Rambus

Security IP

AES-ECB-32-DPA-FIA HW3.0

Common Criteria Security Target Lite

Document Revision: C
Document Date: 2022-07-04
Document Number: 001-033300-503/023
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	2022-03-24	Rambus	• Derived from full Security Target
B	2.1, 2.4	2022-04-15	Rambus	• Added TOE details
C	1.2, 2.1	2022-07-04	Rambus	• Reference to this document title and DEL-User updated

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
[PP84]	Security IC Platform Protection Profile with Augmentation Packages, BSI-CC-PP-0084-2014, Version 1.0
[FIPS-197]	NIST FIPS-197 Advanced Encryption Standard, 2001
[SP800-38A]	NIST SP 800-38A Recommendation for Block Cipher Modes of Operation: Methods and Techniques, 2001
[ERS]	AES-ECB-DPA-FIA HW3.0 External Reference Specification, Revision A
[IG]	AES-ECB-DPA-FIA Cores HW3.0 Integration Guide, Revision C
[USG]	AES-ECB-DPA-FIA HW3.0 User Security Guidance, Revision D
[DEL-User]	Document Template Customer Requirements for Secure Data Handling of Rambus Intellectual Property and Information, 000446, Revision A

1.3 Terms and Abbreviations

Term or abbreviation	Meaning
AES	Advanced Encryption Standard
CC	Common Criteria
CFB mode	Cipher Feedback mode
CTR mode	Counter mode
DPA	Differential Power Attack
EAL	Evaluation Assurance Level
ECB	Electronic Code Book
FIA	Fault Injection Attack
IC	Integrated Circuit
PP	Protection Profile
PRNG	Pseudo-Random Number Generator
SAR	Security Assurance Requirement
SCA	Side Channel Analysis
Security IC	A system, into which the TOE is integrated

SFP	Security Functional Policy
SFR	Security Functional Requirement
ST	Security Target

2 Introduction

2.1 ST Lite Reference

The title of this ST Lite is Rambus *AES-ECB-32-DPA-FIA HW3.0 Common Criteria Security Target Lite*. The document version is C. The date is 04/Jul/2022.

2.2 TOE Reference

The TOE is entitled as *AES-ECB-DPA-FIA cores HW3.0*.

For the sake of simplicity, "HW3.0" is often omitted throughout this ST. The plural form "cores" is used as a synonym of a core family. In some ST paragraphs, the TOE is referred to as the core.

2.3 TOE Overview

The TOE is a first-order differential power attack (DPA) and fault injection attack (FIA) resistant Advanced Encryption Standard (AES) core providing the electronic code book (ECB) mode of operation.

The TOE is delivered to the integrator as synthesizable Verilog RTL description. The integrator is responsible for integrating the TOE into their system, which is referred to as the Security IC throughout this document.

The TOE supports both encryption and decryption directions.

2.4 TOE Description

2.4.1 Physical Scope

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

- Synthesizable Verilog RTL description of the core. The description conforms to the 1394-2001 ("V2K") version of the language.
- Sample TCL synthesis constraints and primitive cell library templates
- Functional test bench and scripts required to build the test bench and run the provided tests.
- TCL script for post-layout verification that the required gate structure is intact.
- The guidance that includes external reference specification [ERS], User Security Guidance [USG] and integration guide [IG].

The TOE delivery package is named 950-033023-300_aes_ecb_32_dpa_fia_28d3300001010702 (with corresponding coreVersion field of 28d3300001010702). The version of the components corresponds to the coreVersion of the package. In addition, the TOE guidance documents have individual revisions as described in Section 1.2.

This list represents the physical scope of the TOE. The Verilog RTL description, Sample TCL, functional test bench, and post-layout verification and guidance are combined in a single TAR package and delivered to the user PGP encrypted.

It should be noted that a secure delivery process [DEL_User] 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 user should follow the instructions as specified in the secure delivery process [DEL_User].

The integrator is responsible for integrating the TOE into their Security IC. This involves implementing the AES-ECB-DPA-FIA cores interface logic and connecting it to the AES-ECB-DPA-FIA cores. The integrator is expected to fully verify the interface logic and test for proper connectivity. Features internal to the AES-ECB-DPA-FIA cores 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

The AES-ECB-DPA-FIA core implements and provides compliance with [FIPS-197] and [SP800-38A]. The TOE provides a possibility to load the keys and the data. After a cryptographic operation, the user has a possibility to invalidate i.e., to destroy the key using the Key Invalidate command.

For implementation and integration of the core inside a large system, basic command and error handling protocols are provided (cf. [ERS]) and supported to prevent and report misusage of the core during run time. In that sense, the AES-ECB-DPA-FIA core provides a fully functional, self-contained, and atomic AES-ECB hardware accelerator ready to be integrated into a larger system.

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

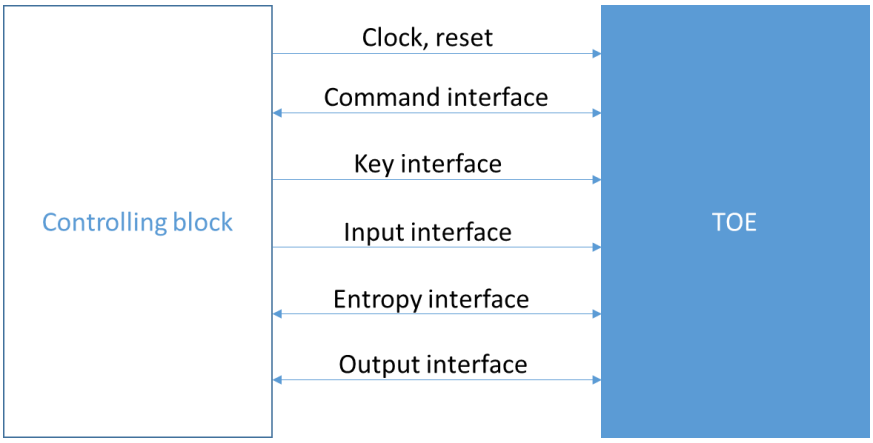

Figure 1 Interface Level Block Diagram

Figure 1 shows the interface level block diagram of the TOE and the controlling block (the test bench). Controlling commands are provided to the TOE through command and control interfaces with appropriate input data on input interface and key data on the key interface. That is, input and key data are provided to the core through different buses. Output is provided through the output interface. If an error is detected, error interface becomes active together with output interface.

One of the TOE interfaces is the entropy interface. A 128-bit random value is required to seed the core's internal pseudo-random number generator (PRNG) module after a reset. This PRNG is used for masking.

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 package that Rambus Inc. provides to the integrator includes the Synthesizable Verilog RTL description of the AES-ECB-DPA-FIA core, sample TCL synthesis constraints and primitive cell library templates, functional

test bench with the corresponding scripts, TCL script for post-layout verification and the TOE guidance [ERS], [IG] and [USG]. The whole lifecycle of the TOE can be seen as a part of Phase 2 for the Security IC.

2.6 Non-TOE Hardware/Software/Firmware

The non-TOE hardware/software/firmware required by the TOE includes the Security IC i.e. a system into which the TOE is integrated. Besides that, it may optionally include the embedded software running on the Security IC that has access to the TOE functionality.

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 ATE_DPT.2, AVA_VAN.5, 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 AES encryption and decryption. 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 one extra organizational security policy, which is added in order to address AES.

The AES functionality is further mapped to the objective for the TOE. The ST also contains three objectives for the environment, two of which originate from [PP]. The third one, namely, 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.

The SFRs used in this ST are a subset of the SFRs claimed in [PP] with an exception of FDP_ITC.1, which is offered by the PP to the ST writers as one of the options.

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 evaluation 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 AES 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.

Policy Name	Policy Definition
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.

5 Security Objectives

5.1 Security Objectives for the TOE

Objective Name	Objective Definition
O.AES	Cryptographic service AES The TOE provides secure hardware based cryptographic services for the AES for encryption and decryption.

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.

Objective Name	Objective Definition
OE.Identification	Identification during TOE Development and Production The TOE environment must enable accurate identification of the TOE during TOE development and production.

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.AES	P.Crypto-Service states that TOE provides secure hardware based cryptographic services while O.AES states that the TOE implements AES. Therefore the O.AES is 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.

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.
- There are no SFR iterations in this ST.

The SFRs defined in this ST are a subset of the SFRs defined in [PP] with an exception of FDP_ITC.1, which is offered by the PP to the ST writers as one of the options.

FCS_COP.1 Cryptographic operation – AES

FCS_COP.1.1 The TSF shall perform **decryption and encryption**[1] in accordance with a specified cryptographic algorithm **AES in ECB mode**[2] and cryptographic key sizes **128 bit, 256 bit**[3] that meet the following: **FIPS 197 [FIPS-197], NIST SP 800-38A [SP800-38A]**[4].

Application note 1. For some TOE configurations only one direction of the cryptographic operation is allowed. It means that in some cases the TOE will only be able to encrypt data and in some other cases the TOE will only be able to decrypt data. More details can be found in Section 2.3 and in [ERS].

FDP_ITC.1 Import of user data without security attributes

FDP_ITC.1.1 The TSF shall enforce the **none**[5] 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**[6].

Application note 2. 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 [IG].

[1] [assignment: list of cryptographic operations]

[2] [assignment: cryptographic algorithm]

[3] [assignment: cryptographic key sizes]

[4] [assignment: list of standards]

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

[6] [assignment: additional importation control rules]

FCS_CKM.4 Key destruction

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **setting the keys to all-zero values**[7] that meets the following: **none**[8].

Application note 3. By default the key is not erased after a cryptographic operation. This enables the user to execute several cryptographic operations in a row. In order to erase a key the user has to call a special command, i.e. the Key Invalidate command.

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)**[9].

Application note 4. The assignment is done in the same way as in [PP].

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**[10].

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

Application note 5. The assignment and the refinement are done in the same way as in [PP].

FDP_IFC.1 Subset information flow control

FDP_IFC.1.1 The TSF shall enforce the **Data Processing Policy**[11] on **all confidential data when they are processed or transferred by the TOE or by the Security IC Embedded Software**[12].

Application note 6. 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 7. 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 such attacks are infeasible

7.2 Security Assurance Requirements

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. The assurance level is EAL4 augmented with ATE_DPT.2, ALC_DVS.2, and AVA_VAN.5.

[7] [assignment: cryptographic key destruction method]

[8] [assignment: list of standards]

[9] [assignment: list of type of failures]

[10] [assignment: list of types of failures in the TSF]

[11] [assignment: information flow control SFP]

[12] [assignment: list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP]

Table 1 Security Assurance Requirements

Class	SAR
Class ADV: Development	Architectural design (ADV_ARC.1)
	Functional Specification (ADV_FSP.4)
	Implementation Representation (ADV_IMP.1)
	TOE Design (ADV_TDS.3)
Class AGD: Guidance documents	Operational User Guidance (AGD_OPE.1)
	Preparative procedures (AGD_PRE.1)
Class ALC: Life-cycle support	CM Capabilities (ALC_CMC.4)
	CM Scope (ALC_CMS.4)
	Delivery (ALC_DEL.1)
	Development Security (ALC_DVS.2)
	Lifecycle Definition (ALC_LCD.1)
	Tools and Techniques (ALC_TAT.1)
Class ASE: Security Target evaluation	Conformance claims (ASE_CCL.1)
	Extended components definition (ASE_ECD.1)
	ST introduction (ASE_INT.1)
	Security objectives (ASE_OBJ.2)
	Derived security requirements (ASE_REQ.2)
	Security problem definition (ASE_SPD.1)
	TOE summary specification (ASE_TSS.1)
Class AVA: Vulnerability analysis	Vulnerability analysis (AVA_VAN.5)
Class ATE: Tests	Coverage (ATE_COV.2)
	Depth (ATE_DPT.2)
	Functional Tests (ATE_FUN.1)
	Independent Testing (ATE_IND.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.

Table 2 SAR Refinements

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. Therefore, the following critical information have to be taken into account in order to ensure integrity and – if necessary confidentiality - (including protection against unauthorised disclosure, unauthorised modification or replacement and theft).** - **Logical design data and configuration data** - **Specific development aids, test and characterization related data, and material for integration support.** **The "development security documentation" shall describe all security measures related to the "TOE design and implementation" in the development environment as defined above.**
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.
ALC_CMC	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]	This refinement refers to mechanisms against physical attacks that require inspection of the layout or tests besides the TSFI. This refinement is regarded out of scope for the TOE, as physical attacks are not in scope and there is no layout to be verified.
	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]	This refinement refers to delivery acceptance procedures to identify the TOE in line with FAU_SAS.1, which is not claimed in this ST. This refinement is out of scope for the TOE.
	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]	This refinement is applicable without any adjustments, but it has been slightly modified for readability and to correct the reference for this ST. **The vulnerability analysis shall include a justification for the rating of information on the TOE available to the attacker and the usage of Open Samples since the protection of such information is demanded according to this Security Target (refer to refinement regarding "Development Security (ALC_DVS)", section 7.2).**

7.3 Security Requirements Rationale

7.3.1 Rationale for the Security Functional Requirements

The following table shows how the SFRs are combined to meet the security objective.

Objective	**TOE SFR**
O.AES	FCS_COP.1 Cryptographic operation – AES
	FDP_ITC.1 Import of user data without security attributes
	FCS_CKM.4 Key destruction
	FRU_FLT.2 Limited fault tolerance
	FPT_FLS.1 Failure with preservation of secure state
	FDP_IFC.1 Subset information flow control

This mapping differs from the one provided in [PP], where O.AES is mapped only to FCS_COP.1 and FCS_CKM.4. The reason for this deviation is that the TOE is only a part of the Security IC and the SFRs defined in this ST focus solely on the security of the TOE.

The six SFRs defined in this ST address various aspects of the AES calculation. The justification for each of the SFRs is given in Table 3 below

Table 3 SFR Justification

SFR	**Justification**
FCS_COP.1	This SFR requires the TOE to implement AES-ECB.
FDP_ITC.1	This SFR requires the TOE to implement key loading and data loading for the AES operations.
FCS_CKM.4	This SFR requires the TOE to be able to destroy AES keys.
FRU_FLT.2	This SFR addresses the limited fault tolerance for the AES operations.
FPT_FLS.1	This SFR states that the TOE shall preserve a secure state when a failure is detected during an AES calculation.
FDP_IFC.1	This SFR states that no user data such as input, output data, intermediate values, keys shall be transferred or processed in plain

7.3.2 Dependencies of the Security Functional Requirements

The following table shows the SFRs defined in this ST, their dependencies, and whether they are satisfied by other security requirements defined in this ST.

Table 4 SFR Dependencies

SFR	Dependencies	Fulfilled?
FCS_COP.1	FDP_ITC.1, FDP_ITC.2 or FCS_CKM.1	Yes, FDP_ITC.1
	FCS_CKM.4	Yes
FDP_ITC.1	FDP_ACC.1 or FDP_IFC.1	No, see the justification below
	FMT_MSA.3	No, see the justification below
FCS_CKM.4	FDP_ITC.1, FDP_ITC.2 or FCS_CKM.1	Yes, FDP_ITC.1
FRU_FLT.2	FPT_FLS.1	Yes
FPT_FLS.1	None	-
FDP_IFC.1	FDP_IFF.1	No, see the justification below

Dependency of FDP_ITC.1 on FDP_ACC.1/FDP_IFC.1 is not satisfied. The reason is as follows. The TOE implements no access control policies or information flow control policies.

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.

Dependency of FDP_IFC.1 on FDP_IFF.1 is not satisfied. The reason is as follows. The specification of FDP_IFF.1 would not capture the nature of the security functional requirement nor add any detail. There are no attributes to be addressed.

7.3.3 Rationale for the Security Assurance Requirements

The rationale for the Security Assurance Requirements repeats the rationale presented in [PP].

The assurance level EAL4 and the augmentation with the requirements ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5 were chosen in order to meet assurance expectations explained in the following paragraphs.

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.

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

7.3.4 Dependencies of the Security Assurance Requirements

The ST claims EAL4 augmented with AVA_VAN.5, ATE_DPT.2 and ALC_DVS.2, similarly to [PP]. The rationale for the SAR dependencies is the same as in [PP].

AVA_VAN.5 has dependencies to ADV_ARC.1 “Security architecture description”, ADV_FSP.2 “Security enforcing functional specification”, ADV_TDS.3 “Basic modular design”, ADV_IMP.1 “Implementation representation of the TSF”, AGD_OPE.1 “Operational user guidance”, and AGD_PRE.1 “Preparative procedures”. All these dependencies are satisfied by EAL4.

ALC_DVS.2 has no dependencies.

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

Therefore all SAR dependencies are fulfilled.

8 TOE Summary Specification

This section describes how the TOE meets each SFR.

8.1 FCS_COP.1 Cryptographic operation – AES

The TOE is the AES-ECB-DPA-FIA core. It implements and provides compliance with the following standards:

a) FIPS 197 [FIPS-197],

b) NIST SP 800-38A [SP800-38A].

The AES-ECB-DPA-FIA core implements dedicated hardware to support and accelerate AES-128 and AES-256 encryptions and decryptions using the ECB mode of operation.

The commands (also referred to as operations) that can be sent to the TOE are described in [ERS]. There are four commands in total:

- Core Initialization
- Key Load
- Cipher
- Key Invalidate

The Core Initialization command initializes the TOE. The Key Load command is used for key loading. The Cipher command can be used for encryption or decryption. The TOE provides a possibility to invalidate the key, which can be done using the Key Invalidate command.

8.2 FDP_ITC.1 Import of user data without security attributes

The TOE provides a possibility to load the key and the data. This can be done using the Key Load command and Cipher commands, respectively.

A key must be loaded before any Cipher operation can occur. Once loaded, the key is retained in the core unless flushed by a subsequent Key Invalidate operation. A key must be invalidated before loading a new key.

8.3 FCS_CKM.4 Key Destruction

The key destruction is done when the Key Invalidate command is executed. In this case all internal core registers (key-dependent data) are cleared.

After a Key Invalidate operation, the core is not able to perform any Cipher operations without loading a new AES key.

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.

The core goes back to the reset state after error consumption.

8.5.1 FDP_IFC.1 Subset information flow control

The TOE has a masked I/O data interface as well as a masked I/O key interface. In addition, the intermediate values and the output of the AES operation are masked.

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

End of Document