not applicable

Requirement	Dependency	Fulfilled?
FDP_ITT.1	(FDP_ACC.1 or FDP_IFC.1)	Yes, FDP_IFC.1
FPT_ITT.1	No dependencies	Not applicable
FDP_IFC.1	FDP_IFF.1	See justification below.
FDP_ITC.1	(FDP_ACC.1 or FDP_IFC.1) and (FMT_MSA.3)	Only FDP_IFC.1. See justification below.

Table 6 SFR dependencies rationale

Dependency of FCS_COP.1/ONCURVE on FCS_CKM.4 is not satisfied. The reason is that no private key is required to execute this functionality.

Dependency of FDP_IFC.1 on FDP_IFF.1 is not satisfied. The reason is that no specific attributes are necessary.

Dependency of FDP_ITC.1 on FMT_MSA.3 is not satisfied. The reason is that no specific attributes have to be initialized in this case.

7.3.3 Rationale for the Security Assurance Requirements

The current TOE is expected to be used by Secure IC developers in a composite evaluation reusing the certification results of this TOE. Therefore, following the same rationale as in the protection profile [PP], the assurance level EAL4 and the augmentation with the requirements ATE_DPT.2, ALC_DVS.2, and AVA_VAN.5 were chosen in order to meet assurance expectations explained in the following paragraph.

An assurance level of EAL4 with the augmentations AVA_VAN.5 and ALC_DVS.2 are required for this type of TOE since it is intended to defend against sophisticated attacks. This evaluation assurance package was selected to permit a developer to gain maximum assurance from positive security engineering based on good commercial practices. In order to provide a meaningful level of assurance that the TOE provides an adequate level of defence against such attacks, the evaluators should have access to the low level design and source code.

7.3.3.1 ALC_DVS.2 Sufficiency of security measures

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 Security IC, and therefore applicable to the current TOE, the TOE is developed and produced within a complex and distributed industrial process which must especially be protected. Details about the implementation, (e.g. from design, test and development tools as well as Initialisation Data) may make such attacks easier. Therefore, in the case of a Security IC, maintaining the confidentiality of the design is very important.

This assurance component is a higher hierarchical component to EAL4 (which only requires ALC_DVS.1). ALC_DVS.2 has no dependencies.

7.3.3.2 AVA_VAN.5 Advanced methodical vulnerability analysis

Due to the intended use of the TOE, it must be shown to be highly resistant to penetration attacks. This assurance requirement is achieved by the AVA_VAN.5 component.

Independent vulnerability analysis is based on highly detailed technical information. The main intent of the evaluator analysis is to determine that the TOE is resistant to penetration attacks performed by an attacker possessing high attack potential.

AVA_VAN.5 has dependencies to ADV_ARC.1 “Security architecture description”, ADV_FSP.4 “Complete functional specification”, ADV_TDS.3 “Basic modular design”, ADV_IMP.1 “Implementation representation of the TSF”, AGD_OPE.1 “Operational user guidance”, AGD_PRE.1 “Preparative procedures”, and ATE_DPT.1 “Testing: basic design”.

All these dependencies are satisfied by EAL4.

It has to be assumed that attackers with high attack potential try to attack Security ICs like smart cards used for digital signature applications or payment systems. Therefore, specifically AVA_VAN.5 was chosen in order to assure that even these attackers cannot successfully attack the TOE.

Note that detailed refinements for assurance requirements are given in Section 6.2.1.

7.3.3.3 ATE_DPT.2 Testing: basic design

ATE_DPT.2 is added to be in line with the security assurance requirements from the [PP].

This assurance component is a higher hierarchical component to EAL4 (which only requires ATE_DPT.1).

ATE_DPT.2 has dependencies to ADV_ARC.1 “Security architecture description”, ADV_TDS.3 “Basic modular design”, and ATE_FUN.1 “Functional testing”.

All these dependencies are satisfied by EAL4.

7.3.4 Security Requirements are internally consistent

The iterations on FCS_COP and FCS_CKM do not conflict since they address different operations with different keys.

8 TOE Summary Specification

8.1 FCS_COP.1 Cryptographic operation

The TOE implements the following cryptographic operations:

- RSA signature generation, signature verification and decryption according to [PKCS#1]. The supported key length is 1024 to 8192 bits. Enforced by: FCS_COP.1/RSA.
- ECDSA signature generation and signature verification according to [ISO 14888-3], [FIPS 186-4], [ANSI X9.62], [ANSSI] and [RFC 5639]. Supported key length is 192 to 521 bits. Enforced by: FCS_COP.1/ECDSA.
- Diffie-Hellman key exchange according to [ISO 11770-3] and [ANSI X9.63]. Supported key length is 192 to 521 bits. Enforced by: FCS_COP.1/ECDH.
- SM2 DSA signature generation and signature verification according to [SM2], [SM2 TR] and [ISO 14888-3]. The supported key length is 256 bits. Enforced by: FCS_COP.1/SM2DSA.

  Note that the TOE does not have a hash core. The hash needs to be provided by the environment.
- Diffie-Hellman key exchange according to [ISO 11770-3] and [ANSI X9.63]. Supported key length is 192 to 521 bits. Enforced by: FCS_COP.1/ECDH
- EdDSA signature generation and signature verification according to [RFC 8032]. The supported key length is 456 and 256 bits. Enforced by: FCS_COP.1/EdDSA
- Tests if, for a given x-coordinate, there is a y such that (x,y) is on the elliptic curve. It also test whether a given (x,y) pair is a point on an elliptic curve. Enforced by: FCS_COP.1/ONCURVE.

8.2 FCS_CKM.4 Key destruction

The TOE provides functions to destroy EC and RSA cryptographic keys by overwriting sensitive data with zeros.

8.3 FCS_CKM.1 Cryptographic key generation

The TOE implements the following cryptographic key generation functionality:

- ECC over GF(p) public key generation according to [ANSI X9.62], [ISO 14888-3] and [FIPS 186-4]. Supported key length is 192 to 521 bits. Enforced by: FCS_CKM.1/ECDSA.
- Diffie-Hellman ECC over GF(p) public key generation according to [ISO 11770-3], [ANSI X9.63], [RFC 7748] and [NIST SP 800-186]. The supported key length is 192 to 521 bits. Enforced by: FCS_CKM.1/ECDH.
- SM2 DSA ECC over GF(p) public key generation according to [SM2] Part 1. The supported key length is 256 bits. Note that the TOE does not have a hash core and therefore, the hash need to be performed out of the TOE. Enforced by: FCS_CKM.1/SM2DSA.
- EdDSA ECC over GF(p) public key generation according to [RFC 8032]. The supported key length is 456 and 256 bits. Enforced by: FCS_CKM.1/EdDSA.

8.4 FRU_FLT.2 Limited fault tolerance

In the situation when no FIA is detected by the fault detection functionality (cf. Section 8.5) the TOE operates normally and is capable of executing all commands.

8.5 FPT_FLS.1 Failure with preservation of secure state

The TOE is designed to detect and report internal faults, which can be transient or permanent faults. These faults can occur due to a laser beam, EM pulse, power glitch, temperature change or any other possible method that can disturb operations and inject faults that will result in an erroneous behavior.

Whenever a fault is detected the TOE the core continues to the end of the operation with dummy data and then enters the error state. The core goes back to the reset state after error consumption.

8.6 FDP_IFC.1 Subset information flow control

Handling of sensitive data in shares protects the TOE from potential side-channel attacks. In addition, most data paths are 64 bits wide or more.

Blinding techniques are implemented for RSA and ECC operations.

This functionality serves as a countermeasure against side-channel analysis.

8.7 FDP_ITT.1 Basic internal transfer protection

Handling of sensitive data in shares protects the TOE from potential side-channel attacks. In addition, most data paths are 64 bits wide or more.

Blinding techniques are implemented for RSA and ECC operations.

This functionality serves as a countermeasure against side-channel analysis.

8.8 FPT_ITT.1 Basic internal TSF data transfer protection

Handling of sensitive data in shares protects the TOE from potential side-channel attacks. In addition, most data paths are 64 bits wide or more.

Blinding techniques are implemented for RSA and ECC operations.

This functionality serves as a countermeasure against side-channel analysis.

8.9 FDP_ITC.1 Import of user data without security attributes

In order to perform the cryptographic operations with ECC defined in FCS_COP.1 and FCS_CKM.1 it is required to import several parameters (e.g. the private key or nonce).

Hashes also need to be imported to support the ECC functionality in FCS_CKM.1.

RSA operations defined in FCS_COP.1 do also require the import of parameters like the message or ciphertext, modulus or the blinded private exponent.