Common.SECC

Rule Book 1.7

Attachment 6b to Annex 3

Template for

Evaluation Technical Report (ETR) – Part AVA

Version 1.1

1April, 2019

**Single Evaluation Report**

as part of the

Evaluation Technical Report

**ETR-Part** **AVA**

**Evaluation of CC Assurance Class** **AVA**

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

Version:  
##Version

Date:  
##Date

Filename:  
Attachment-6-for-Annex-3-AVA\_RB17-1.1.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 |
| 1.00 | 20.11.2018 |  | Initial version |
| 1.01 | 29 November 2018 |  | Endorsed by Common.SECC |
| 1.1 | 1 April 2019 |  | Editorial changes |

**Document Invariants**

|  |  |  |
| --- | --- | --- |
| Name | Invariant (edit here) | Output value |
| Filename and size | calculated automatically | Attachment-6-for-Annex-3-AVA\_RB17-1.1.docx (104693 Bytes) |
| 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

[Basis of the evaluation and documentation used 6](#_Toc6294862)

[1 Evaluation objective / Dependencies 7](#_Toc6294863)

[2 Requirements for evidence and evaluation 8](#_Toc6294864)

[3 Evaluation results 9](#_Toc6294865)

[3.1 AVA\_POI.1/Vulnerability analysis 10](#_Toc6294866)

[3.1.1 AVA\_POI.1.1E 10](#_Toc6294867)

[3.1.2 AVA\_POI.1.2E 12](#_Toc6294868)

[3.1.3 AVA\_POI.1.3E 15](#_Toc6294869)

[3.1.4 AVA\_POI.1.4E 19](#_Toc6294870)

[3.2 Indications for Potential Vulnerabilities 44](#_Toc6294871)

[3.3 Missing Information 44](#_Toc6294872)

[3.4 Questions to / Conditions on the Developer 44](#_Toc6294873)

[3.5 Necessary Changes/Improvements 44](#_Toc6294874)

[3.6 Effects on other Documents 44](#_Toc6294875)

[4 Annex 45](#_Toc6294876)

[4.1 Glossary and list of acronyms 45](#_Toc6294877)

[4.2 Bibliography 45](#_Toc6294878)

# 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 [CC1], [CC2] and [CC3]) and the Common Evaluation Methodology (see [CEM] and [POI CEM]) in accordance with the Security Target [ST]. The subject of the current report is the assessment of the vulnerabilities of the TOE as required by the Assurance Class AVA. This Assurance Class comprises merely one Assurance Family: AVA\_POI (Vulnerability Analysis), whereby it defines several Assurance Components, being dependent on the evaluation assurance package chosen.

The supporting documents [POI AttackPot] and [POI AttackMeth] were used in the course of this evaluation task.

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

AVA\_POI.1.1D and AVA\_POI.1.2D

containing the POI components:

* MSR
* MiddleTSF
* PEDMiddleTSF
* IC Card Reader
* CoreTSF
* CoreTSFKeys

The following contributions were provided:

TOE suitable for testing,

##TOE name (short) Security Target, [ST]

##TOE name (short) Functional Specification, [FSP],

##TOE name (short) Design, [TDS],

##TOE name (short) Security Architecture, [ARC],

##TOE name (short) Life-Cycle, [ALC],

##TOE name (short) Testing, [ATE] (Test specifications and test protocols),

##TOE name (short) Guidance, [AGD], (Operational and Preparative)

and the documents the above contributions refer to.

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

Or, in case of a re-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 potential vulnerabilities identified during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses or quantitative or statistical analysis of the security behaviour of the underlying security mechanisms), could allow attackers to violate the SFRs (TSP). Hereby the requirements given by the Common Criteria, [CC\_P3] are to apply. This report also treats residual vulnerabilities (not violating TSP), if any.

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

|  |  |
| --- | --- |
| **AVA\_POI.1** |  |
| MSR | Basic POI vulnerability analysis |
| MiddleTSF | Basic POI vulnerability analysis |
| PEDMiddleTSF | Low POI vulnerability analysis |
| IC Card Reader | POI-EnhancedLow vulnerability analysis |
| CoreTSF | Moderate POI Vulnerability Analysis |
| CoreTSFKeys | High POI vulnerability analysis |

According to the Common Criteria, Part 3 this assurance component implies the following dependencies:

|  |  |
| --- | --- |
| AVA\_POI.1 | ADV\_ARC.1 Security architecture design  ADF\_FSP.2 Security-enforcing Functional Specification  ADV\_TDS.1 Basic design  AGD\_OPE.1 Operational user guidance  AGD\_PRE.1 Preparative procedures |

# Requirements for evidence and evaluation

The evaluation was performed on the basis of the Common Evaluation Methodology [CEM]. The examinations conducted in this report are grouped into work units according to the CEM and CEM POI. The following table shows the dependencies between the work units defined by the CEM and the Common Criteria assurance elements defined by [CC3].

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 [POI CEM] | Verdict |
| --- | --- | --- | --- | --- |
|  | AVA\_POI.1.1E |  |  | **##PASS ##FAIL ##INCONCLUSIVE** |
|  | AVA\_POI.1.1C |  | AVA\_POI.1-1 |  |
|  |  |  | AVA\_POI.1-2 |  |
|  | AVA\_POI.1.2E |  |  | **##PASS ##FAIL ##INCONCLUSIVE** |
|  | AVA\_POI.1.1C |  | AVA\_POI.1-3 |  |
|  | AVA\_POI.1.3E |  |  | **##PASS ##FAIL ##INCONCLUSIVE** |
|  | AVA\_POI.1.1C |  | AVA\_POI.1-4 |  |
|  |  |  | AVA\_POI.1-5 |  |
|  | AVA\_POI.1.4E |  |  | **##PASS ##FAIL ##INCONCLUSIVE** |
|  | AVA\_POI.1.1C |  | AVA\_POI.1-6 |  |
|  |  |  | AVA\_POI.1-7 |  |
|  |  |  | AVA\_POI.1-8 |  |
|  |  |  | AVA\_POI.1-9 |  |
|  |  |  | AVA\_POI.1-10 |  |
|  |  |  | AVA\_POI.1-11 |  |
|  |  |  | AVA\_POI.1-12 |  |

# Evaluation results

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

## AVA\_POI.1/Vulnerability analysis

**Summary Verdict for the Assurance Component AVA\_POI.1:**  
**##PASS ##FAIL ##INCONCLUSIVE**.  
The **Magnetic Stripe Reader component of the POI, MiddleTSF’s components, PEDMiddleTSF’s components, IC Card Reader components, CoreTSF’s components and CoreTSFKeys components** meet all requirements of the assurance component AVA\_POI.1. This result is based on the results provided by the evaluator actions and performed work units below.

### AVA\_POI.1.1E

Evaluator action element:

**AVA\_POI.1.1E:** The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

Content and presentation of evidence elements:

**AVA\_POI.1.1C:** The **Magnetic Stripe Reader component of the POI,** **MiddleTSF’s components,** **PEDMiddleTSF’s components, IC Card Reader components,** **CoreTSF’s components** and **CoreTSFKeys** **components** shall be suitable for testing.

Work units:

**[AVA\_POI.1-1]** The evaluator ***shall examine*** the **Magnetic Stripe Reader component of the POI, MiddleTSF’s components, PEDMiddleTSF’s components, IC Card Reader com-ponents, CoreTSF’s components and CoreTSFKeys components** to determine that the test configuration is consistent with the configuration under evaluation as specified in the ST.

The current work unit deals with the question whether the component of the POI under testing is configured in accordance with the ST.

Summary:

The evaluator found the related information in [ST], chap. Add chapter. The evaluated items of the representation were the following Add summary .

Analysis:

The ST, sec. Add section lists the following configurations of the TOE being under evaluation: Add configuration

The evaluator applied the following procedure(s) in order to determine the current instantiations of the TOE provided: Add description

The developer provided the following instantiations of the TOE: Add, if applicable, the instantiations of the TOE

The evaluator compared { Add configuration } with {Add, if applicable, the instantiations of the TOE } and {Add TOE reference}, respectively, and found out that they are or are not commensurate with each other.

Then the evaluator referred to the operational environment as stated in the ST, sec. Add section and found the following conditions being applicable to the test environment: Add description. The evaluator checked for fulfilment of these conditions within the current test environment.

Or: Then the evaluator referred to the operational environment as stated in the ST, sec. Add section and did not find any special conditions which could be applicable to the test environment.

The tests were performed using calibrated test resources. The quality of calibration is confirmed by the accreditation certificate Add information. Or: The evaluator confirms that the test equipment used is calibrated as appropriate.

Assessment and Verdict:

The evaluator’s analysis showed the following:

* not all configurations of the components of the POI declared being under evaluation in the ST are also being tested; the configuration Add configuration was or was not tested due to the reason that Add reason
* the unique reference of the components of the POI under testing is not commensurate with the configuration of the component of the POI being under evaluation as stated in the ST and with the component of the POI reference as managed by the CM.

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

**[AVA\_POI.1-2/MSR]** The evaluator ***shall examine*** the **Magnetic Stripe Reader component of the POI, MiddleTSF’s components, PEDMiddleTSF’s components, IC Card Reader components, CoreTSF’s components and CoreTSFKeys components** to determine that it has been installed properly and is in a known state.

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 in Add reference. The evaluated items of the representation were the following Add information.

Analysis:

Or: The installation and configuration steps have already been done in the context of the work unit AGD\_PRE.1-3 Add reference to section in AGD report.

Assessment and Verdict:

Based on the analysis above the evaluator confirms (or disproves) that the component of the POI being tested is exactly commensurate with the component of the POI as it is intended in the ST (‘known state’). He encountered no (or the following) difficulties during this activity: Add description

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

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

### AVA\_POI.1.2E

Evaluator action element:

AVA\_POI.1.2E The evaluator *shall perform* a search of public domain sources to identify potential vulnerabilities in the **Magnetic Stripe Reader component of the POI, MiddleTSF’s components, PEDMiddleTSF’s components, IC Card Reader components, CoreTSF’s components and CoreTSFKeys components**

Content and presentation of evidence elements:

AVA\_POI.1.1C The **Magnetic Stripe Reader component of the POI, MiddleTSF’s components, PEDMiddleTSF’s components, IC Card Reader components, CoreTSF’s components and CoreTSFKeys components** shall be suitable for testing.

Work units:

**[AVA\_POI.1-3]** The evaluator ***shall examine*** sources of information publicly available to identify potential vulnerabilities in the **Magnetic Stripe Reader component of the POI, MiddleTSF’s components, PEDMiddleTSF’s components, IC Card Reader components, CoreTSF’s components and CoreTSFKeys components**.

The current work unit focuses on what actions were taken to identify potential vulnerabilities. A list of potential vulnerabilities applicable to the component of the POI is expected in the context of the work unit AVA\_POI.1-5.

Summary:

The evaluator applied the following procedure for investigating publicly available sources of information for the **Magnetic Stripe Reader component of the POI,** **MiddleTSF’s components,** **PEDMiddleTSF’s components, IC Card Reader components,** **CoreTSF’s components** and **CoreTSFKeys** **components** of the POI type: Add summary

Analysis:

**Magnetic Stripe Reader component of the POI:**

The component of the POI type in question is Add component (cf. ASE\_INT.1-6, ASE\_INT.1-7 in ASE report). The component of the POI uses the following specific technologies: Add information, see [TDS], sec. Add section.

During the previous evaluation activities the evaluator identified the following areas of concern:

1. area\_1, cf. [ADV\_Report], sec. Add reference,
2. area\_2, cf. [AGD\_Report], sec. Add reference,
3. area\_2, cf. [ATE\_Report], sec. Add reference,
4. etc.

Considering an attacker with *equal or higher then POI-Basic* attack potential, the evaluators proceed as follows in order to identify potential vulnerabilities in component of the POI’s technologies: Add description

**MiddleTSF’s components**

The component of the POI type in question is Add component (cf. ASE\_INT.1-6, ASE\_INT.1-7 in ASE report). The component of the POI uses the following specific technologies: Add information, see [TDS], sec. Add section.

During the previous evaluation activities the evaluator identified the following areas of concern:

1. area\_1, cf. [ADV\_Report], sec. Add reference,
2. area\_2, cf. [AGD\_Report], sec. Add reference,
3. area\_2, cf. [ATE\_Report], sec. Add reference,
4. etc.

Considering an attacker with *equal or higher then POI-Basic* attack potential, the evaluators proceed as follows in order to identify potential vulnerabilities in component of the POI’s technologies: Add description

**PEDMiddleTSF’s components**

The component of the POI type in question is Add component (cf. ASE\_INT.1-6, ASE\_INT.1-7 in ASE report). The component of the POI uses the following specific technologies: Add information, see [TDS], sec. Add section.

During the previous evaluation activities the evaluator identified the following areas of concern:

1. area\_1, cf. [ADV\_Report], sec. Add reference,
2. area\_2, cf. [AGD\_Report], sec. Add reference,
3. area\_2, cf. [ATE\_Report], sec. Add reference,
4. etc.

Considering an attacker with *equal or higher then POI-Basic* attack potential, the evaluators proceed as follows in order to identify potential vulnerabilities in component of the POI’s technologies: Add description

**IC Card Reader components**

The component of the POI type in question is Add component (cf. ASE\_INT.1-6, ASE\_INT.1-7 in ASE report). The component of the POI uses the following specific technologies: Add information, see [TDS], sec. Add section.

During the previous evaluation activities the evaluator identified the following areas of concern:

1. area\_1, cf. [ADV\_Report], sec. Add reference,
2. area\_2, cf. [AGD\_Report], sec. Add reference,
3. area\_2, cf. [ATE\_Report], sec. Add reference,
4. etc.

Considering an attacker with *equal or higher then POI-Basic* attack potential, the evaluators proceed as follows in order to identify potential vulnerabilities in component of the POI’s technologies: Add description

**CoreTSF’s components**

The component of the POI type in question is Add component (cf. ASE\_INT.1-6, ASE\_INT.1-7 in ASE report). The component of the POI uses the following specific technologies: Add information, see [TDS], sec. Add section.

During the previous evaluation activities the evaluator identified the following areas of concern:

1. area\_1, cf. [ADV\_Report], sec. Add reference,
2. area\_2, cf. [AGD\_Report], sec. Add reference,
3. area\_2, cf. [ATE\_Report], sec. Add reference,
4. etc.

Considering an attacker with *equal or higher then POI-Basic* attack potential, the evaluators proceed as follows in order to identify potential vulnerabilities in component of the POI’s technologies: Add description

**CoreTSFKeys** **components**

The component of the POI type in question is Add component (cf. ASE\_INT.1-6, ASE\_INT.1-7 in ASE report). The component of the POI uses the following specific technologies: Add information, see [TDS], sec. Add section.

During the previous evaluation activities the evaluator identified the following areas of concern:

1. area\_1, cf. [ADV\_Report], sec. Add reference,
2. area\_2, cf. [AGD\_Report], sec. Add reference,
3. area\_2, cf. [ATE\_Report], sec. Add reference,
4. etc.

Considering an attacker with *equal or higher then POI-Basic* attack potential, the evaluators proceed as follows in order to identify potential vulnerabilities in component of the POI’s technologies: Add description

…

Assessment and Verdict:

Based on the analysis above the evaluator confirms (disproves) that he was able to identify potential vulnerabilities in the components of the POI using information available.

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

**Verdict for AVA\_POI.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.

### AVA\_POI.1.3E

Evaluator action element:

AVA\_POI.1.3E The evaluator *shall perform* an independent vulnerability analysis of the **Magnetic Stripe Reader component of the POI, MiddleTSF’s components, PEDMiddleTSF’s components, IC Card Reader components, CoreTSF’s components and CoreTSFKeys components** using the guidance documentation, functional specification, design and security architecture description **as well as the available implementation representation and the mapping of SFRs to the implementation representation** to identify potential vulnerabilities.

Content and presentation of evidence elements:

AVA\_POI.1.1C The **Magnetic Stripe Reader component of the POI, MiddleTSF’s components, PEDMiddleTSF’s components, IC Card Reader components, CoreTSF’s components and CoreTSFKeys components** shall be suitable for testing.

Work units:

**[AVA\_POI.1-4]** The evaluator ***shall conduct*** a search of ST, guidance documentation, functional specification, **Magnetic Stripe Reader component of the POI, MiddleTSF’s components, PEDMiddleTSF’s components, IC Card Reader components, CoreTSF’s components and CoreTSFKeys components** design and security architecture description evidence to identify possible potential vulnerabilities in the **Magnetic Stripe Reader component of the POI, MiddleTSF’s components, PEDMiddleTSF’s components, IC Card Reader components, CoreTSF’s components and CoreTSFKeys components**.

The current work unit focuses on what actions were taken to identify potential vulnerabilities. A final list of potential vulnerabilities applicable to the component of the POI is expected in the context of the work unit AVA\_POI.1-5, where the results of examination of the publicly available sources (work unit AVA\_POI.1-3) and of the current work unit will be merged.

Summary:

The evaluator applied the following procedure for investigating relevant evaluation contributions for the **Magnetic Stripe Reader component of the POI,** **MiddleTSF’s components,** **PEDMiddleTSF’s components, IC Card Reader components,** **CoreTSF’s components** and **CoreTSFKeys** **components** of the POI: Add summary

Analysis:

The evaluator identified specific areas of concern for the current component of the POI in the work unit AVA\_POI.1-3 above, whereby the following evaluation contributions were used: ASE, ADV, ATE and AGD.

The evaluator searched for potential vulnerabilities for the current component of the POI whilst evaluating the developer contributions for the single evaluation aspects in the context of the assurance classes ADV, AGD and ATE, where the relevant clues are also documented (see Add references to sections in the reports ADV, ATE and AGD).

The certification body did not provide any list of generic potential vulnerabilities being relevant for the components of the POI type.

Or: The certification body provided a list of generic potential vulnerabilities being relevant for the components of the POI type, cf. Add reference to vulnerability list.

Having performed the previous work unit and the current activities, the evaluator identified the following potential vulnerabilities accounting merely the components of the POI type / components of the POI specific technology / components of the POI specific implementation, but not its intended operational environment (so called ‘raw list’):

**Magnetic Stripe Reader component of the POI**

VUL\_R.1: …,

VUL\_R.2: …

…

**MiddleTSF’s components**

…

This sequence of the ‘raw’ vulnerabilities also reflects the priorities in which they should be considered. The reasons for this evaluator’s point of view are as follows:

**Magnetic Stripe Reader component of the POI**

VUL\_R.1: Add Explanation for exploitability / non-exploitability

VUL\_R.2: Add Explanation for possible exploitability / non-exploitability

…

**MiddleTSF’s components**

…

Having performed the analysis above the evaluator decided to consider the following remaining potential vulnerabilities, which may be exploitable in the intended component of the POI’s environment:

**Magnetic Stripe Reader component of the POI**

VUL\_P.1: == VUL\_R.1,

…

**MiddleTSF’s components**

…

The question, whether this potential vulnerability can indeed be exploited in the intended environment, will be considered in the further analysis within this assurance component.

Assessment and Verdict:

Based on the analysis above the evaluator confirms (or disproves) that he was able to identify potential vulnerabilities in the components of the POI using components of the POI specific information available.

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

**[AVA\_POI.1-5** The evaluator ***shall record*** in the ETR the identified potential vulnerabilities that are candidates for testing and applicable to the **Magnetic Stripe Reader component of the POI, MiddleTSF’s components, PEDMiddleTSF’s components, IC Card Reader components, CoreTSF’s components and CoreTSFKeys components** in its operational environment.

The current work unit deals with creating the final list of potential vulnerabilities identified in the component of the POI which may be exploitable in its operational environment.

Summary:

The evaluator applied the following procedure while creating a list of potential vulnerabilities applicable to the components of the POI in its operational environment: Add summary

Analysis:

Firstly, the evaluator created a ‘raw list’ of potential vulnerabilities based on the results gained while performing the previous work unit; this ‘raw list’ merely considers the current components of the POI type / components of the POI specific technology / components of the POI specific implementation, but not its intended operational environment:

VUL\_R.1: …

VUL\_R.2: ..

…

Secondly, the evaluator reconstructed the formal assumptions about the component of the POI operational environment. In order to do this he referred to the [ST], sec. Add reference from ST:

|  |  |
| --- | --- |
| A.1 | short description of the assumption, cf. also [AGD\_OPE], sec. Add reference |
| A.2 | short description of the assumption, cf. also [AGD\_OPE], sec. Add reference |
| … | … |
| A.n | short description of the assumption, cf. also [AGD\_OPE], sec. Add reference |

Then he analysed, for each potential vulnerability of the ‘raw list’, whether it might be exploitable in the intended operational environment:

VUL\_R.1:

Explanation for exploitability / non-exploitability considering the operational environment.

VUL\_R.2:

Explanation for possible exploitability / non-exploitability considering the operational environment.

…

Having performed the analysis above the evaluator decided to consider the following remaining potential vulnerabilities, which may be exploitable in the intended component of the POI’s environment:

VUL\_P.1: == VUL\_R.1,

…

This list of potential vulnerabilities being applicable to the component of the POI in its operational environment will be reported (cited) in the ETR. We do not recommend publishing the list of the potential vulnerabilities.

The question, whether this potential vulnerability can indeed be exploited in the intended environment, will be considered in the further analysis within this assurance component.

Assessment and Verdict:

The evaluator confirms (or disproves) that he was able to create a list of potential vulnerabilities applicable to the component of the POI in its operational environment.

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

**Verdict for AVA\_POI.1.3E:**  
**##PASS ##FAIL ##INCONCLUSIVE**   
The evaluator confirms (##or disproves) that the information provided in the analysed documentation meet all requirements for content and presentation of evidence.

### AVA\_POI.1.4E

Evaluator action element:

AVA\_POI.1.4E The evaluator *shall conduct* penetration testing, based on the identified potential vulnerabilities, to determine that the **Magnetic Stripe Reader component of the POI, MiddleTSF’s components, PEDMiddleTSF’s components, IC Card Reader components, CoreTSF’s components and CoreTSFKeys components** is resistant to attacks performed by an attacker possessing **attack potential equal or higher than** **components assigned attack potential with a minimum attack potential for the exploitation phase of a value defined in [POI AttackPot]:**

|  |  |
| --- | --- |
| **MSR** | **POI-Basic** |
| **MiddleTSF** | **POI-Basic** |
| **PEDMiddleTSF** | **POI-Low** |
| **IC Card Reader** | **POI-EnhancedLow** |
| **CoreTSF** | **POI-Moderate** |
| **CoreTSFKeys** | **POI-High** |

Content and presentation of evidence elements:

AVA\_POI.1.1C/MSR The **Magnetic Stripe Reader component of the POI, MiddleTSF’s components, PEDMiddleTSF’s components, IC Card Reader components, CoreTSF’s components and CoreTSFKeys components** shall be suitable for testing.

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

PCIG2: In particular the evaluator shall exploit public-knowledge vulnerabilities on all SFR-supporting TSFIs of the following types: Link Layer Protocols, IP Protocols, Security Protocols, IP Services. Exploitation methods shall include at least replay of messages and exploitation of insecure exception handling.

Work units:

**[AVA\_POI.1-6]** The evaluator ***shall devise*** penetration tests, based on the independent search for potential vulnerabilities.

The current work unit deals rather with a ‘mental’ preparation of the evaluator for penetration testing. Together with the next work unit they represent a common context while reflecting different abstraction levels: the current work unit deals with a ‘high level’ outlining sensible attack scenarios planned to be performed as penetration tests, whilst the next one – with producing the related penetration test documentation including the relevant test cases and other necessary conditions for conducting penetration tests.

Due to these deliberations, the activity ‘devising penetration tests’ means – in the current context – ‘inventing appropriate attack scenarios for penetration tests’.

Summary:

The evaluator applied the following procedure while devising the set of attack scenariosfor penetration testsbased on the list of potential vulnerabilities applicable to the components of the POI in its operational environment: Add summary.

Analysis:

Based on the potential vulnerabilities identified as the candidates for penetration testing in the previous work unit, the evaluator devised the attack scenarios for penetration tests (see table below) which could exploit these potential vulnerabilities in the components of the POI’s operational environment.

He also considered the major characteristics of the security architecture as described in Add reference to ARC being not covered by functional testing (cf. ATE\_FUN, sec. Add reference).

**Magnetic Stripe Reader component**

The major characteristics are:

MCH\_1: …

MCH\_2: ..

…

The evaluator referred to the documentation for the functional testing in ATE Add reference and came to the conclusion that all major characteristics of the security architecture have already sufficiently (or not completely) been covered by functional testing, see ATE, sec. Add reference to ATE report.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Attack scenario for penetration testing | Short description of the attack scenario | Potential vulnerabilities might be exploited by the attack scenario (as listed in AVA\_VAN.1-5) | Theoretically estimated minimal attack potential needed for performing this AS, if possible / appropriate, cf. [POI AttackPot] | Comments |
| AS.1 | Add description | - VUL\_P.1  Add key words  - VUL\_P.2  Add key words  - … | Elapsed time = value =  points explanation for the value assigned, if necessary  Expertise =  value =  points explanation for the value assigned, if necessary  component of the POI Knowledge = value = points explanation for the value assigned, if necessary  Opportunity = value = points explanation for the value assigned, if necessary  Equipment = value = points explanation for the value assigned, if necessary  Sum: points | Add comments |
| … | Add description | … | … | … |

Table 1: Attack scenarios: Magnetic Stripe Reader component

The table above shows that each potential vulnerability identified as a candidate for penetration testing in the previous work unit is or is not covered by at least one attack scenario for penetration testing.

Since the attack scenarios AS.1, AS.3,…(or other) possess an attack potential being beyond *POI-Basic*, the evaluator decided to dispense with performing penetration tests for them, but to report these attack scenarios and the potential vulnerabilities attributed to them as residual vulnerabilities (VUL\_RSD.n) in the ETR (cf. the work unit AVA\_POI.1-12).

Or only add reference to the table in the Attack methods document performed by the evaluator

**MiddleTSF’s components**

The major characteristics are:

MCH\_1: …

MCH\_2: …

…

The evaluator referred to the documentation for the functional testing [ATE] and came to the conclusion that all major characteristics of the security architecture have already sufficiently (or not completely) been covered by functional testing, see Add, if applicable reference to ATE report

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Attack scenario for penetration testing | Short description of the attack scenario | Potential vulnerabilities might be exploited by the attack scenario (as listed in AVA\_VAN.1-5) | Theoretically estimated minimal attack potential needed for performing this AS, if possible / appropriate, cf. [POI AttackPot] | Comments |
| AS.1 | Add description | - VUL\_P.1  Add key words  - VUL\_P.2  Add key words  - … | Elapsed time = value =  points explanation for the value assigned, if necessary  Expertise =  value =  points explanation for the value assigned, if necessary  component of the POI Knowledge = value = points explanation for the value assigned, if necessary  Opportunity = value = points explanation for the value assigned, if necessary  Equipment = value = points explanation for the value assigned, if necessary  Sum: points | Add comments |
| … | Add description | … | … | … |

Table 2: Attack scenarios: MiddleTSF’s components

The table above shows that each potential vulnerability identified as a candidate for penetration testing in the previous work unit is (or not) covered by at least one attack scenario for penetration testing.

Since the attack scenarios AS.1, AS.3,…(or other) possess an attack potential being beyond *POI-Basic*, the evaluator decided to dispense with performing penetration tests for them, but to report these attack scenarios and the potential vulnerabilities attributed to them as residual vulnerabilities (VUL\_RSD.n) in the ETR (cf. the work unit AVA\_POI.1-12).

Or add reference to the table in the Attack methods document performed by the evaluator

**PEDMiddleTSF’s components**

The major characteristics are:

MCH\_1: …

MCH\_2: …

…

The evaluator referred to the documentation for the functional testing [ATE] and came to the conclusion that all major characteristics of the security architecture have already sufficiently (or not completely) been covered by functional testing, see Add, if applicable reference to ATE report

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Attack scenario for penetration testing | Short description of the attack scenario | Potential vulnerabilities might be exploited by the attack scenario (as listed in AVA\_VAN.1-5) | Theoretically estimated minimal attack potential needed for performing this AS, if possible / appropriate, cf. [POI AttackPot] | Comments |
| AS.1 | Add description | - VUL\_P.1  Add key words  - VUL\_P.2  Add key words  - … | Elapsed time = value =  points explanation for the value assigned, if necessary  Expertise =  value =  points explanation for the value assigned, if necessary  component of the POI Knowledge = value = points explanation for the value assigned, if necessary  Opportunity = value = points explanation for the value assigned, if necessary  Equipment = value = points explanation for the value assigned, if necessary  Sum: points | Add comments |
| … | Add description | … | … | … |

Table 3: Attack scenarios: PEDMiddleTSF’s components

The table above shows that each potential vulnerability identified as a candidate for penetration testing in the previous work unit is (or not) covered by at least one attack scenario for penetration testing.

Since the attack scenarios AS.1, AS.3,…(or other) possess an attack potential being beyond *POI-Low*, the evaluator decided to dispense with performing penetration tests for them, but to report these attack scenarios and the potential vulnerabilities attributed to them as residual vulnerabilities (VUL\_RSD.n) in the ETR (cf. the work unit AVA\_POI.1-12).

Or add reference to the table in the Attack methods document performed by the evaluator

**IC Card Reader components**

The major characteristics are:

MCH\_1: …

MCH\_2: …

…

The evaluator referred to the documentation for the functional testing [ATE] and came to the conclusion that all major characteristics of the security architecture have already sufficiently (or not completely) been covered by functional testing, see Add, if applicable reference to ATE report

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Attack scenario for penetration testing | Short description of the attack scenario | Potential vulnerabilities might be exploited by the attack scenario (as listed in AVA\_VAN.1-5) | Theoretically estimated minimal attack potential needed for performing this AS, if possible / appropriate, cf. [POI AttackPot] | Comments |
| AS.1 | Add description | - VUL\_P.1  Add key words  - VUL\_P.2  Add key words  - … | Elapsed time = value =  points explanation for the value assigned, if necessary  Expertise =  value =  points explanation for the value assigned, if necessary  component of the POI Knowledge = value = points explanation for the value assigned, if necessary  Opportunity = value = points explanation for the value assigned, if necessary  Equipment = value = points explanation for the value assigned, if necessary  Sum: points | Add comments |
| … | Add description | … | … | … |

Table 4: Attack scenarios: IC Card Reader components

The table above shows that each potential vulnerability identified as a candidate for penetration testing in the previous work unit is (or not) covered by at least one attack scenario for penetration testing.

Since the attack scenarios AS.1, AS.3, …(or other) possess an attack potential being beyond *POI-EnhancedLow*, the evaluator decided to dispense with performing penetration tests for them, but to report these attack scenarios and the potential vulnerabilities attributed to them as residual vulnerabilities (VUL\_RSD.n) in the ETR (cf. the work unit AVA\_POI.1-12).

Or only add reference to the table in the Attack methods document performed by the evaluator

**CoreTSF’s components**

The major characteristics are:

MCH\_1: …

MCH\_2: …

…

The evaluator referred to the documentation for the functional testing [ATE] and came to the conclusion that all major characteristics of the security architecture have already sufficiently (or not completely) been covered by functional testing, see Add, if applicable reference to ATE report.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Attack scenario for penetration testing | Short description of the attack scenario | Potential vulnerabilities might be exploited by the attack scenario (as listed in AVA\_VAN.1-5) | Theoretically estimated minimal attack potential needed for performing this AS, if possible / appropriate, cf. [POI AttackPot] | Comments |
| AS.1 | Add description | - VUL\_P.1  Add key words  - VUL\_P.2  Add key words  - … | Elapsed time = value =  points explanation for the value assigned, if necessary  Expertise =  value =  points explanation for the value assigned, if necessary  component of the POI Knowledge = value = points explanation for the value assigned, if necessary  Opportunity = value = points explanation for the value assigned, if necessary  Equipment = value = points explanation for the value assigned, if necessary  Sum: points | Add comments |
| … | Add description | … | … | … |

Table 5: Attack scenarios: CoreTSF’s components

The table above shows that each potential vulnerability identified as a candidate for penetration testing in the previous work unit is (or not) covered by at least one attack scenario for penetration testing.

Since the attack scenarios AS.1, AS.3,… (or other) possess an attack potential being beyond *POI-Moderate*, the evaluator decided to dispense with performing penetration tests for them, but to report these attack scenarios and the potential vulnerabilities attributed to them as residual vulnerabilities (VUL\_RSD.n) in the ETR (cf. the work unit AVA\_POI.1-12).

Or only add reference to the table in the Attack methods document performed by the evaluator

**CoreTSFKeys components**

The major characteristics are:

MCH\_1: …

MCH\_2: …

…

The evaluator referred to the documentation for the functional testing [ATE] and came to the conclusion that all major characteristics of the security architecture have already sufficiently (or not completely) been covered by functional testing, see Add, if applicable reference to ATE report

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Attack scenario for penetration testing | Short description of the attack scenario | Potential vulnerabilities might be exploited by the attack scenario (as listed in AVA\_VAN.1-5) | Theoretically estimated minimal attack potential needed for performing this AS, if possible / appropriate, cf. [POI AttackPot] | Comments |
| AS.1 | Add description | - VUL\_P.1  Add key words  - VUL\_P.2  Add key words  - … | Elapsed time = ##value = ##points ##explanation for the value assigned, if necessary  Expertise = ##value = ##points ##explanation for the value assigned, if necessary  component of the POI Knowledge = ##value = ##points ##explanation for the value assigned, if necessary  Opportunity = ##value = ##points ##explanation for the value assigned, if necessary  Equipment = ##value = ##points ##explanation for the value assigned, if necessary  Sum: ## points | Add comments |
| … | Add description | … | … | … |

Table 6: Attack scenarios: CoreTSFKeys components

The table above shows that each potential vulnerability identified as a candidate for penetration testing in the previous work unit is (or not) covered by at least one attack scenario for penetration testing.

Since the attack scenarios AS.1, AS.3,…(or other) possess an attack potential being beyond *POI-High*, the evaluator decided to dispense with performing penetration tests for them, but to report these attack scenarios and the potential vulnerabilities attributed to them as residual vulnerabilities (VUL\_RSD.n) in the ETR (cf. the work unit AVA\_POI.1-12).

Or only add reference to the table in the Attack methods document performed by the evaluator

Assessment and Verdict:

The evaluator confirms (or disproves) that he was able to create a list of attack scenarios for penetration tests being sensible in components of the POI’s operational environment.

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

**[AVA\_POI.1-7]** The evaluator ***shall produce*** penetration test documentation for the tests based on the list of potential vulnerabilities in sufficient detail to enable the tests to be repeatable. […]

The current work unit deals with producing test documentation (specification) for the penetration tests.

Summary:

The evaluator produced the penetration test documentation (test specification) based on the attack scenarios developed in the previous work unit.

Analysis:

Based on the list of attack scenarios being sensible in the component of the POI’s operational environment created within the previous work unit the evaluator specified the penetration tests needed to be performed.

While producing penetration test documentation the evaluator did not encounter additional potential vulnerabilities and/or additional attack scenarios to which the component of the POI in its environment could be susceptible.

Or While producing penetration test documentation the evaluator encountered additional potential vulnerabilities and/or additional attack scenarios to which the component of the POI in its environment could be susceptible. Hence, he iterated the work unit AVA\_POI.1-5 and supplemented the work unit AVA\_POI.1-6.

Assessment and Verdict:

The evaluator confirms (or disproves) that he was able to create penetration test documentation in sufficient detail to enable the tests to be repeatable.

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

**[AVA\_POI.1-8]** The evaluator ***shall conduct*** penetration testing.

The current work unit deals with practical conducting penetration testing.

Summary:

The evaluator conducted penetration testing Add the premises of the developer (address) or/and in the evaluation lab on Add date. The following persons attended this activity: the responsible certifier Add name, supporting staff of the developer.

Add additional statements, if necessary.

Analysis:

The evaluator performed each penetration test as planned and specified in the penetration test documentation created in the context of the previous work unit.

All additional conditions in and elements of the test environment needed for performing these tests, if any, are directly stated within the test protocols in the next work unit.

Assessment and Verdict:

The evaluator confirms (or disproves) that he was able to conduct penetration testing according to his test documentation.

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

**[AVA\_POI.1-9]** The evaluator ***shall record*** the actual results of the penetration tests.

The current work unit deals with recording penetration test results.

Summary:

No deviations were found between the expected and the actual results of the penetration tests.

Or There are the following deviations between the expected and the actual results of the penetration tests, namely for the test cases:

|  |  |  |  |
| --- | --- | --- | --- |
| Test ID | Expected result, cf. specification in AVA\_POI.1-6 | actual test result | comments (critical or not for the current activity with reference to the analysis below) |
| ET.1 | … | … | … |
| … | … | … | … |

Table 7: Penetration test deviations (overview)

Analysis:

The setup and the results of the penetration tests performed by the evaluator are shown in the table below.

The column ‘Attack Scenario’ refers to the corresponding attack scenario as stated in the work unit AVA\_POI.1-6. The column ‘SFRs’ denotes the related SFRs as defined in [ST], for which a certain security aspect is tested. The column ‘test reference’ lists references and contains comments and rationale like deviations of test results, where necessary.

The corresponding protocol files (test logs) carry a file name Add name containing the relevant Test-ID from the table below.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Test ID | Attack Scenario, cf. AVA\_POI.1-6 | SFRs related, cf. [ST] | triggering instructions / actions | Security aspect, test description and result | Test reference / additional conditions / result deviations |
| ET.1 | AS…. | … |  | It is the goal of this test to …  Test description:  …  Expected result: …  Actual result: … | … |
| … |  |  |  |  |  |

Table 8: Penetration tests

The table above shows, amongst other, that no deviations were found between the expected and the actual test results.

Or The table above shows, amongst other, that there are deviations between the expected and the actual test results. They are reasoned in the last column of the table.

Assessment and Verdict:

The evaluator confirms (or disproves) that he was able to record the actual results of the penetration tests.

No deviations were found between the actual results of the penetration tests and the expected test results, which would not explained satisfactory.

Or There are some deviations between the actual results of the penetration tests and the expected test results having not been explained satisfactory.

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

**[AVA\_POI.1-10]** The evaluator ***shall report*** in the ETR the evaluator penetration testing effort, outlining the testing approach, configuration, depth and results.

The current work unit deals with reporting the penetration testing conducted.

Summary:

Add summary

Analysis:

Overview:

The penetration testing was partially performed using the developer’s testing environment, partially using the test environment of the CLEF.

All configurations of the component of the POI being intended to be covered by the current evaluation were tested.

The overall test result is that no deviations were found between the expected and the actual test results; moreover, no attack scenario with the attack potential Basic was actually successful.

Penetration testing approach:

Add a short overview/listing here for **each** component

**Magnetic Stripe Reader component of the POI**

…

**MiddleTSF’s components,**

…

**PEDMiddleTSF’s components,**

…

**IC Card Reader components,**

…

**CoreTSF’s components**

…

**CoreTSFKeys** **components**

…

Components of the POI test configurations:

Add a short overview/listing here for **each** component

**Magnetic Stripe Reader component of the POI**

…

**MiddleTSF’s components,**

…

**PEDMiddleTSF’s components,**

…

**IC Card Reader components,**

…

**CoreTSF’s components**

…

**CoreTSFKeys** **components**

…

Attack scenarios having been tested:

Add a short overview/listing here for **each** component

**Magnetic Stripe Reader component of the POI**

…

**MiddleTSF’s components,**

…

**PEDMiddleTSF’s components,**

…

**IC Card Reader components,**

…

**CoreTSF’s components**

…

**CoreTSFKeys** **components**

…

SFRs penetration tested:

Add a short overview/listing here for **each** component

**Magnetic Stripe Reader component of the POI**

…

**MiddleTSF’s components,**

…

**PEDMiddleTSF’s components,**

…

**IC Card Reader components,**

…

**CoreTSF’s components**

…

**CoreTSFKeys** **components**

…

If applicable The remaining SFRs were analysed, but not penetration tested due to non-exploitability of the related attack scenarios in the component of the POI’s operational environment also including an attacker with an *equal or higher than the assigned attack potential:*

|  |  |
| --- | --- |
| **MSR** | **POI-Basic** |
| **MiddleTSF** | **POI-Basic** |
| **PEDMiddleTSF** | **POI-Low** |
| **IC Card Reader** | **POI-EnhancedLow** |
| **CoreTSF** | **POI-Moderate** |
| **CoreTSFKeys** | **POI-High** |

Verdict for the sub-activity:

The overall test result is that (no) deviations were found between the expected and the actual test results. (No) attack scenario with an attack potential *equal or higher than the assigned attack potential (*was actually successful) in the components of the POI’s operational environment as defined in [ST] provided that all measures required by the developer are applied.

|  |  |
| --- | --- |
| **MSR** | **POI-Basic** |
| **MiddleTSF** | **POI-Basic** |
| **PEDMiddleTSF** | **POI-Low** |
| **IC Card Reader** | **POI-EnhancedLow** |
| **CoreTSF** | **POI-Moderate** |
| **CoreTSFKeys** | **POI-High** |

Assessment and Verdict:

The evaluator confirms (or disproves) that he was able to report his penetration testing effort for the ETR.

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

**[AVA\_POI.1-11]** The evaluator ***shall examine*** the results of all penetration testing to determine that the **Magnetic Stripe Reader component of the POI, MiddleTSF’s components, PEDMiddleTSF’s components, IC Card Reader components, CoreTSF’s components and CoreTSFKeys components**, in its operational environment, are resistant to an attacker possessing an attack potential as follows:

MSR POI-Basic

MiddleTSF POI-Basic

PEDMiddleTSF POI-Low

IC Card Reader POI-EnhancedLow

CoreTSF POI-Moderate

CoreTSFKeys POI-High

The current work unit deals with assessment whether the components of the POI are resistant as claimed in the [ST].

*The current work unit is the only one where the evaluator has to assess the results of the penetration testing concerning their impact on the vulnerability assessment.* The violation of the SFRs is the criteria for decision, whether an identified potential vulnerability is relevant for the components of the POI.   
Please note that there might be SFRs (e.g. FCS\_COP.1) requiring certain security functionality, but not stating which property (confidentiality, integrity, etc.) of an asset is protected by them. In such a case it is necessary also to refer to the security objectives related to this SFR.   
Addressing security objectives might also be necessary for the assessment of sufficiency of security mechanisms covered by ADV\_ARC.

Summary:

**Magnetic Stripe Reader component of the POI,**

The evaluator did find any clues for the component of the POI being not resistant to attackers with an attack potential of *equal or higher than POI-Basic*.

Or There are the following clues for the component of the POI being not resistant to attackers with an attack potential of *equal or higher than POI-Basic*:

Clue\_1: …

Clue\_2: …

…

**MiddleTSF’s components**

The evaluator did find any clues for the component of the POI being not resistant to attackers with an attack potential of *equal or higher than POI-Basic*.

Or There are the following clues for the component of the POI being not resistant to attackers with an attack potential of *equal or higher than POI-Basic*:

Clue\_1: …

Clue\_2: …

…

**PEDMiddleTSF’s components**

The evaluator did find any clues for the component of the POI being not resistant to attackers with an attack potential of *POI-Low*.

Or There are the following clues for the component of the POI being not resistant to attackers with an attack potential of *POI-Low*:

Clue\_1: …

Clue\_2: …

…

**IC Card Reader components**

The evaluator did find any clues for the component of the POI being not resistant to attackers with an attack potential of *POI-EnhancedLow*.

Or There are the following clues for the component of the POI being not resistant to attackers with an attack potential of *POI-EnhancedLow*:

Clue\_1: …

Clue\_2: …

…

**CoreTSF’s components**

The evaluator did find any clues for the component of the POI being not resistant to attackers with an attack potential of *POI-Moderate*.

Or There are the following clues for the component of the POI being not resistant to attackers with an attack potential of *POI-Moderate*:

Clue\_1: …

Clue\_2: …

…

**CoreTSFKeys components**

The evaluator did find any clues for the component of the POI being not resistant to attackers with an attack potential of *POI-High*.

Or There are the following clues for the component of the POI being not resistant to attackers with an attack potential of *POI-High*:

Clue\_1: …

Clue\_2: …

…

Analysis:

The attack scenarios for which penetration testing was performed are identified in the work unit AVA\_POI.1-6 (remark ‘penetration testing is necessary for determination’).

Based on this list and on the results of the penetration tests the following table was created during the analysis:

|  |  |  |  |
| --- | --- | --- | --- |
| Attack scenario  (see AVA\_POI.1-6) | Penetration test related  (see AVA\_POI.1-9) | Attack potential of the current attack scenario, points according to CEM, B.4 | Any SFR has not been met?  (if the AS was not successful, then ‘no’; if the AS was successful, then list of SFRs having not been met) |
| AS.1 | ET.1 | Elapsed time = value = points explanation for the value assigned, if necessary  Expertise = value = points explanation for the value assigned, if necessary  component of the POI Knowledge = value = points explanation for the value assigned, if necessary  Opportunity = value = points explanation for the value assigned, if necessary  Equipment = value = points explanation for the value assigned, if necessary  Sum: points | no  Or list of SFRs violated |
| … | … | … | … |

Table 9: Attack scenarios covered by the penetration testing

Or only add reference to the table in the Attack methods document performed by the evaluator

Assessment and Verdict:

Using the table above the evaluator comes to the following conclusion:

No attack scenarios were successful in the components of the POI’s operational environment.

Or The attack scenario AS… was successful because the SFR .. was not met while applying this scenario. Nevertheless, the Add component of the POI security policy was not undermined by this attack scenario due to the fact that the related attack potential (… points) is bigger *than equal or higher than* Add potential, cf. [POI CEM]. Hence, this does not contradict the assurance component AVA\_POI.1; thus, the TSP is not undermined by this attack scenario. The vulnerabilities related to AS… are to treat as residual vulnerabilities (VUL\_RSD.n): they will be reported as required by AVA\_POI.1-12.

Add other

Since there is no attack scenario undermining the TSP, the evaluator decided that the Add component of the POI, in its operational environment, is resistant to an attacker possessing a Add potential. It means that there are no exploitable vulnerabilities (VUL\_E). Hence, this work unit is **fulfilled** (pass).

Or Since there is at least one attack scenario undermining the TSP, the evaluator decided that the Add component of the POI, in its operational environment, is not resistant to an attacker possessing *an equal or higher* Add potential attack potential. It means that there is at least one exploitable vulnerability. Hence, this work unit is **not fulfilled** (fail).

**[AVA\_POI.1-12]** The evaluator ***shall report*** in the ETR all exploitable vulnerabilities and residual vulnerabilities, […].

The current work unit deals with reporting all exploitable vulnerabilities and residual vulnerabilities found.

Summary:

Add summary

Analysis:

Based on the results of the previous work unit and of the work unit AVA\_POI.1-6, the evaluator created the ‘Vulnerabilities Report’ above.

Having performed the vulnerability analysis, the evaluator determined that the components of the POI are free of exploitable vulnerabilities.

Or Having performed the vulnerability analysis, the evaluator determined that the POI has the following exploitable vulnerabilities:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Attack scenario applicable to the component of the POI in its operational environment | Short description of the attack scenario | Exploitable vulnerabilities might be exploited by the attack scenario | Theoretically estimated or tested minimal attack potential needed for performing this AS, cf. [POI CEM] | Source |
| AS…. | … | - VUL\_E.1  - VUL\_E.2  - VUL\_E.3 | Elapsed time = value = points explanation for the value assigned, if necessary  Expertise = value = points explanation for the value assigned, if necessary  component of the POI Knowledge = value = points explanation for the value assigned, if necessary  Opportunity = value = points explanation for the value assigned, if necessary  Equipment = value = points explanation for the value assigned, if necessary  Sum: points | … |
| … | … | … | … | … |

Table 10: Exploitable vulnerabilities

Residual vulnerabilities result from the theoretical analysis and the penetration testing of the attack scenarios devised.

Having performed the vulnerability analysis, the evaluator determined that the components of the POI are free of residual vulnerabilities.

Or Having performed the vulnerability analysis, the evaluator determined that there are following residual vulnerabilities:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Attack scenario applicable to the component of the POI in its operational environment | Short description of the attack scenario | Residual vulnerabilities might be exploited by the attack scenario | Theoretically estimated or tested minimal attack potential needed for performing this AS, cf. [POT CEM] | Source |
| AS…. | … | - VUL\_RSD.1  - VUL\_RSD.2  - VUL\_RSD.3 | Elapsed time = value = points explanation for the value assigned, if necessary  Expertise = value = points explanation for the value assigned, if necessary  component of the POI Knowledge = value = points explanation for the value assigned, if necessary  Opportunity = value = points explanation for the value assigned, if necessary  Equipment = value = points explanation for the value assigned, if necessary  Sum: points | … |
| … | … | … | … | … |

Table 11: Residual vulnerabilities

Assessment and Verdict:

The evaluator confirms (or disproves) that he was able to report all exploitable and residual vulnerabilities for the ETR.

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

**Verdict for AVA\_POI.1.4E:**  
**##PASS ##FAIL ##INCONCLUSIVE**   
The evaluator confirms (##or disproves) (##or 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 being additionally to them having already been treated in the current evaluation report above.

## Missing Information

Add, if applicable, further information, which the developer/sponsor has to provide.

## Questions to / Conditions on the Developer

Add, if applicable questions, recommendations to or conditions on the developer.

## Necessary Changes/Improvements

Add, if applicable, changes which should be done by the developer.

## Effects on other Documents

Add, if applicable, effects on other documents.

# Annex

## Glossary and list of acronyms

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

|  |  |  |
| --- | --- | --- |
| abbreviation | term | definition / explanation |
| ST | Security Target | … |
| … | … | … |
|  |  |  |

## Bibliography

Criteria and Methodology

[CC1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, Sept 2012, Version 3.1, Revision 4, CCMB-2012-09-001

[CC2] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, Sept 2012, Version 3.1, Revision 4, CCMB-2012-09-002

[CC3] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, Sept 2012, Version 3.1, Revision 4, CCMB-2012-09-003

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation methodology, Sept 2012, Version 3.1, Revision 4, CCMB-2012-09-004

Legislatives and Standards

Add reference or none

Evaluation Reports

Add reference

Developer Documents

Add reference

[ATECOV] Developer test coverage..

…

Other documents

[POI CEM] Joint Interpretation Library – CEM Refinements for POI Evaluation, Version 1.0, 27th May 2011. *Note: POI evaluations shall rely on the current version of this document at the moment of the evaluation.*

[POI AttackPot] Joint Interpretation Library / Application of Attack Potential to POIs, Version 1.92, 11th August 2014. *Note: POI evaluations shall rely on the current version of this document at the moment of the evaluation.*

[POI AttackMeth] Joint Interpretation Library / Attack Methods for POIs, Version 1.94, February 2015. *Note: POI evaluations shall rely on the current version of this document at the moment of the evaluation.*

Add reference