Common.SECC

Rule Book

Attachment 2 to Annex 3

Template for

Evaluation Technical Report (ETR) –
Part AGD & ADV

Version 2.2

22 December 2020

**Single Evaluation Report**

as part of the

Evaluation Technical Report

**ETR-Part** **AGD & ADV**

**Evaluation of CC Assurance Classes** **AGD & ADV**

**Evaluation Assurance Level** **EAL-POI**

Version:
##Version

Date:
##Date

Filename:
Attachment-2-for-Annex-3-AGD-ADV.docx

Product:
##TOE name (long)

Developer:
##Sponsor (short)
##Address sponsor

Evaluation Facility:
##Evaluation facility

Registration ID:
for future use

Evaluator:
##name Evaluators

Quality assurance:
##name QA

The following document is a template

Black text must be used without change. Especially headlines including the numbering of the headlines must not be changed.

Placeholders are marked in red colour and tagged with ##. The evaluator shall replace the placeholders with the actual value regarding the TOE consistently throughout all Single Evaluation Reports and documents.

The evaluator shall edit, if necessary, the red marked text and then change the colour to black. The green text must be considered by the evaluator and has to be deleted in the final version of the document.

Document Information

History of changes

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Approved | Changes |
| 2.0 | 23 January 2019 |  | After JTEMS comments |
| 2.1 | 1 April 2019 |  | Editorial changes |
| 2.2 | 22 December 2020 |  | Editorial changes |

**Document Invariants**

|  |  |  |
| --- | --- | --- |
| Name | Invariant (edit here) | Output value |
| Filename and size | calculated automatically | Automatic |
| Current version | ##Version | ##Version |
| Date | ##Date | ##Date |
| Classification | Company confidential | Company confidential |
| TOE name (long) | ##TOE name (long) | ##TOE name (long) |
| TOE name (short) | ##TOE name (short) | ##TOE name (short) |
| Sponsor (long) | ##Sponsor (long) | ##Sponsor (long) |
| Sponsor (short) | ##Sponsor (short) | ##Sponsor (short) |
| Developer (short) | ##Developer (short) | ##Developer (short) |
| Evaluation facility | ##Evaluation facility | ##Evaluation facility |
| Registration ID |   | For future use |
| Certification body (long) | Common Security Evaluation and Certification Consortium | Common Security Evaluation and Certification Consortium |
| Certification body (short) | Common.SECC | Common.SECC |

Table of contents

[I. Assurance Class AGD 8](#_Toc57360680)

[1 Impact in case of a delta process 8](#_Toc57360681)

[2 Basis of the evaluation and documentation used 8](#_Toc57360682)

[3 Evaluation objective / Dependencies 10](#_Toc57360683)

[4 Requirements for evidence and evaluation 11](#_Toc57360684)

[5 Evaluation results 12](#_Toc57360685)

[5.1 AGD\_OPE.1 Operational User Guidance 13](#_Toc57360686)

[5.1.1 AGD\_OPE.1.1E 13](#_Toc57360687)

[5.2 AGD\_PRE.1 Preparative Procedures 25](#_Toc57360688)

[5.2.1 AGD\_PRE.1.1E 25](#_Toc57360689)

[5.2.2 AGD\_PRE.1.2E 28](#_Toc57360690)

[5.3 Indications for Potential Vulnerabilities 31](#_Toc57360691)

[5.4 Missing Information 31](#_Toc57360692)

[5.5 Questions to / Conditions on the Developer 31](#_Toc57360693)

[5.6 Necessary Changes/Improvements 31](#_Toc57360694)

[5.7 Effects on other Documents 31](#_Toc57360695)

[II. Assurance Class ADV 32](#_Toc57360696)

[6 Impact in case of a delta process 32](#_Toc57360697)

[7 Basis of the evaluation and documentation used 32](#_Toc57360698)

[8 Evaluation objective / Dependencies 34](#_Toc57360699)

[9 Requirements for evidence and evaluation 35](#_Toc57360700)

[10 Evaluation results 37](#_Toc57360701)

[10.1 ADV\_ARC.1 Security architecture description 38](#_Toc57360702)

[10.1.1 ADV\_ARC.1.1E 38](#_Toc57360703)

[10.2 ADV\_FSP.2 Security-enforcing functional specification 46](#_Toc57360704)

[10.2.1 ADV\_FSP.2.1E 46](#_Toc57360705)

[10.2.2 ADV\_FSP.2.2E 53](#_Toc57360706)

[10.3 ADV\_TDS.1 Basic design 55](#_Toc57360707)

[10.3.1 ADV\_TDS.1.1E 55](#_Toc57360708)

[10.3.2 ADV\_TDS.1.2E 62](#_Toc57360709)

[10.4 Indications for Potential Vulnerabilities 64](#_Toc57360710)

[10.5 Missing Information 64](#_Toc57360711)

[10.6 Questions to / Conditions on the Developer 64](#_Toc57360712)

[10.7 Necessary Changes/Improvements 65](#_Toc57360713)

[10.8 Effects on other Documents 65](#_Toc57360714)

[III. Annex 66](#_Toc57360715)

[11 SFR coverage 66](#_Toc57360716)

[12 Glossary and list of acronyms 69](#_Toc57360717)

[13 Bibliography 70](#_Toc57360718)

1. Assurance Class AGD

# Impact in case of a delta process

*## In case of a delta process the impact resulting from the changes that have been applied to the product have to be discussed in this chapter only. Therefore, the evaluator might use the suitable parts of the Impact Analysis Report.*

*## The differences between the certified and the changed TOE should solely be discussed in this chapter. The remaining resp. following chapters should contain the appropriately marked changes with respect to the previous evaluation process. Furthermore, the following chapters should not mention the previous TOE to obtain a consistent description allowing further delta processes.*

## The current evaluation process is not a delta process.

# Basis of the evaluation and documentation used

The evaluation basis for the current ##TOE name (long) (TOE) is the version 3.1 of the Common Criteria (see [1], [2], and [3]) and the Common Evaluation Methodology (see [4]) in accordance with the Security Target [ST].

TOE identification according to [ST]:

|  |  |
| --- | --- |
| Hardware Version  | ##HW version |
| Firmware Version: | ##FW version |
| Guidance documents | ##guidance docs |

The subject of the current report is the evaluation of the guidance documents of the TOE as required by the Assurance Class AGD. This Assurance Class comprises two Assurance Families: AGD\_OPE (Operational User Guidance) and AGD\_PRE (Preparative Procedures), whereby each of them defines merely single Assurance Component AGD\_OPE.1 and AGD\_PRE.1, respectively, being independent of the evaluation assurance package chosen.

The following Developer Action Elements are required:

AGD\_OPE.1.1.D

AGD\_PRE.1.1.D

The developer contributions are listed in ETR.

There are no further references to former evaluations of the TOE or to any observation reports.

##Or, in case of a delta evaluation: the evaluator should here refer to the previous certification process and, optionally, give a short description of the main impacting factors.

# Evaluation objective / Dependencies

The objective of this particular Single Evaluation Report is to find out, whether and how the document [AGD] provided by the developer meets the requirements given by the Common Criteria, [3]. If the documentation does not meet the requirements or if it contains inconsistencies or deficiencies, it is also treated in this report.

In detail, the following assurance components are analysed in this report:

|  |  |
| --- | --- |
| AGD\_OPE.1 | Operational user guidance |
| AGD\_PRE.1 | Preparative procedures |

According to the Common Criteria, Part 3 these assurance components imply the following dependencies:

|  |  |
| --- | --- |
| AGD\_OPE.1 | ADV\_FSP.1 Basic functional specification |
| AGD\_PRE.1 | No dependencies |

# Requirements for evidence and evaluation

The evaluation was performed on the basis of the Common Evaluation Methodology [4]. The examinations conducted in this report are grouped into work units according to the CEM. The following table shows the dependencies between the work units defined by the CEM and the Common Criteria assurance elements defined by [3].

An evaluator action element shall be applied to the content and presentation of evidence element. The relevant application instructions are given in the respective work units as shown below:

| No. | evaluator action element (to be applied to content and presentation of evidence elements) | Refinement | related evaluator work units according to [4] | Verdict |
| --- | --- | --- | --- | --- |
|  | AGD\_OPE.1.1E |  |  | **##PASS##FAIL##INCONCLUSIVE** |
|  |  AGD\_OPE.1.1C |  | AGD\_OPE.1-1 |  |
|  |  AGD\_OPE.1.2C | yes | AGD\_OPE.1-2 |  |
|  |  AGD\_OPE.1.3C | yes | AGD\_OPE.1-3 |  |
|  |  AGD\_OPE.1.4C |  | AGD\_OPE.1-4 |  |
|  |  AGD\_OPE.1.5C |  | AGD\_OPE.1-5 |  |
|  |  AGD\_OPE.1.6C |  | AGD\_OPE.1-6 |  |
|  |  AGD\_OPE.1.7C |  | AGD\_OPE.1-7 |  |
|  |  |  | AGD\_OPE.1-8 |  |
|  | AGD\_PRE.1.1E |  |  | **##PASS##FAIL##INCONCLUSIVE** |
|  |  AGD\_PRE.1.1C |  | AGD\_PRE.1-1 |  |
|  |  AGD\_PRE.1.2C |  | AGD\_PRE.1-2 |  |
|  | AGD\_PRE.1.2E |  |  | **##PASS##FAIL##INCONCLUSIVE** |
|  |  no element assigned(this evaluator action element has to be applied to the TOE itself) |  | AGD\_PRE.1-3 |  |

Table 1: Requirements for evidence and evaluation

# Evaluation results

**Summary Verdict for the Assurance Class AGD:**
**##PASS ##FAIL##INCONCLUSIVE**.
*##If all work units are met:* Because all assurance requirements to be examined in this report have a positive evaluation result (PASS), the entire evaluation aspect (assurance class AGD) is assessed with PASS.

*##if a work unit is not fulfilled:* The TOE fulfils not all requirements of the assurance components AGD\_OPE.1 and AGD\_PRE.1. For further details please refer to Sections 5.4, 5.5 and 5.6 below.

## AGD\_OPE.1 Operational User Guidance

**Summary Verdict for the Assurance Component AGD\_OPE.1:**
**##PASS##FAIL##INCONCLUSIVE**.
*##If all work units are met:* The TOE meets all requirements of the assurance component AGD\_OPE.1. This result is based on the evaluator actions and work units documented below.

### AGD\_OPE.1.1E

Evaluator action element:

AGD\_OPE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

*Application Note from [PP]:*

*In particular, for SFR-supporting features related to Open Protocols, the following holds:*

*DTR H1: The evaluator shall not limit to the human users of the TOE. The evaluator shall ensure that the mapping between all SFR-supporting TSFIs and guidance is complete and consistent.*

*##note that the application note above does not require any additional evaluator action with respect to the standard assessment of AGD\_OPE.1 according to CC and CEM. Similar considerations hold for any of the refinements and application notes listed in [PP] with regard to the Open Protocols features.*

*Application note from [PP]:*

*Developing and manufacturing of the TOE are part of the developer phase. During the developer phase the initial cryptographic keys are loaded and if required also other cryptographic keys are loaded into the POI. Additionally, cryptographic keys can also be loaded during the user phase. The ST author shall define where the developer phase ends and where the user phase begins in relation to cryptographic key loading.*

*##note that the application note above does not require any additional evaluator action with respect to the standard ST evaluation tasks according to CC and CEM.*

In line with the structure presented in chapter 4 of this document, CC elements for content and presentation of evidence are discussed one by one in the following subsections in the context of their relevant work units.

#### AGD\_OPE.1.1C

AGD\_OPE.1.1C The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

##### AGD\_OPE.1-1

**[AGD\_OPE.1-1]** The evaluator ***shall examine*** the operational user guidance to determine that it describes, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

The current work unit deals with all user-accessible functions independent of their relevance for TSF, i.e. independent of the fact, whether a user accessible function is part of TSF or not.

Summary:

The evaluator found the information related in [AGD], ….

Analysis:

The evaluator shall analyse the relevant description and confirm whether the interfaces listed in document [AGD] are meaningful and correspond to the interfaces described in [ADV]. Inconsistencies should be checked. The evaluator shall verify whether for each user role and for each user-accessible interface, information on privileges and warnings is provided and is meaningful.

As an example of how the vendor provided the necessary information, the following table is an extraction from evidence [AGD]:

| **User role** | **Available interfaces** | **Privileges and warnings** | **Parameters** |
| --- | --- | --- | --- |
| ‘Merchant/Attendant’ |  |  |  |
| ‘Terminal Administrator/Terminal Management System’ |  |  |  |
| ‘Application Developer’ |  |  |  |

Table 2: User roles and user available interfaces

Assessment and Verdict:

The analysis allowed the evaluator to conclude that:

* all user roles are listed in the guidance documentation;
* all user-accessible TOE functions are stated in guidance;
* Privileges and warning messages are stated (when appropriate) for user roles and indication of documents with further details is provided.

Hence, the current work unit is **fulfilled (pass) ##or not (fail).**

#### AGD\_OPE.1.2C

AGD\_OPE.1.2C The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

*Application Note from [PP]:*

*In particular, for SFR-supporting features related to Open Protocols, the following holds:*

*DTR H1: The device has security guidance that describes how protocols and services must be used for each TSFI. The operational user guidance shall also describe how to use the available protocol or service interfaces provided by the TOE in a secure manner. The operational guidance not only describes human interactions with the TOE but also the secure integration with other systems, devices or applications.*

*##note that the application note above does not require any additional evaluator action with respect to the standard assessment of AGD\_OPE.1 according to CC and CEM. Similar considerations hold for any of the refinements and application notes listed in [PP] with regard to the Open Protocols features.*

##### AGD\_OPE.1-2

**[AGD\_OPE.1-2]** The evaluator ***shall examine*** the operational user guidance to determine that it describes, for each user role, the secure use of the available interfaces provided by the TOE.

The current work unit deals with secure use of the TOE interfaces independent of their relevance for the TSF. It is assumed that TSF and non-TSF portions of the TOE are effectively separated and do not interfere with each other. Any use of non-TSF interfaces must not affect the TSF. Therefore, merely a *functional* description of non-TSF interfaces in the guidance documentation suffices.

Description of the TSF-interfaces (TSFI) must be detailed. It must focus on their *secure* use. An examination of such interfaces is subject of the next work unit (AGD\_OPE.1-3).

The appropriate TOE’s usage in the context of its environment will be analysed in work unit AGD\_OPE.1-6.

Summary:

The evaluator found the relevant information in [AGD], ….

Analysis:

For the analysis, the evaluator shall review the relevant documents where details on the secure usage of each interface are provided and check whether there is any contradictions nor missing information.

Assessment and Verdict:

The evaluator reviewed all guidance documents and determined that they describe, for each user role, the secure use of the available interfaces provided by the TOE.

The evaluator determined that the TOE has security guidance that describes how protocols and interfaces must be used for each interface that is accessible by the device applications.

Hence, the current work unit is in this part **fulfilled (pass) ##or not (fail).**

#### AGD\_OPE.1.3C

AGD\_OPE.1.3C The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

*Application Note:*

*In particular, for SFR-supporting features the following holds:*

*PCIH3: The device has guidance for key management describing how keys and certificates must be used.*

1. The key-management guidance is at the disposal of internal users, and/or of application developers, system integrators, and end-users of the platform.
2. Key-management security guidance describes the properties of all keys and certificates that can be used by the platform.
3. Key-management security guidance describes the responsibilities of the platform vendor, application developers, system integrators, and end-users of the platform.
4. Key-management security guidance ensures secure use of keys and certificates

##### AGD\_OPE.1-3

**[AGD\_OPE.1-3]** The evaluator ***shall examine*** the operational user guidance to determine that it describes, for each user role, the available security functionality and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

The current work unit deals with a secure use of TOE interfaces being relevant for the TSF, i.e. TSFI. All non-TSF interfaces have already been considered in the previous work unit (AGD\_OPE.1-2). It is assumed that TSF and non-TSF portions of the TOE are effectively separated and do not interfere each other. Therefore, the current work unit exclusively focuses on TSF and TSFI.

Summary:

The evaluator found the information related in [AGD], ….

Analysis:

##The evaluator reviewed the [AGD] documents while addressing work unit AGP\_OPE.1-2. Note that extensive details on parameters (and secure values) applicable to APIs are provided by the vendor in documents [AGD] and have been reviewed by the evaluator in work units ADV\_FSP.2-4 and ADV\_FSP.2-5.

Assessment and Verdict:

Based on the analysis and results in the context of the current work unit, the evaluator determines that the operational user guidance describes (##or not), for each user role, the available security functionality and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

Therefore the current work unit is **fulfilled (pass) ##or not (fail).**

#### AGD\_OPE.1.4C

AGD\_OPE.1.4C The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

##### AGD\_OPE.1-4

**[AGD\_OPE.1-4]** The evaluator ***shall examine*** the operational user guidance to determine that it describes, for each user role, each type of security-relevant event relative to the user functions that need to be performed, including changing the security characteristics of entities under the control of the TSF and operation following failure or operational error.

The current work unit deals with security-relevant events, which may occur during operation/configuration of the TOE and being visible at the user-accessible interfaces, with the aim to enable a user of the TOE to react on such events.

Summary:

The evaluator found the information related in [AGD], ….

Analysis:

##The evaluator analysed descriptions of security-relevant events and came to the conclusion that they are sufficient to identify the source of such an event and the responses of each user in order to maintain a secure state.

From review of the afore mentioned documents, the evaluator identified the following security-relevant events that have been indicated to the following users:

|  |  |
| --- | --- |
| User Role | Security-relevant events and recommended actions |
| ‘Merchant/Attendant’ |  |
| ‘Terminal Administrator/Terminal Management System’ |  |
| ‘Application Developer’ |  |

 Table 3 Security-relevant events

Assessment and Verdict:

Based on the result of the analysis above, the evaluator determines that the operational user guidance describes (##or not), for each user role, each type of security-relevant event relative to the user functions that need to be performed, including changing the security characteristics of entities under the control of the TSF and operation following failure or operational error.

Hence, the current work unit is **fulfilled (pass) ##or not (fail).**

#### AGD\_OPE.1.5C

AGD\_OPE.1.5C The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

##### AGD\_OPE.1-5

**[AGD\_OPE.1-5]** The evaluator ***shall examine*** the operational user guidance and other evaluation evidence to determine that the guidance identifies all possible modes of operation of the TOE (including, if applicable, operation following failure or operational error), their consequences and implications for maintaining secure operation.

Chapter 16 (Vulnerability Assessment) of the Common Criteria, Part 3: Common Criteria for Information Technology Security Eval-uation, Part 3: Security Assurance Components, Version 3.1, Revision 5, April 2017, CCMB-2017-04-003 [3] addresses operational vulnerability and misuse investigation in § 452. These ‘misuse investigation’ activities depend on the elements AGD\_OPE.1.5C–1.7C and parts of assurance family AGD\_PRE.

Summary:

The evaluator found the information related in [AGD], ….

Analysis:

The evaluator shall analyse all possible modes of operation of the TOE as described in [AGD]. The TOE contains … modes of operation. The modes are…

Assessment and Verdict:

Based on the result of the analysis above, the evaluator determines that guidance identifies (##or not) all possible modes of operation of the TOE (including, if applicable, operation following failure or operational error), their consequences and implications for maintaining secure operation.

Hence, the current work unit is **fulfilled (pass) ##or not (fail).**

#### AGD\_OPE.1.6C

AGD\_OPE.1.6C The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

##### AGD\_OPE.1-6

**[AGD\_OPE.1-6]** The evaluator ***shall examine*** the operational user guidance to determine that it describes, for each user role, the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

This sub-activity is very important to ensure the consistency of the TSF. Correctness and effectiveness of TSF is examined in several assurance components. The organisational and technical measures required by the TOE operational environment are addressed in assurance class AGD (WUs AGD\_OPE.1-6 and AGD\_PRE.1-2) only.

The guidance shall describe organisational and technical measures that have to be followed by the users in order to achieve the security objectives for the TOE operational environment. The current work unit contributes to misuse investigation by analysis, whether the environmental measures described in the guidance are indeed sufficient for enforcing of the security objectives for the TOE environment.

Summary:

The evaluator found the relevant information in [AGD], ….

Analysis:

##In order to facilitate the analysis of appropriateness of the TOE external security measures, the developer created the following table mapping the security objectives for the operational

environment (as described in the [ST]) to the security measures to be followed by each user role to implement such security objectives. The following table can be found in document [AGD].

| security objectives for the operational environment (from [ST]) | Security Measures per user role |
| --- | --- |
| OE.POISurveyProcedural measures like inspections and guidance will prevent manipulations of the TOE enclosure. Procedural measures like inspections and guidance for manipulations of the IC card interface will prevent attacks based on electronic circuits mounted at the IC card interface of the TOE's Card Reader. Those responsible for the TOE establish and implement procedures for training and vetting administrators of the TOE, or training the supervisors. | ## |
| OE.MerchantSurveyIn case of a fraudulent Merchant performing attacks via manipulations of the enclosure or the interfaces of the TOE, especially the IC card interface, the payment schemes shall detect manipulations of a large number of payment transactions at the same merchant with their surveillance systems. | ## |
| OE.UserEducationThe Cardholder shall be informed by his/her bank to keep the PIN secret. | ## |
| OE.SecureDevicesThe payment application providers have chosen appropriate security measures to protect devices interacting with the TOE e.g. the IC card. | ## |
| OE.KeyManagementCryptographic keys are securely managed. Especially the generation and installation of cryptographic keys and certificates are done in a manner that private or secret cryptographic keys are protected against disclosure and all cryptographic keys are protected against modification when they are processed outside the POI. Furthermore, there are procedures that support and maintain the unique identification of the TOE based on unique cryptographic keys for the protection of the online interface. | ## |
| OE.PinAndCardManagementUser PINs as well as the IC Cards are securely managed by the Issuer. Especially the PIN as well as the IC Card transfer between Issuer and Cardholder takes place in a manner that the confidentially of the PINs is ensured and the misuse of the cards is prevented by organisational measures. | ## |
| OE.WellFormedPayApp Well-formed Payment ApplicationPayment Applications implemented on the POI will make use of the security mechanisms provided by the TOE in a sense that the security of the defined assets as specified in this PP cannot be affected. The payment application is especially responsible for the transaction flow of a payment transaction (e.g. performing a payment transaction as result of verification of risk management parameter and other verification results like PIN verification). | ## |
| OE.LocalDevicesThe environment of the TOE shall protect the connection between Local Devices and other POI components via security organisational measures or by using the cryptographic means provided by the POI. | ## |

 Table 4: Mapping of security objectives for the operational environment and security measures implemented by user roles

Assessment and Verdict:

Based on the result of the analysis above, the evaluator determines that operational user guidance describes (##or not), for each user role, the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

Hence, the current work unit is **fulfilled (pass) ##or not (fail).**

#### AGD\_OPE.1.7C

AGD\_OPE.1.7C The operational user guidance shall be clear and reasonable.

##### AGD\_OPE.1-7

**[AGD\_OPE.1-7]** The evaluator ***shall examine*** the operational user guidance to determine that it is clear.

The current work unit contributes to misuse investigation by analysis, whether the guidance can reasonably be misconstrued by a human user.

Summary:

The evaluator reviewed the entire set of vendor evidences that constitute the guidance documentations [AGD]. In order to determine the completeness and correctness of the guidance documentation, the evaluator compared the information in guidance with the information provided by the vendor in [ADV] and all [DESIGN\_DOCS].

Analysis:

##As a result of the analysis:

* the evaluator did not find any inconsistencies:
	+ between information stated in different guidance documents and/or
	+ among different sections within the same guidance document.
* The evaluator did not find any missing information. All details that the evaluator expected to find about secure usage of any of the interfaces were correctly presented by the vendor.
* The evaluator did not find misplaced information. All details that the evaluator expected to find in any specific guidance document were indeed found in that guidance document.
* The evaluator did not find misleading information that might cause a user to assume that an insecure usage of an interface is actually secure.

Assessment and Verdict:

Based on the result of the analysis above, the evaluator came to the conclusion that the guidance cannot (## or can) reasonably be misunderstood by a human user. . If the user follows the guidance documentation [AGD] no situation will occur (##or: a situation may occur) where the TOE is operated in an insecure state while the user presumes the state is secure.

Therefore the evaluator determines that the operational user guidance is clear. Hence, the current work unit is **fulfilled** (pass).

##### AGD\_OPE.1-8

**[AGD\_OPE.1-8]** The evaluator ***shall examine*** the operational user guidance to determine that it is reasonable.

The current work unit contributes to misuse investigation by analysis, whether assumptions about the TOE’s usage and demands on its operational environment are realistic and plausible.

Summary:

The evaluator performed this evaluation tasks while performing the previous work units (in particular, see AGD\_OPE.1-7).

The evaluator reviewed the entire set of vendor evidences that constitute the guidance documentation [AGD]. In order to determine whether the guidance documentation is reasonable, the evaluator compared the information in guidance with the information provided by the vendor in [ADV] and all [DESIGN\_DOCS].

Analysis:

##In order to carry out the analysis, the evaluator searched in an informal way for:

* any requirements, assumptions or recommendation regarding the secure usage of the TOE within the user guidance seeming to be unreasonable or unrealistic and did not find any.
* any requirements, assumptions or recommendation regarding the operational environment of the TOE within the user guidance being not consistent with the ST and did not find any.

Assessment and Verdict:

Based on the result of the analysis above, the evaluator concluded that the assumptions about the TOE’s usage and demands on its operational environment described in the user guidance are (## or not) realistic and plausible.

Therefore the evaluator determines that the operational user guidance is reasonable. Hence, the current work unit is **fulfilled** (pass).

**Verdict for AGD\_OPE.1.1E:**
**##PASS##FAIL##INCONCLUSIVE**
The evaluator confirms (##disproves) that the information provided in the analysed documentation meet all requirements for content and presentation of evidence.

## AGD\_PRE.1 Preparative Procedures

**Summary Verdict for the Assurance Component AGD\_PRE.1:**
**##PASS##FAIL##INCONCLUSIVE**
*##If all work units are met:* The TOE meets all requirements of the assurance component AGD\_PRE.1. This result is based on the evaluator actions and work units documented below.

### AGD\_PRE.1.1E

Evaluator action element:

AGD\_PRE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

*Application Note:*

*In particular, for SFR-supporting features related to Open Protocols, the following holds:*

*DTR H2 The device has guidance that describes the default configuration for each TSFI of the following types: Link Layer Protocols, IP Protocols, Security Protocols, IP Services. The evaluator shall ensure that the mapping between all SFR-supporting TSFIs and preparative procedures is complete and consistent.*

*##note that the application note above does not require any additional evaluator action with respect to the standard assessment of AGD\_PRE.1 according to CC and CEM. Similar considerations hold for any of the refinements and application notes listed in [PP] with regard to the Open Protocols features.*

In line with the structure presented in chapter 4 of this document, CC elements for content and presentation of evidence are discussed one by one in the following subsections in the context of their relevant work units.

#### AGD\_PRE.1.1C

AGD\_PRE.1.1C The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

##### AGD\_PRE.1-1

**[AGD\_PRE.1-1]** The evaluator ***shall examine*** the provided acceptance procedures to determine that they describe the steps necessary for secure acceptance of the TOE in accordance with the developer's delivery procedures.

This work unit deals with the minimal requirements on the content of acceptance procedures, if any. The general objective of any acceptance procedure is ensuring that the delivered TOE is the complete evaluated instance. This general objective will be achieved by several single measures like checking TOE version, verifying integrity of the TOE and authenticity of the TOE dispatcher as well as applying a structured well‑defined acceptance procedure.

Summary:

The evaluator found the information related in [AGD], ….

Analysis:

##The document [AGD] defines an installation/configuration chain before the TOE becomes operational. Due to this fact the TOE developer addresses several acceptance procedures for different ‘delivery interfaces’ (the TOE is passed from the TOE manufacturer to the first user, then to the next user in this installation/configuration chain through such ‘delivery interfaces’).

Assessment and Verdict:

Based on the result of the analysis above, the evaluator determines that the procedures necessary for the secure acceptance of the delivered TOE have been provided (##or: have not been provided, but the TOE developer sufficiently reasoned (##or not), why it is not possible that the TOE user will use a product being not the TOE, but believing it were the TOE).

Based on the result of the analysis above, the evaluator concluded that the acceptance procedures cover (##or not) all the delivery interfaces being appropriate for the TOE. The acceptance procedures, for each delivery interface, describe the steps necessary for secure acceptance of the TOE in ##not sufficient details.

Therefore the evaluator determines that the acceptance procedures describe (##or not) the steps necessary for secure acceptance of the TOE in accordance with the developer's delivery procedures.

Furthermore, he determines that the acceptance procedures described are ##not appropriate to ensure that the delivered TOE is the complete evaluated instance.

Hence, the current work unit is **fulfilled (pass) ##or not (fail).**

#### AGD\_PRE.1.2C

AGD\_PRE.1.2C The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

##### AGD\_PRE.1-2

**[AGD\_PRE.1-2]** The evaluator ***shall examine*** the provided installation procedures to determine that they describe the steps necessary for secure installation of the TOE and the secure preparation of the operational environment in accordance with the security objectives in the ST.

This work unit deals with the minimal requirements on the content of preparative procedures, if any.

[3], Chapter 16 ‘Vulnerability Assessment’, § 452 addresses operational vulnerability and misuse investigation. These ‘misuse investigation’ activities are described and have to be done in the context of the elements AGD\_PRE.1.2C (Work Unit AGD\_PRE.1-2) and the evaluator action AGD\_PRE.1.2E as well as partially within the assurance family AGD\_OPE.

This sub-activity is very important for getting the TSF consistent. The description of the preparative procedures shall contain organisational and technical measures enforcing achievement of the security objectives for the TOE operational environment and having to be followed by the users installing/configuring the TOE. While correctness and effectiveness of TSF is being examined within several different assurance components, the assurance class AGD (Work units AGD\_OPE.1-6 and AGD\_PRE.1-2) is the only aspect, where appropriateness of organisational and technical measures, having to be enforced in the TOE operational environment, is treated.

Summary:

The evaluator found the information related in [AGD], ….

Analysis:

##The document [AGD] defines an installation/configuration chain before the TOE becomes operational. Due to this fact the TOE developer addresses several preparative procedures for different parties being authorised to install and to configure the TOE.

References to Work Unit AGD\_OPE.1-6 is expected here, for completeness.

Assessment and Verdict:

Based on the result of the analysis above, the evaluator determines that the procedures necessary for the secure installation of the TOE have been provided (##or: have not been provided, but the TOE developer sufficiently reasoned (##or not), why such a procedure is not necessary).

Based on the result of the analysis above, the evaluator determines that the preparative procedures address ##not all the user roles being authorised to install/configure the TOE.

Furthermore, the evaluator determines that the preparative procedures, for each relevant user role, describe the steps necessary for secure installation/configuration of the TOE in ##not sufficient details, so that they are ##not clearly understandable for the user.

Besides this, the evaluator determines that preparative guidance describes (##or not), for each user role possible for the preparative procedures, the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

Overall, the evaluators determine that the installation procedures describe (##or not) the steps necessary for secure installation of the TOE and the secure preparation of the operational environment in accordance with the security objectives in the ST. The preparative procedures described are ##not appropriate to ensure that the TOE is installed and configured in such a way, that it will be operated in the scope of validity of its security certificate.

Hence, the current work unit is **fulfilled (pass) ##or not (fail).**

**Verdict for AGD\_PRE.1.1E:**
**##PASS##FAIL##INCONCLUSIVE**
The evaluator confirms (##disproves) that the information provided meet all requirements for content and presentation of evidence.

### AGD\_PRE.1.2E

Evaluator action element:

AGD\_PRE.1.2E The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

In line with the structure presented in chapter 4 of this document, CC elements for content and presentation of evidence are discussed one by one in the following subsections in the context of their relevant work units.

##### AGD\_PRE.1-3

**[AGD\_PRE.1-3]** The evaluator ***shall perform*** all user procedures necessary to prepare the TOE to determine that the TOE and its operational environment can be prepared securely using only the supplied preparative procedures.

This work unit enforces a *practical* assessment of the preparative guidance including the acceptance and the preparative procedures.

The aim of the current sub-activity is to advance the TOE from its deliverable state through the acceptance and installation/configuration procedures to its operational state using only the preparative guidance supplied.

The current work unit contributes to misuse investigation by a practical assessment, whether the preparative guidance enables each user, involved into acceptance, installation and configuration of the TOE, to perform his task(s) appropriately using only the supplied preparative guidance.

Before the evaluator started with the current sub-activity, he successfully completed all previous work units of the current assurance component.

Summary:

Due to the character of the current evaluator action it is not possible to refer to concrete sections or chapters in [AGD]. The evaluator refers here to the work units AGD\_PRE.1-1 to AGD\_PRE.1-2, where the content and the structure of the preparative guidance were analysed in detail.

Analysis:

##In the context of the current evaluator action the evaluator performed the following steps:

1. The evaluator checked that the TOE is exactly in the state as it is delivered from its manufacturer. He also used this TOE for all next steps.
2. The evaluator performed all acceptance steps as described in [AGD] using merely the description of the acceptance procedure.
3. The evaluator carried out all preparative steps as described in [AGD] using merely the description of the preparative procedure (installation/customising/configuration) at the accepted TOE.
4. The evaluator investigated the configuration of the ‘final’ TOE in its operational life phase and compared it with the TOE description in the ST.

Assessment and Verdict:

Based on the results of the activities above, the evaluator confirms (##or disproves in case of any difficulties encountered during this activity indicating incomplete, unclear or unreasonable guidance) that it is not possible that the TOE user will accept a product being not the TOE, but believing it were the TOE.

Furthermore, the evaluator confirms (##or disproves in case of any difficulties encountered during this activity indicating incomplete, unclear or unreasonable guidance) that the ‘final’ TOE in its operational life phase is identical to the TOE as it is described in the ST (i.e. the TOE is operated in the scope of validity of its security certificate).

Therefore the evaluator determines that the TOE and its operational environment can (##or cannot) be prepared securely using only the supplied preparative user guidance.

Hence, the current work unit is **fulfilled (pass) ##or not (fail).**

**Verdict for AGD\_PRE.1.2E:**
**##PASS##FAIL##INCONCLUSIVE**
The evaluator confirms (##or disproves) that the TOE can be prepared securely for operation.

## Indications for Potential Vulnerabilities

##The evaluator did not find any potential vulnerability indicated by the current evaluation aspect.

## Missing Information

##There is no further information, which the developer/sponsor has to provide.

*##In the case of the verdict ‘inconclusive’, the evaluator is expected to put some issues into the sections ‘Missing Information’ or ‘Questions to and Conditions on the Developer’ of his single evaluation report, cf. AIS14.*

## Questions to / Conditions on the Developer

##There are no questions, recommendations to or conditions on the developer.

*##In the case of the verdict ‘inconclusive’, the evaluator is expected to put some issues into the sections ‘Missing Information’ or ‘Questions to and Conditions on the Developer’ of his single evaluation report, cf. AIS14.*

## Necessary Changes/Improvements

##No changes are required from the developer.

*##In the case of the verdict ‘fail’, the evaluator is expected to put some issues into the section ‘Necessary Changes/Improvements’ of his single evaluation report, cf. AIS14.*

## Effects on other Documents

##There are no effects on other documents.

1. Assurance Class ADV

# Impact in case of a delta process

*## In case of a delta process the impact resulting from the changes that have been applied to the product have to be discussed in this chapter only. Therefore, the evaluator might use the suitable parts of the Impact Analysis Report.*

*## The differences between the certified and the changed TOE should solely be discussed in this chapter. The remaining resp. following chapters should contain the appropriately marked changes with respect to the previous evaluation process. Furthermore the following chapters should not mention the previous TOE to obtain a consistent description allowing further delta processes.*

## The current evaluation process is not a delta process

# Basis of the evaluation and documentation used

The evaluation basis for the current ##TOE name (long) (TOE) is the version 3.1 of the Common Criteria (see [1] , [2], and [3]) and the Common Evaluation Methodology (see [4]) in accordance with the Security Target [ST].

TOE identification according to [ST]:

|  |  |
| --- | --- |
| Hardware Version  | ##HW version |
| Firmware Version: | ##FW version |
| Guidance documents | ##guidance docs |

The subject of the current report is the evaluation of the development of the TOE as required by the Assurance Class ADV. This Assurance Class comprises six Assurance Families: (ADV\_ARC) Security Architecture, (ADV\_FSP) Functional Specification and (ADV\_TDS) TOE Design, whereby each of them defines several Assurance Components, respectively, being dependent of the evaluation assurance package chosen.

The Developer Action Elements required for the developer are the following:

ADV\_ARC.1.1D
ADV\_ARC.1.2D
ADV\_ARC.1.3D

ADV\_FSP.2.1D
ADV\_FSP.2.2D

ADV\_TDS.1.1D,
ADV\_TDS.1.2D

The developer contributions are listed in ETR.

There are no further references to former evaluations of the TOE or to any observation reports.

*##Or, in case of a delta evaluation: The evaluator should here refer to the previous certification process and, optionally, give a short description of the main impacting factors.*

# Evaluation objective / Dependencies

The objective of this particular Single Evaluation Report is to find out, whether and how the document [ADV] provided by the developer meets the requirements given by the Common Criteria, [3]. If the documentation does not meet the requirements or if it contains inconsistencies or deficiencies, it is also treated in this report.

In detail, the following assurance components are analysed in this report:

|  |  |
| --- | --- |
| ADV\_ARC.1 | Security architecture description |
| ADV\_FSP.2 | Security-enforcing functional specification |
| ADV\_TDS.1 | Basic design |

According to the Common Criteria, Part 3 these assurance components imply the following dependencies:

|  |  |
| --- | --- |
| ADV\_ARC.1 | ADV\_FSP.1 Basic Functional SpecificationADV\_TDS.1 Basic design |
| ADV\_FSP.2 | ADV\_TDS.1 Basic design  |
| ADV\_TDS.1 | ADV\_FSP.2 Security-enforcing functional specification |

# Requirements for evidence and evaluation

The evaluation was performed on the basis of the Common Evaluation Methodology [4]. The work units are grouped according to the CEM. The following table shows the dependencies between the work units defined by the CEM and the Common Criteria assurance elements defined by [3].

An evaluator action element shall be applied to the content and presentation of evidence element. The relevant application instructions are given in the respective work units as shown below:

| No. | evaluator action element (to be applied to content and presentation of evidence) | Refinement | respective evaluator work units according to [4] | Verdict |
| --- | --- | --- | --- | --- |
|  | ADV\_ARC.1.1E |  |  | **##PASS ##FAIL ##INCONCLUSIVE** |
|  |  ADV\_ARC.1.1C |  | ADV\_ARC.1-1 |  |
|  |  ADV\_ARC.1.2C | yes | ADV\_ARC.1-2 |  |
|  |  ADV\_ARC.1.3C | yes | ADV\_ARC.1-3 |  |
|  |  ADV\_ARC.1.4C | yes | ADV\_ARC.1-4 |  |
|  |  ADV\_ARC.1.5C | yes | ADV\_ARC.1-5 |  |
|  | ADV\_FSP.2.1E |  |  | **##PASS ##FAIL ##INCONCLUSIVE** |
|  |  ADV\_FSP.2.1C |  | ADV\_FSP.2-1 |  |
|  |  ADV\_FSP.2.2C |  | ADV\_FSP.2-2 |  |
|  |  |  | ADV\_FSP.2-3 |  |
|  |  ADV\_FSP.2.3C | yes | ADV\_FSP.2-4 |  |
|  |  |  | ADV\_FSP.2-5 |  |
|  |  ADV\_FSP.2.4C |  | ADV\_FSP.2-6 |  |
|  |  ADV\_FSP.2.5C |  | ADV\_FSP.2-7 |  |
|  |  ADV\_FSP.2.6C |  | ADV\_FSP.2-8 |  |
|  | ADV\_FSP.2.2E |  |  | **##PASS ##FAIL ##INCONCLUSIVE** |
|  |  |  | ADV\_FSP.2-9 |  |
|  |  |  | ADV\_FSP.2-10 |  |
|  | ADV\_TDS.1.1E |  |  | **##PASS ##FAIL ##INCONCLUSIVE** |
|  |  ADV\_TDS.1.1C |  | ADV\_TDS.1-1 |  |
|  |  ADV\_TDS.1.2C |  | ADV\_TDS.1-2 |  |
|  |  ADV\_TDS.1.3C | yes | ADV\_TDS.1-3 |  |
|  |  ADV\_TDS.1.4C |  | ADV\_TDS.1-4 |  |
|  |  ADV\_TDS.1.5C |  | ADV\_TDS.1-5 |  |
|  |  ADV\_TDS.1.6C |  | ADV\_TDS.1-6 |  |
|  | ADV\_TDS.1.2E |  |  | **##PASS ##FAIL ##INCONCLUSIVE** |
|  |  |  | ADV\_TDS.1-7 |  |
|  |  |  | ADV\_TDS.1-8 |  |

# Evaluation results

**Summary Verdict for the Assurance Class ADV:**
**##PASS ##FAIL ##INCONCLUSIVE**.
*##If all work units are met:* Because all assurance requirements to be examined in this report have a positive evaluation result (PASS), the entire evaluation aspect (assurance class ADV) is assessed with PASS.

*##if a work unit is not fulfilled:* The TOE does not fulfil all requirements of the assurance components ADV\_ARC.1, ADV\_FSP.1, ADV\_FSP.2, ADV\_FSP.3, ADV\_FSP.4, ADV\_FSP5, ADV\_TDS.1, ADV\_TDS2. For further details please refer to Sections 5.4, 5.5 and 5.6 below.

## ADV\_ARC.1 Security architecture description

**Summary Verdict for the Assurance Component ADV\_ARC.1:**
**##PASS ##FAIL ##INCONCLUSIVE**.
*##If all work units are met:* The TOE meets all requirements of the assurance component ADV\_ARC.1.This result is based on the evaluator actions and work units documented below.

### ADV\_ARC.1.1E

Evaluator action element:

ADV\_ARC.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

In line with the structure presented in chapter 9 of this document, CC elements for content and presentation of evidence are discussed one by one in the following subsections in the context of their relevant work units.

#### ADV\_ARC.1.1C

ADV\_ARC.1.1C The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.

##### ADV\_ARC.1-1

**[ADV\_ARC.1-1]** The evaluator **shall examine** the security architecture description to determine that the information provided in the evidence is presented at a level of detail commensurate with the descriptions of the SFR-enforcing abstractions contained in the functional specification and TOE design document.

The current work unit deals with the level of detail required for the security architecture description. The security architecture description shall be presented at a level of detail commensurate with the descriptions of the SFR-enforcing abstractions contained in the functional specification and TOE design documentation.

Summary:

The evaluator found the related information that will be summarised in the following in ##… .

Analysis:

The evaluator’s analysis description shall show that security architecture description is presented at a level of detail commensurate with the descriptions of the SFR-enforcing abstractions contained in the functional specification and TOE design documentation.

Assessment and Verdict:

The evaluator has examined that ##not all parts of the security architecture description are presented at a level of detail commensurate with the descriptions of the SFR-enforcing abstractions contained in the functional specification and TOE design documentation. There was ##no evidence found that parts of the security architecture description are presented at a level of detail commensurate with the descriptions of the SFR-enforcing abstractions contained in the functional specification and TOE design documentation.

Hence, the current work unit is **fulfilled** (pass) or is **not fulfilled** (fail).

#### ADV\_ARC.1.2C

ADV\_ARC.1.2C The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.

*Refinement from [PP]:*

*If the POI\_DATA package is included in the set of evaluated SFRs, the security architecture description shall describe the security domains that result from the application separation principle (requirement EPCN2), specified in FDP\_ACC.1/POI\_DATA, FDP\_ACF.1/POI\_DATA and FDP\_RIP.1/POI\_DATA. This design information shall explain the mechanisms used to achieve application separation. It shall describe how isolation of payment application data is achieved, how the correct execution of the payment application is enforced as well as the management of Cardholder communication interface during payment application execution and how interference from other applications is avoided.*

##### ADV\_ARC.1-2

**[ADV\_ARC.1-2]** The evaluator **shall examine** the security architecture description to determine that it describes the security domains maintained by the TSF.

The current work unit deals with the description of the security domains maintained by the TSF. These security domains shall be described in the security architecture description.

Summary:

The evaluator found the related information that will be summarised in the following in ##… .

Analysis:

The evaluator’s analysis description shall show that the security architecture description describes the security domains maintained by the TSF.

##The evaluator has identified the following security domains...

##The security architecture description describes the following security domains…

The evaluator shall analyse whether the security architecture documentation describes the security domains that result from the application separation principle as defined in the refinement of ADV\_ARC.1.2C.

Assessment and Verdict:

The evaluator has examined for the security domains maintained by the TSF that the security architecture description describes ##does not describe these security domains. There was ##no evidence found for the security architecture description provided that the security architecture description describes the security domains maintained by the TSF.

Hence, the current work unit is **fulfilled** (pass) or is **not fulfilled** (fail).

#### ADV\_ARC.1.3C

ADV\_ARC.1.3C The security architecture description shall describe how the TSF initialisation process is secure.

*Refinement from [PP]:*

*In particular, for SFR-supporting features related to Open Protocols, the following holds:*

*PCIH2: In particular, the security architecture shall demonstrate how the default configuration is secure for each TSFI of the following types : Link Layer Protocols, IP Protocols, Security Protocols, IP Services.*

*##note that the application note above does not require any additional evaluator action with respect to the standard assessment of ADV\_ARC.1 according to CC and CEM. Similar considerations hold for any of the refinements and application notes listed in [PP] with regard to the Open Protocols features.*

##### ADV\_ARC.1-3

 **[ADV\_ARC.1-3]** The evaluator **shall examine** the security architecture description to determine that the initialisation process preserves security.

This work unit deals with the initialisation process. The security architecture description shall describe those mechanisms that ensure that the TSF enters a secure initial state.

Summary:

The evaluator found the related information that will be summarised in the following in ##… .

Analysis:

The evaluator’s analysis description shall show that the security architecture description describes that the initialisation process preserves security.

##The evaluator has identified the following aspects of the initialisation process...

##The security architecture description describes the above listed aspects of the initialisation process in the following way…

The evaluator shall analyse whether the default configuration is secure for each TSFI listed in refinement in ADV\_ARC.1.3C.

Assessment and Verdict:

The evaluator has examined for the initialisation process that the security architecture description describes ##does not describe that the initialisation process preserves security. There was ##no evidence found that the initialisation process preserves security.

Hence, the current work unit is **fulfilled** (pass) or is **not fulfilled** (fail).

#### ADV\_ARC.1.4C

ADV\_ARC.1.4C The security architecture description shall demonstrate that the TSF protects itself from tampering.

*Refinement from [PP]:*

*In particular, the security architecture description shall demonstrate that,*

* *PCIA4: Sensitive functions or data are only used in the protected areas(s) of the PED. This refinement is not applicable for the POI-CHIP-ONLY configuration.*
* *PCIA10: Secure components intended for unattended devices contain an anti-removal mechanism to protect against unauthorized removal and/or unauthorized re-installation. This refinement is not applicable for the POI-CHIP-ONLY configuration. This part of the TSF is assigned to PEDMiddleTSF and thus AVA\_POI.1/PEDMiddleTSF has to be applied to this property of the security architecture.*
* *PCIB18: The operating system of the device must contain only the software (components and services) necessary for the intended operation. The operating system must be configured securely and run with least privilege.*
* *PCIB20: The POI is capable of performing only its designed functions - i.e., there is no hidden functionality. The only approved functions performed by the POI are those allowed by the policy.*
* *PCID1: It is neither feasible to penetrate the IC Card Reader to make any additions, substitutions, or modifications to either the IC Card Reader's hardware or software, in order to determine or modify any sensitive data, nor is it possible for both an IC card and any other foreign object to reside within the card insertion slot. This refinement is not applicable for the POI-CHIP-ONLY configuration.*
* *PCID2 : The opening for the insertion of the IC card is in full view of the cardholder during card insertion so that any untoward obstructions or suspicious objects at the opening are detectable. This refinement is not applicable for the POI-CHIP-ONLY configuration.*
* *PCID3 : The ICC reader is constructed so that wires running out of the slot of the IC Card Reader to a recorder or a transmitter (an external bug) can be observed by the Cardholder. This refinement is not applicable for the POI-CHIP-ONLY configuration.*

*Refinement from [PP]:*

*In particular, for SFR-supporting features related to Open Protocols, the following holds:*

* *PCIH3: In particular the security architecture shall demonstrate how the TSF protects an unauthorized tampering of keys or certificates*

##### ADV\_ARC.1-4

 **[ADV\_ARC.1-4]** The evaluator **shall examine** the security architecture description to determine that it contains information sufficient to support a determination that the TSF is able to protect itself from tampering by untrusted active entities.

The current work unit deals with the security architecture aspect self-protection. The security architecture description shall contain information sufficient to support a determination that the TSF is able to protect itself from tampering by untrusted active entities.

Summary:

The evaluator found the related information that will be summarised in the following in ##… .

Analysis:

The evaluator’s analysis description shall show that the security architecture description supports a determination that the TSF is able to protect itself from tampering by untrusted active entities.

##The evaluator has identified the following aspects contributing to self-protection...

##The security architecture description describes the above listed aspects of self‑protection…

The evaluator shall check whether all the refinements listed in ADV\_ARC.1.4C are met.

Assessment and Verdict:

The evaluator has examined for the aspect self‑protection that the security architecture description contains ##does not contain information sufficient to support a determination that the TSF is able to protect itself from tampering by untrusted active entities. There was ##no evidence found for the security architecture description provided that the TSF is able to protect itself from tampering by untrusted active entities.

Hence, the current work unit is **fulfilled** (pass) or is **not fulfilled** (fail).

#### ADV\_ARC.1.5C

ADV\_ARC.1.5C The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.

*Refinement from [PP]:*

*In particular, the security architecture description shall demonstrate that:*

* *PCIA2: Failure of a single security mechanism does not compromise PED security. Protection against a threat is based on a combination of at least two independent security mechanisms (these mechanisms may be based on the same principles or technology, such as sensors, as long as their operation is independent – e.g. multiple switches activated on opening of the device casing are not independent). This refinement is not applicable in the POI-CHIP-ONLY configuration.*
* *PCIB16: All prompts for non-PIN data entry are under the control of the cryptographic unit of the device. If the prompts are stored inside the cryptographic unit, they cannot feasibly be altered without causing the erasure of the unit’s cryptographic keys. If the prompts are stored outside the cryptographic unit, cryptographic mechanisms must exist to ensure the authenticity and the proper use of the prompts and that modification of the prompts or improper use of the prompts are prevented.*
* *EPC-CHIP-ONLYB16: Cryptographic mechanisms must exist to ensure the authenticity and the proper use of the prompts and that modification of the prompts or improper use of the prompts are prevented.*

*Refinement from [PP]:*

*In particular, for SFR-supporting features related to Open Protocols, the following holds:*

* *PCIG2: The security architecture shall demonstrate:*
	+ *How the TSF protects itself from the exploitation of a public-knowledge vulnerability on a TSFI of the following types : Link Layer Protocols, IP Protocols, Security Protocols, IP Services, including*
		- *exploitation of replay of messages (PCII5),*
		- *exploitation of insecure exception handling (PCII5).*
* *PCIH3: The security architecture shall demonstrate:*
	+ *How the TSF protects itself from bypass of the SFR-enforcing functionality via an unexpected usage of keys or certificates.*

*##note that the refinement above does not require any additional evaluator action with respect to the standard assessment of ADV\_ARC.1 according to CC and CEM. Similar considerations hold for any of the refinements and application notes listed in [PP] with regard to the Open Protocols features.*

##### ADV\_ARC.1-5

 **[ADV\_ARC.1-5]** The evaluator **shall examine** the security architecture description to determine that it presents an analysis that adequately describes how the SFR-enforcing mechanisms cannot be bypassed.

The current work unit deals with the security architecture aspect non-bypassability. The security architecture description shall present an analysis that adequately describes how the SFR-enforcing mechanisms cannot be bypassed.

Summary:

The evaluator found the related information that will be summarised in the following in ##… .

Analysis:

The evaluator’s analysis description shall show that the security architecture description presents an analysis that adequately describes how the SFR-enforcing mechanisms cannot be bypassed.

##The evaluator has found the analysis of non-bypassability in section ## of the security architecture description…

##The evaluator has examined the analysis of non-bypassability for the following SFR-enforcing mechanisms…

##The security architecture description presents an analysis that adequately describes how the SFR-enforcing mechanisms cannot be bypassed.…

The evaluator shall check whether all the refinements listed in ADV\_ARC.1.5C are met.

Assessment and Verdict:

The evaluator has examined for the aspect non-bypassability that the security architecture description presents ##does not present an analysis that adequately describes how the SFR-enforcing mechanisms cannot be bypassed. There was ##no evidence found for the security architecture description provided that the SFR‑enforcing mechanisms can be bypassed.

Hence, the current work unit is **fulfilled** (pass) or is **not fulfilled** (fail).

**Verdict for ADV\_ARC.1.1E:**
**##PASS ##FAIL ##INCONCLUSIVE**
The evaluator confirms (##disproves) that the information provided in the analysed documentation meet all requirements for content and presentation of evidence.##arc

## ADV\_FSP.2 Security-enforcing functional specification

**Summary Verdict for the Assurance Component ADV\_FSP.2:**
**##PASS ##FAIL ##INCONCLUSIVE**.
*##If all work units are met:* The TOE meets all requirements of the assurance component ADV\_FSP.2. This result is based on the evaluator actions and work units documented below.

### ADV\_FSP.2.1E

Evaluator action element:

ADV\_FSP.2.1E The evaluator ***shall confirm*** that the information provided meets all requirements for content and presentation of evidence.

In line with the structure presented in chapter 9 of this document, CC elements for content and presentation of evidence are discussed one by one in the following subsections in the context of their relevant work units.

#### ADV\_FSP.2.1C

ADV\_FSP.2.1C The functional specification shall completely represent the TSF.

##### ADV\_FSP.2-1

**[ADV\_FSP.2-1]** The evaluator ***shall examine*** the functional specification to determine that the TSF is fully represented.

In order to identify the TSFI, TSF have to be identified. Therefore the current work unit deals with the question whether the TSF is fully represented or not.

Summary:

The evaluator checked the functional specification document [ADV] and the supporting documents. Completeness of the functional specification in representing the TSF is assessed by the evaluator by comparing the interfaces described in [ADV] with the rest of the developer evidence and with the TOE itself.

Analysis:

##By examining the functional specification [ADV\_FSP], the supporting document [APIS], the rest of the vendor evidence ([ADV\_TDS], [ADV\_ARC] and [DESIGN\_DOCS]) and the TOE itself, the evaluator found sufficient information showing that the TSF is fully represented by the TSFIs.

In document [ADV\_FSP], the vendor identifies which interfaces of the device are SFR-enforcing TSFIs and which ones are SFR-supporting or non-interfering TSFIs.

SFR-enforcing TSFIs are listed as follows:

…

The table below provides an overview of the checks that the evaluator performed on the rest of the vendor evidence and on the device itself in order to assess that the functional specification provides a full representation of the TSF.

| **Identifier of TSF components** | **References** | **Are there interfaces (network protocols or hardware interfaces), that are described in one of these documents, but not defined in [ADV\_FSP]?** |
| --- | --- | --- |
| ## | ## | ## |

Table 5: Representation of TSF

Assessment and Verdict:

As shown in the Table 5, the TSF is completely represented in the design documents. The corresponding interface descriptions are given in the functional specification as referenced in the third column of the table.

The evaluators have ##not found the TSF represented by the FSP.

Hence, the current work unit is **fulfilled** (pass) or is **not fulfilled** (fail).

#### ADV\_FSP.2.2C

ADV\_FSP.2.2C The functional specification shall describe the purpose and method of use for all TSFI.

##### ADV\_FSP.2-2

**[ADV\_FSP.2-2]** The evaluator shall examine the functional specification to determine that it states the purpose of each TSFI.

This work unit deals with the question if the purpose of each identified TSFI is given.

Summary:

For each TSFI, the evaluators found a description of its purpose in the functional specification.##or: The functional specification does not provide a description of purpose for every TSFI.

Analysis:

The Functional Specification describes the purpose of each TSFI..

The table below provides the full list of TSFIs as identified by the vendor in [ADV] with their classification and indication of purpose, SFR-enforcing actions, method of use, parameters and error messages (when applicable).

| **TSFI** | **Categorisation (SFR-enforcing?)** | **Purpose** | **Method of use** | **In/Out Parameters** | **Error messages** |
| --- | --- | --- | --- | --- | --- |
| ## | ## | ## | ## | ## |  |

Table 6: Description of purpose and method of use in the functional specification

Assessment and Verdict:

As shown in Table 6, the Functional Specification describes ##does not describe the purpose of all TSFI. The evaluators examined the descriptions referenced in Table 6 as well as other documentation related to the TSFIs. They came to the conclusion that the TSFI purpose descriptions in the Functional Specification ##do not represent the related TSFIs accurately. The Functional Specification states the purpose of each TSFI. The explanations are ##not sufficient to understand the intended uses of the TSFIs.

Hence, the current work unit is **fulfilled** (pass) or is **not fulfilled** (fail).

##### ADV\_FSP.2-3

**[ADV\_FSP.2-3]** The evaluator *shall examine* the functional specification to determine that the method of use for each TSFI is given.

This work unit deals with the question if the functional specification describes how to use each TSFI.

Summary and Analysis:

Table 6 from work unit ADV\_FSP.2-2 (or corresponding work unit of higher level of ADV\_FSP) identifies the sections of the Functional Specification describing the TSFIs’ methods of use. The evaluators examined these descriptions. They cover each TSFI accurately and sufficiently to prepare tests.

Assessment and Verdict:

Therefore the evaluators determine that the method of use for each TSFI has ## not been provided in the functional specification.

Hence, the current work unit is **fulfilled** (pass) or is **not fulfilled** (fail).

#### ADV\_FSP.2.3C

ADV\_FSP.2.3C The functional specification shall identify and describe all parameters associated with each TSFI.

*Refinement from [PP]:*

*If the TOE claims conformance to package "SFR-supporting features related to Open Protocols", the following holds.*

*PCIF1: The TSFIs consisting in protocols or services shall be considered at least SFR-supporting and shall define the following parameters:*

* *Protocol name*
* *Protocol type:*
	+ *Link Layer Protocols*
	+ *IP Protocols*
	+ *Security Protocols*
	+ *IP Services*
	+ *Other*
* *Protocol number (for IP protocols)*
* *Port number (for IP services)*

*##note that the application note above does not require any additional evaluator action with respect to the standard assessment of ADV\_FSP.2 according to CC and CEM. Similar considerations hold for any of the refinements and application notes listed in [PP] with regard to the Open Protocols features.*

##### ADV\_FSP.2-4

**[ADV\_FSP.2-4]** The evaluator ***shall examine*** the presentation of the TSFI to determine that it completely identifies all parameters associated with every TSFI.

This work unit deals with the question, whether all interface parameters of every TSFI are provided.

Summary:

The TSFI have been identified in work units ADV\_FSP.2-1. They are shown in Table 6. The evaluators confirmed that the method of use as well as the parameters of all TSFIs have been identified.

**Analysis:**

##The evaluators examined the parameters of the TSFIs together with the description of their purpose and method of use. In order to verify that the functional specification identifies the parameters of the TSFIs completely, the evaluators took other evidence (design description, security architecture, user guidance, implementation) into account.

The evaluator shall check whether the refinement of ADV\_FSP.2.3C is met.

Assessment and Verdict:

Therefore the evaluators ##did not determined that the TSFI representation identifies all parameters associated with every TSFI.

Hence, the current work unit is **fulfilled** (pass) or is **not fulfilled** (fail).

#####  ADV\_FSP.2-5

**[ADV\_FSP.2-5]** The evaluator ***shall examine*** the presentation of the TSFI to determine that it completely and accurately describes all parameters associated with every TSFI.

This work unit deals with the question if all parameters of every TSFI are described accurately and the description of parameters is complete.

Summary:

##This work unit was worked out together with previous work unit. When the evaluators examined the purpose and method of use of the TSFI, they also examined the rest of the interface description (actions, error messages etc.). Thus they have verified that the functional specification contains all parameters associated with every TSFI.

Analysis:

##Since the completeness and accuracy of the parameter description can only be confirmed when other evidences are taken into account, the evaluators examined the parameter descriptions by taking into account the design description and the implementation representation. Thus the evaluators verified that sufficient information is given to provide a complete description of each parameter.

The evaluator shall check whether the refinement of ADV\_FSP.2.3C is met.

Assessment and Verdict:

##Considering the security architecture, the design description and the implementation the evaluators reviewed the parameter description. .... They came to conclusion that the parameter description is accurate and meaningful.

Therefore the evaluators ##can not confirm that the presentation of the TSFI completely and accurately describes all parameters associated with every TSFI.

Hence, the current work unit is **fulfilled** (pass) or is **not fulfilled** (fail).

#### ADV\_FSP.2.4C

ADV\_FSP.2.4C For SFR-enforcing TSFIs, the functional specification shall describe the SFR-enforcing actions associated with the TSFI.

##### ADV\_FSP.2-6

 **[ADV\_FSP.2-6]** The evaluator ***shall examine*** the presentation of the TSFI to determine that it completely and accurately describes the SFR-enforcing actions associated with the SFR-enforcing TSFIs.

This work unit deals with the question, whether all SFR‑enforcing actions associated with the SFR‑enforcing TSFI are completely and accurately described in the presentation of the TSFI.

Summary:

##The evaluators examined the presentation of the TSFI when previous work units were worked out. Thus they confirmed that the description consist the actions associated with the TSFIs.

Analysis:

##Since the completeness and accuracy of the parameter description can only be confirmed when other evidences are taken into account, the evaluators examined the parameter descriptions by taking into account the design description and the implementation representation. The evaluators verified that sufficient information is given to provide a complete description of each parameter.

Assessment and Verdict:

Therefore the evaluators has ##not determined that the presentation of the TSFI describes completely and accurately the SFR-enforcing actions associated with the SFR‑enforcing TSFIs.

Hence, the current work unit is **fulfilled** (pass) or is **not fulfilled** (fail).

#### ADV\_FSP.2.5C

ADV\_FSP.2.5C For SFR-enforcing TSFIs, the functional specification shall describe direct error messages resulting from processing associated with the SFR-enforcing actions.

##### ADV\_FSP.2-7

 **[ADV\_FSP.2-7]** The evaluator ***shall examine*** the presentation of the TSFI to determine that it completely and accurately describes error messages that may result from SFR-enforcing actions associated with each SFR-enforcing TSFI.

This work unit deals with the question, whether the presentation of the TSFI describes error messages of SFR‑enforcing actions completely and accurately. Since several activities of this work unit correspond to the activities of the previous work unit (ADV\_FSP.2‑6), the evaluators just concentrate the activities that have not been described under previous work unit.

Summary:

The evaluator found the related information that will be summarised in the following in ##… .

##Examining the functional specification the evaluators found a complete and accurate description of error messages that may result from SFR‑enforcing actions of the SFR‑enforcing TSFI.

Analysis:

The evaluator referred to the description of the errors resulting from SFR-enforcing actions in Table 6. Extensive information on the error messages associated with SFR-enforcing TSFIs is presented in documents [APIS].

Assessment and Verdict:

Therefore the evaluators confirm ##disprove that the presentation of the TSFI completely and accurately describes error messages that may result from SFR‑enforcing actions associated with each SFR‑enforcing TSFI.

Hence, the current work unit is **fulfilled** (pass) or is **not fulfilled** (fail).

#### ADV\_FSP.2.6C

ADV\_FSP.2.6C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

##### ADV\_FSP.2-8

**[ADV\_FSP.2-8]** The evaluator ***shall check*** that the tracing links the SFRs to the corresponding TSFIs.

This work unit deals with the question, whether the developer has provided information to associate the TSFI to the SFRs that are affine to this TSFI.

Summary and Analysis:

The evaluator found the related information in document [MAPPING]. In this document, the vendor lists for each TSFI the SFRs of the [ST] that relate to it and provides some brief comments. The evaluator summarised such mapping in section 11 of this document.

Assessment and Verdict:

Examining the SFRs defined in [ST] the evaluators verified that each SFR is presented in the table. Furthermore the table shows that at least one SFR‑supporting or SFR‑enforcing TSFI is mapped to each SFR.

The evaluator has ##not found a tracing linking the SFRs to the corresponding TSFIs.

Hence, the current work unit is **fulfilled** (pass) or is **not fulfilled** (fail).

**Verdict for ADV\_FSP.2.1E:**
**##PASS ##FAIL ##INCONCLUSIVE**
The evaluator confirms (##disproves) that the information provided in the analysed documentation meet all requirements for content and presentation of evidence.

### ADV\_FSP.2.2E

Evaluator action element:

ADV\_FSP.2.2E The evaluator ***shall determine*** that the functional specification is an accurate and complete instantiation of the SFRs.

In line with the structure presented in chapter 4 of this document, CC elements for content and presentation of evidence are discussed one by one in the following subsections in the context of their relevant work units.

##### ADV\_FSP.2-9

**[ADV\_FSP.2-9]** The evaluator ***shall examine*** the functional specification to determine that it is a complete instantiation of the SFRs.

This work unit addresses the completeness of the SFR instantiation as defined in the ST. Since the next work unit addresses the accuracy of the SFR instantiations both work units are conducted together.

##The evaluators examined the completeness of the instantiation together with the next work unit and determined that the functional specification is ##not a complete instantiation of the SFRs.

Hence, the current work unit is **fulfilled** (pass) or is **not fulfilled** (fail).

##### ADV\_FSP.2-10

 **[ADV\_FSP.2-10]** The evaluator ***shall examine*** the functional specification to determine that it is an accurate instantiation of the SFRs.

This work unit deals with the accuracy of the SFR instantiation.

Summary and Analysis:

The evaluator found the related information that will be summarised in the following in ##… .

## section 11 maps the SFRs to the related TSFIs. The evaluators verified that the table lists all SFRs by checking the ST.

Assessment and Verdict:

##As shown in section 11 all SFRs in ST are ##not sufficiently met by one or more TSFI.

The evaluators ##do not confirm that the functional specification is an accurate instantiation of the SFRs.

Hence, the current work unit is **fulfilled** (pass) or is **not fulfilled** (fail).

**Verdict for ADV\_FSP.2.2E:**
**##PASS ##FAIL ##INCONCLUSIVE**
The evaluator confirms (##disproves) that the information provided in the analysed documentation meet all requirements for content and presentation of evidence.

## ADV\_TDS.1 Basic design

**Summary Verdict for the Assurance Component ADV\_TDS.1:**
**##PASS ##FAIL ##INCONCLUSIVE**.
*##If all work units are met:* The TOE meets all requirements of the assurance component ADV\_TDS.1. This result is based on the evaluator actions and work units documented below.

### ADV\_TDS.1.1E

Evaluator action element:

ADV\_TDS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

In line with the structure presented in chapter 9 of this document, CC elements for content and presentation of evidence are discussed one by one in the following subsections in the context of their relevant work units.

#### ADV\_TDS.1.1C

ADV\_TDS.1.1C The design shall describe the structure of the TOE in terms of subsystems.

##### ADV\_TDS.1-1

**[ADV\_TDS.1-1]** The evaluator ***shall examine*** the TOE design to determine that the structure of the entire TOE is described in terms of subsystems.

The other evidence presented for the TOE being examined may also consist of user guidance which extends the mandatory input to the work unit.

Summary:

The evaluator found the related information that will be summarised in the following in ##… .

Analysis:

##In document [ADV\_TDS], the vendor identified the following subsystems (together with a brief description and reference to more detailed evidences, when needed, for each subsystem):

…

Assessment and Verdict:

The evaluator determined that the structure of the TOE is ##not described in terms of subsystems.

The evaluator determined that ##not all of the subsystems of the TOE are identified.

Hence, the current work unit is **fulfilled** (pass) or is **not fulfilled** (fail).

#### ADV\_TDS.1.2C

ADV\_TDS.1.2C The design shall identify all subsystems of the TSF.

##### ADV\_TDS.1-2

**[ADV\_TDS.1-2]** The evaluator ***shall examine*** the TOE design to determine that all subsystems of the TSF are identified.

In order to distinguish between the non-TSF and the SFR-non-interfering subsystems the evaluator may use the following rule of thumb: There is no interaction between the non-TSF and TSF subsystems of the TOE, whereby the SFR-non-interfering subsystems can interact (and, likely, do this) with the SFR-supporting and SFR-enforcing subsystems.

Summary:

The evaluator found the related information that will be summarised in the following in ##… .

Analysis:

##The analysis of the identification of all subsystems of the TOE as TSF or non-TSF was performed as follows.

##The following are the subsystems of the TSF .... None of such subsystems is missing.

Assessment and Verdict:

The evaluator has determined that ##not all subsystems of the TSF are identified. There is ##no (##at least one) subsystem being not accounted as part of the TSF.

Hence, the current work unit is **fulfilled** (pass) or is **not fulfilled** (fail).

#### ADV\_TDS.1.3C

ADV\_TDS.1.3C The design shall describe the behaviour of each SFR-supporting or SFR-non-interfering TSF subsystem in sufficient detail to determine that it is not SFR-enforcing.

*Refinement from [PP]:*

*In particular, for SFR-supporting features related to Open Protocols, the following holds: The design shall describe the behaviour of each SFR-supporting or SFR non-interfering TSF sub-system in sufficient detail to determine that it is not SFR-enforcing. For all SFR-supporting TSF subsystem implementing a security protocol, the design shall describe*

* *PCII2: how the device provides confidentiality of data sent over a network connection, including*
	+ *Encryption mechanism with key sizes appropriate for the algorithm(s) in question.*
	+ *Encryption provided by using keys that are established in a secure manner using appropriate key-management procedures, such as those listed in NIST SP800-21, Guidelines for Implementing Cryptography*
* *PCII3: how the device is able to provide the integrity of data that is sent over a network connection, including*
	+ *Integrity provided by a MAC as defined in ISO 16609, or by a digital signature.*
	+ *Hashing provided by at least one of the following algorithms: SHA-224, SHA-256, SHA-384, and SHA-512.*
* *PCII4: how the device uses a declared security protocol to authenticate the server.*
	+ *Server authentication with key sizes appropriate for the algorithm(s) in question.*
	+ *Hashing provided by at least one of the following algorithms: SHA-224, SHA-256, SHA-384, and SHA-512.*
	+ *verification of the validity of public keys received by the platform.*
	+ *verification of the authenticity of public keys received by the platform.*
* *PCII6: How the platform implements session management.*
	+ *Tracking of all connections and restriction of the number of sessions that can remain active on the platform to the minimum necessary number.*
	+ *Time limits for sessions and insurance that sessions are not left open for longer than necessary.*

*##note that the application note above does not require any additional evaluator action with respect to the standard assessment of ADV\_TDS.1 according to CC and CEM. Similar considerations hold for any of the refinements and application notes listed in [PP] with regard to the Open Protocols features.*

##### ADV\_TDS.1-3

**[ADV\_TDS.1-3]** The evaluator ***shall examine*** the TOE design to determine that each SFR-supporting or SFR-non-interfering subsystem of the TSF is described such that the evaluator can determine that the subsystem is SFR-supporting or SFR-non-interfering.

The SFR-enforcing behaviour has to be summarised according to ADV\_TDS1.4C. The description level according to ADV\_TDS.1.3C for SFR-supporting or SFR-non-interfering TSF subsystem should not be expected to be more detailed then that for the SFR-enforcing behaviour. In ADV\_TDS.1-7 and ADV\_TDS.1-8 the evaluator will examine the TOE design for the coverage of SFRs by it. The results from these work units could be used within current work unit. The work unit can be stated satisfied, if the developer provides uniform level of documentation for the TOE design, i.e. a high-level.

Summary:

The evaluator found the related information that will be summarised in the following in ##… .

Analysis:

##The evaluator reviewed the subsystems that have been defined by the vendor and assessed that they are all defined at the same level of detail. The descriptions are brief, but allow the evaluator to determine whether a subsystems is SFR-enforcing.

The evaluator shall check whether the refinement of ADV\_TDS.1.3C is met.

Assessment and Verdict:

The evaluator determined that ##not for each SFR-supporting and for each SFR-non-interfering subsystem without high-level description the subsystem is described in such a manner that it can be determined that this subsystem is non-SFR-enforcing. There is ##no (##at least one) SFR-supporting or SFR-non-interfering subsystem for which such determination cannot be made based on the description provided for this subsystem.

Hence, the current work unit is **fulfilled** (pass) or is **not fulfilled** (fail).

#### ADV\_TDS.1.4C

ADV\_TDS.1.4C The design shall summarise the SFR-enforcing behaviour of the SFR-enforcing subsystems.

##### ADV\_TDS.1-4

**[ADV\_TDS.1-4]** The evaluator ***shall examine*** the TOE design to determine that it provides a complete, accurate, and high-level description of the SFR-enforcing behaviour of the SFR-enforcing subsystems.

The SFR-enforcing behaviour has to be summarised. In ADV\_TDS.1-7 and ADV\_TDS.1-8 the evaluator will examine the design for the coverage of SFRs by the TOE design. The results from these work units could be used within the current work unit. I.e. during this examination the evaluator should be able to identify any missing information. The evaluator will require additional missing information from the developer because of his responsibility to determine that he has sufficient information for the subsystems’ category (SFR-enforcing, etc.). A coverage (and accuracy) of SFRs by the TOE design description also indicates that the SFR-enforcing behaviour is described at a sufficient level. The determination of the completeness and accuracy of the TOE design with respect to functional specification can be based on the work unit ADV\_TDS.1-6 and, with respect to implementation representation, on the work unit ADV\_IMP.1-3.

Summary:

The evaluator found the related information that will be summarised in the following in ##… .

Analysis:

##The evaluator observed that all defined subsystems are SFR enforcing and their SFR-enforcing behaviour is sufficiently described in document [ADV\_TDS] and in the additional supporting documentation. The SFR mapping will be addressed by the evaluator in further details in section ADV\_TDS.1-6 of this report and section 11.

Assessment and Verdict:

The evaluator has determined that ##not for each SFR-enforcing subsystem a description of the SFR-enforcing behaviour was provided, and that the description was ##not provided at high level. For ##no (##at least one) subsystem which identified as SFR-enforcing there is no high-level description of the SFR-enforcing behaviour.

The evaluator has determined that the TOE design is ##not complete and ##inaccurate (e.g. with respect to security target, functional specification, security architecture description and implementation representation). There is ##no contradiction to other information. ##None (##Other) information indicates SFR-behaviour for which there is no high-level description.

Hence, the current work unit is **fulfilled** (pass) or is **not fulfilled** (fail).

#### ADV\_TDS.1.5C

ADV\_TDS.1.5C The design shall provide a description of the interactions among SFR-enforcing subsystems of the TSF, and between the SFR-enforcing subsystems of the TSF and other subsystems of the TSF.

##### ADV\_TDS.1-5

**[ADV\_TDS.1-5]** The evaluator ***shall examine*** the TOE design to determine that interactions between the subsystems of the TSF are described.

The evaluator examines the interactions among SFR-enforcing subsystems, and between SFR-enforcing subsystems and other subsystems of the TSF. The purpose of the description is to provide the reader (e.g. the evaluator) a better understanding of how the TSF performs its functions. The evaluator will use his own judgement when assessing the completeness of the description. The judgement can be based also on whether the evaluator gained better understanding of how the TSF performs its functions

Summary:

The evaluator found the related information that will be summarised in the following in ##… .

Analysis:

##The evaluator has analysed the TOE design for providing the description of interactions among the SFR-enforcing and between the SFR-enforcing and other TSF subsystems. During the analysis it was in focus that this description provides a better understanding on how the TSF performs its functions by exchanging data and/or control information between subsystems.

##A detailed report is given for the following examples of an interaction ...

Assessment and Verdict:

The evaluator has determined that interactions among SFR-enforcing subsystems and between the SFR-enforcing subsystems and the other TSF subsystems are ##not described in the TOE design and that the description addresses (##does not address) the interaction by means of data and control information.

The evaluator has ##not determined the completeness of the description. The evaluator has ##not encountered any (##some) unclear interactions and any (##some) SFR-related interactions that are apparently not described and which description is considered by the evaluator to be required to understand the overall security or security functionality provided by the TSF.

Hence, the current work unit is **fulfilled** (pass) or is **not fulfilled** (fail).

#### ADV\_TDS.1.6C

ADV\_TDS.1.6C The mapping shall demonstrate that all TSFIs trace to the behaviour described in the TOE design that they invoke.

##### ADV\_TDS.1-6

**[ADV\_TDS.1-6]** The evaluator ***shall examine*** the TOE design to determine that it contains a complete and accurate mapping from the TSFI described in the functional specification to the subsystems of the TSF described in the TOE design.

The developer shall provide a mapping from the TSFI as stated in the functional specification to the lowest level of decomposition available in the TOE design. The mapping shall demonstrate that all behaviour described in the TOE design is mapped to the TSFIs invoking it.

The evaluator will examine the mapping from the TSFI described in the functional specification to the TSF subsystems described in the TOE design. The demonstration of the opposite direction which is also contained in the developer’s description of the TOE design can provide additional support to the evaluator’s work. The mapping will identify, for each TSFI, a subsystem being initially involved when an operation is requested at that TSFI, and identify the various subsystems that are primarily responsible for implementing the functionality. The evaluator will extensively use and examine the mapping in the work units ADV\_TDS.1-7 and ADV\_TDS.1-8 for SFR-enforcing TSFIs and related subsystems/modules.

Summary:

The evaluator found the related information that will be summarised in the following in ##… .

Analysis:

##The analysis of the mapping from the TSFI (described in FSP) to the TSF subsystems/modules (the lowest level available should be selected) (described in TOE design) concerning the completeness and the accuracy of the mapping was performed as follows .....

##Please refer to the following table for details of the results of the analysis ....

Assessment and Verdict:

The evaluator has determined that the mapping from the TSFI described in the functional specification to the lowest level of decomposition available in the TOE design (##subsystems ##modules) is ##not complete. There is (##a) ##no TSFI that is not mapped to at least one ##subsystem (##module).

The evaluator has determined that the mapping from the TSFI described in the functional specification to the lowest level of decomposition available in TOE design (##subsystems ##modules) is ##inaccurate. The evaluator has ##not encountered any TSFI being not mapped at TSF boundary or whose mapping does not make a sense (as judged by the evaluator because this would not support the evaluator in understanding the system and implementation of the SFRs).

Hence, the current work unit is **fulfilled** (pass) or is **not fulfilled** (fail).

**Verdict for ADV\_TDS.1.1E:**
**##PASS ##FAIL ##INCONCLUSIVE**
The evaluator confirms (##disproves) that the information provided in the analysed documentation meet all requirements for content and presentation of evidence.

### ADV\_TDS.1.2E

Evaluator action element:

ADV\_TDS.1.2E The evaluator shall determine that the design is an accurate and complete instantiation of all security functional requirements.

In line with the structure presented in chapter 4 of this document, CC elements for content and presentation of evidence are discussed one by one in the following subsections in the context of their relevant work units.

##### ADV\_TDS.1-7

**[ADV\_TDS.1-7]** The evaluator ***shall examine*** the TOE security functional requirements and the TOE design, to determine that all ST security functional requirements are covered by the TOE design.

The tracing provided by the developer for ADV\_FSP shall already have demonstrated that the SFRs trace to TSFIs in the functional specification. Together with the mapping from the TSFI to the subsystems of TSF provided by the developer in the TOE design the coverage of the TOE security functional requirements by the TOE design can be examined. The mapping will likely be from a functional requirement to a set of subsystems, but it may have to be at a level of detail below the subsystem or even element level of the requirements, because of operations performed on the functional requirement by the ST author. The work can be done based on the work unit ADV\_TDS.1-8.

Summary:

The evaluator found the related information that will be summarised in the following in ##… .

Analysis:

##The analysis of the completeness of the coverage of ST security functional requirements by the TOE design was done as follows. Please note that this work was done in conjunction with the work unit ADV\_TDS.1-8. ....

Assessment and Verdict:

The evaluator has determined the (##not all parts of) ##not all ST security functional requirements are covered by the TOE design. ##No (##There is at least one) ST security functional requirement ##which is not covered.

Hence, the current work unit is **fulfilled** (pass) or is **not fulfilled** (fail).

##### ADV\_TDS.1-8

**[ADV\_TDS.1-8]** The evaluator ***shall examine*** the TOE design to determine that it is an accurate instantiation of all security functional requirements.

The tracing provided by the developer for ADV\_FSP shall already have demonstrated that the SFRs are traced to TSFIs in the functional specification. Together with the mapping from the TSFI to the subsystems of TSF provided by the developer in the TOE design the coverage of the TOE security functional requirements by the TOE design can be examined. The map will likely be from a functional requirement to a set of subsystems, but it may have to be at a level of detail below the subsystem or even element level of the requirements, because of operations performed on the functional requirement by the ST author. The work done in this work unit can be used for the work unit ADV\_TDS.1-7. In the current work unit the evaluator provides also an evidence that the TOE design description contains sufficient information on i) the structure of the TOE, ii) on TSF behaviour, iii) on interactions of subsystems and iv) on mapping from TSFI to the design, to aid the evaluator in understanding the overall functionality and security functionality provided by the TSF.

Summary:

The evaluator found the related information that will be summarised in the following in ##… .

Analysis:

##By inspection of the provided documentation, the evaluator verified that:

* all SFRs listed in the ST have been addressed by the vendor, who provided a design description of how the SFR is implemented;
* each SFR is mapped to a number of subsystem that collectively implement the security functional requirement.
* the evaluator further verified that the identified set of subsystems provides an accurate description of how the requirement is implemented.

All SFRs were analysed by the evaluator, who reported in section 11 the mapping of SFRs against subsystems as proposed by the vendor.

Assessment and Verdict:

The evaluator determined that ##not all ST security functional requirements are accurately instantiated by the TOE design. There is ##a ##no part of a ST security functional requirements not accurately instantiated in the TOE design.

Hence, the current work unit is **fulfilled** (pass) or is **not fulfilled** (fail).

**Verdict for ADV\_TDS.1.2E:**
**##PASS ##FAIL ##INCONCLUSIVE**
The evaluator confirms (##disproves) that the information provided in the analysed documentation meet all requirements for content and presentation of evidence.

## Indications for Potential Vulnerabilities

##The evaluator did not find any potential vulnerability indicated by the current evaluation aspect.

## Missing Information

##There is no further information, which the developer/sponsor has to provide.

*##In the case of the verdict ‘inconclusive’, the evaluator is expected to put some issues into the sections ‘Missing Information’ or ‘Questions to and Conditions on the Developer’ of his single evaluation report, cf. AIS14.*

## Questions to / Conditions on the Developer

##There are no questions, recommendations to or conditions on the developer.

*##In the case of the verdict ‘inconclusive’, the evaluator is expected to put some issues into the sections ‘Missing Information’ or ‘Questions to and Conditions on the Developer’ of his single evaluation report, cf. AIS14.*

## Necessary Changes/Improvements

##There are no changes should be done by the developer.

*##In the case of the verdict ‘fail’, the evaluator is expected to put some issues into the section ‘Necessary Changes/Improvements’ of his single evaluation report, cf. AIS14.*

## Effects on other Documents

##There are no effects on other documents.

1. Annex

# SFR coverage

In this section SFRs from the ST are listed in the first column. The second column summarizes in which subsystem these SFRs are satisfied by the TOE, with references to the relevant sections of the report when needed. The third column maps the SFRs to the TSFIs of the TOE.

Table 7 Mapping of SFRs to subsystems and TSFIs

| SFR (ST) | Mapping to Subsystems (TDS) | SFR-enforcing TSFI (FSP) |
| --- | --- | --- |
| **PIN Entry package** |  |  |
| FDP\_IFC.1/PIN\_ENTRY Subset information flow control |  |  |
| FDP\_ITC.1/PIN\_ENTRY Import of user data without security attributes |  |  |
| FPT\_EMSEC.1/PIN\_ENTRY TOE Emanation |  |  |
| FIA\_UAU.2/PIN\_ENTRY User authentication before any action |  |  |
| FIA\_UID.1/PIN\_ENTRY Timing of identification |  |  |
| FTA\_SSL.3/PIN\_ENTRY TSF-initiated termination |  |  |
| **ENC\_PIN package** |  |  |
| FDP\_IFC.1/ENC\_PIN Subset information flow control |  |  |
| FDP\_IFF.1/ENC\_PIN Simple security attributes |  |  |
| FMT\_MSA.1/ENC\_PIN Management of security attributes |  |  |
| FMT\_SMR.1/ENC\_PIN Security roles |  |  |
| FIA\_UID.1/ENC\_PIN Entry Timing of identification |  |  |
| FDP\_RIP.1/ENC\_PIN Subset residual information protection |  |  |
| FDP\_ITT.1/ENC\_PIN Basic internal transfer protection |  |  |
| FTP\_TRP.1/ENC\_PIN Trusted path |  |  |
| **PLAIN\_PIN package** |  |  |
| FDP\_IFC.1/PLAIN\_PIN Subset information flow control |  |  |
| FDP\_IFF.1/PLAIN\_PIN Simple security attributes |  |  |
| FDP\_RIP.1/PLAIN\_PIN Subset residual information protection |  |  |
| FDP\_ITT.1/PLAIN\_PIN Basic internal transfer protection |  |  |
| FMT\_MSA.1/PLAIN\_PIN Management of security attributes |  |  |
| FIA\_UID.1/PLAIN\_PIN Entry Timing of identification |  |  |
| **IC Card Reader package** |  |  |
| FDP\_IFC.1/ICCardReader Subset information flow control |  |  |
| FDP\_IFF.1/ICCardReader Simple security attributes |  |  |
| FDP\_RIP.1/ICCardReader Subset residual information protection |  |  |
| FDP\_ITT.1/ICCardReader Basic internal transfer protection |  |  |
| FDP\_ACC.1/ICCRLoader Subset Access control |  |  |
| FDP\_ITC.1/ICCRLoader Import of user data without security attributes |  |  |
| **POI\_DATA package** |  |  |
| FDP\_ACC.1/POI\_DATA Subset Access Control |  |  |
| FDP\_ACF.1/POI\_DATA Security attribute based access control |  |  |
| FDP\_RIP.1/POI\_DATA Subset residual information protection |  |  |
| FDP\_ITT.1/POI\_DATA Basic internal transfer protection |  |  |
| FDP\_UIT.1/POI\_DATA Data exchange integrity |  |  |
| FDP\_UCT.1/POI\_DATA Basic data exchange confidentiality |  |  |
| FTP\_ITC.1/POI\_DATA Inter-TSF trusted channel |  |  |
| **CoreTSF package** |  |  |
| FPT\_TST.1/CoreTSF TSF testing |  |  |
| FPT\_FLS.1/CoreTSF Failure with preservation of secure state |  |  |
| FDP\_ACC.1/CoreTSFLoader Subset access control |  |  |
| FDP\_ITC.1/CoreTSFLoader Import of user data without security attributes |  |  |
| **PEDMiddleTSF package** |  |  |
| FPT\_TST.1/PEDMiddleTSF TSF testing |  |  |
| FPT\_FLS.1/PEDMiddleTSF Failure with preservation of secure state |  |  |
| FDP\_ACC.1/PEDMiddleTSFLoader Subset access control |  |  |
| FDP\_ITC.1/PEDMiddleTSFLoader Import of user data without security attributes |  |  |
| **MiddleTSF package** |  |  |
| FDP\_ACC.1/ApplicationLoader Subset access control |  |  |
| FDP\_ITC.1/ ApplicationLoader import of user data without security attributes |  |  |
| FDP\_ACC.1/MiddleTSFLoader Subset access control |  |  |
| FDP\_ITC.1/MiddleTSFLoader Import of user data without security attributes |  |  |
| FPT\_FLS.1/MiddleTSF Failure with preservation of secure state |  |  |
| **PED Prompt Control package** |  |  |
| FDP\_ACC.1/PEDPromptControl Subset access control |  |  |
| FDP\_ACF.1/PEDPromptControl Security attribute based access control |  |  |
| **Cryptography package** |  |  |
| FCS\_RND.1 Quality metric for random numbers |  |  |
| FCS\_COP.1 Cryptographic operation |  |  |
| FDP\_ITC.2 Import of user data with security attributes |  |  |
| FTP\_ITC.1 Inter-TSF trusted channel |  |  |
| FPT\_TDC.1 Inter-TSF basic TSF data consistency |  |  |
| **Physical Protection package** |  |  |
| FPT\_PHP.3/CoreTSF Resistance to physical attack |  |  |
| FPT\_EMSEC.1/CoreTSF TOE Emanation |  |  |
| FPT\_PHP.3/ICCardReader Resistance to physical attack |  |  |
| FPT\_PHP.3/MSR Resistance to physical attack |  |  |
| **SRED Basis Package** |  |  |
| FMT\_SMR.1/SRED Security roles |  |  |
| FIA\_UID.1/SRED Timing of identification |  |  |
| FIA\_UAU.2/SRED User authentication before any action |  |  |
| FTA\_SSL.3/SRED TSF-initiated termination |  |  |
| FDP\_ITC.1/SRED Import of user data without security attributes |  |  |
| FPT\_FLS.1/SRED Failure with preservation of secure state |  |  |
| FPT\_TST.1/SRED TSF testing |  |  |
| FDP\_ACC.1/SRED Subset access control |  |  |
| FDP\_ACF.1/SRED Security attribute based access control |  |  |
| FPT\_PHP.3/SRED Resistance to physical attack |  |  |
| FPT\_EMSEC.1/SRED TOE Emanation |  |  |
| FMT\_MSA.1/SRED Management of security attributes |  |  |
| FTP\_ITC.1/SRED Inter-TSF trusted channel |  |  |
| **SRED Cryptography Package** |  |  |
| FTP\_ITC.1/SRED\_CRYPTO Inter-TSF trusted channel |  |  |
| FDP\_ITC.2/SRED\_CRYPTO Import of user data with security attributes |  |  |
| FPT\_TDC.1/SRED\_CRYPTO Inter-TSF basic TSF data consistency |  |  |
| FCS\_COP.1/SRED\_Crypto Cryptographic operation |  |  |
| **SRED End-to-end protection** |  |  |
| FDP\_IFC.1/SRED\_E2E Subset information flow control |  |  |
| FDP\_IFF.1/SRED\_E2E Simple security attributes |  |  |
| FMT\_MSA.1/SRED\_E2E Management of security attributes |  |  |
| FIA\_UID.1/SRED\_E2E Timing of identification |  |  |
| FDP\_RIP.1/SRED\_E2E Subset residual information protection |  |  |
| FDP\_ITT.1/SRED\_E2E Basic internal transfer protection |  |  |
| FTP\_TRP.1/SRED\_E2E Trusted path |  |  |

# Glossary and list of acronyms

|  |  |
| --- | --- |
| term | definition / explanation |
| ## … |  |
|  |  |

|  |  |  |
| --- | --- | --- |
| abbreviation | term | definition / explanation |
| ST | Security Target | refer to [1]  |
| ## … |  |  |
|  |  |  |

# Bibliography

Criteria and Methodology

[1] Common Criteria, Part 1: Common Criteria for Information Technology Security Eval-uation, Part 1: Introduction and General Model, Version 3.1, Revision 5, April 2017, CCMB-2017-04-001

[2] Common Criteria, Part 2: Common Criteria for Information Technology Security Eval-uation, Part 2: Security Functional Components, Version 3.1, Revision 5, April 2017, CCMB-2017-04-002

[3] Common Criteria, Part 3: Common Criteria for Information Technology Security Eval-uation, Part 3: Security Assurance Components, Version 3.1, Revision 5, April 2017, CCMB-2017-04-003

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 5, April 2017, CCMB-2017-04-004

Legislatives and Standards

## or none

Evaluation Reports

[ETR] ##Title ETR, ##Author, Version ##, ##Date

See ETR for full list of evaluation reports.

Developer Documents

See ETR for full list

Other documents

## certificates, protection profiles etc.

[PP] Point of interaction protection profile, Version 4, 06th March 2015

[POI CEM] Terminals Evaluation Methodology – CEM refinement, Version 1.0, May 2011, JTEMS