| | | | |
|---|---|---|---|
| **Item Title** | Supporting document ND – Evaluation Activities for Network Device cPP -V0.3 | **Reviewer** | *German Scheme (BSI Germany)* |
| **Item Identifier** | *ND-SD* | **Review Date** | 2014-11-28 |
| **Version; Date:** | *0.3; 2014-10* | | |

**Notes :-**

| | | |
|---|---|---|
| Severity | 1 | **Significant** - Conflicts with current CC/CEM/CCRA. Needs a substantial change in the meaning of the document or a related CC/CEM change request and rationale to CCDB/MC |
| | 2 | **Moderate** - Normally clarifications or proposed improvements to the compliance with CC/CEM/CCRA - unlikely to impact other areas. |
| | 3 | **Minor** - Does not affect the correct operation or interpretation of the item. These are usually syntax and format errors which have no effect on the meaning or interpretation of the item. |

*This is a public commenting process: the text of comments and responses may be distributed, or made available in other ways, without restriction during the process.*

| No. | Location | Comment | Suggested Change | Severity | Action |
|---|---|---|---|---|---|

| No. | Location | Comment | Suggested Change | Severity | Action |
|---|---|---|---|---|---|
| **1.** | *ND-SD* | The relation between the Evaluation Activities and the CEM is unclear.<br>Following statements were found:<br>Foreword: "This is a supporting document, intended to complement the Common Criteria version 3 and the associated Common Evaluation Methodology for Information Technology Security Evaluation."<br>Chapter 1.2 Structure of the Document: "In general, if all Evaluation Activities (for both SFRs and SARs) are successfully completed in an evaluation then it would be expected that the overall verdict for the evaluation is a 'pass'."<br>According to the new CCRA the CC and the CEM are still mandatory documents for the evaluation and all requirements in those documents have to be fulfilled.<br>In accordance with the CEM paragraph 57, the evaluator shall assign 'pass' verdict if and only if all of the constituent work units are satisfied.<br>Without a direct relation between evaluation activities and work units the evaluator has a difficulty to assigns pass/fail verdict. | Provide a clear statement that all CEM work units according the assurance families chosen in the cPP have to be fulfilled and that the evaluation activities from the SD are refinements for certain work units.<br><br>For each evaluation activity (for SFRs and SARs) there has to be a reference to a certain work unit in order to enable the evaluator to assign a pass/fail verdict. | Significant | An updated Supporting Document template has been created to address this comment. The intent is that the new SD template will be populated and will replace the existing SD for the Firewall. The updated template states that the evaluator performs the CEM work units associated with ASE, ALC_CMC.1, ALC_CMS.1, AGD_OPE.1, AGD_PRE.1, and ATE_IND.1. For the ADV_FSP.1 component, the SD template supplements the CEM work units – called Evaluation Activities (EAs) – to capture the intent of the work units. A mapping of work units to EAs is included in the template and is presented at the end of this table for the reader's convenience. |

| No. | Location | Comment | Suggested Change | Severity | Action |
|---|---|---|---|---|---|
| **2.** | Chapter 3.5 | "For each vulnerability found, the evaluator either provides a rationale with respect to its non-applicability, or the evaluator formulates a test (using the guidelines provided for ATE_IND) to confirm the vulnerability, if suitable."<br>The meaning of "if suitable" is unclear.<br>From point of view of the German scheme each vulnerability has to be resolved (either by rationale or test). | Delete or explain the limitation "if suitable". | Significant | Agreed that each vulnerability has to be resolved. The "if suitable" was meant to address the testing aspect. If a test was too onerous or couldn't be carried out reliably, then the developer may be able to address it through analysis and some form of a rationale. |

| No. | Location | Comment | Suggested Change | Severity | Action |
|---|---|---|---|---|---|
| **3.** | Chapter 2 | The evaluation activities for some of the crypto related SFRs are not sufficient. | Provide more detailed evaluation activities, preferably agreed in the CCDB cryptoWG. | Significant | Yes, we look forward to hearing from the CCDB Crypto WG for direction in this area. We want to be consistent as to what is being done across technologies where appropriate. However, there has not yet been any output in the area of evaluation activities from the Crypto WG. Therefore, until the Crypto WG publishes definitive guidance, the iTC considers the evaluation activities to be sufficient.. When the Crypto WG publishes evaluation activities, they will be incorporated in the next version of the SD. |

The following table comes from the new SD template and shows how the ADV_FSP.1 work units are covered by the Evaluation Activities.

| CEM ADV_FSP.1 Work Units | Evaluation Activities |
|---|---|
| ADV_FSP.1-1 The evaluator ***shall examine*** the functional specification to determine that it states the purpose of each SFR-supporting and SFR-enforcing TSFI. | 5.2.1.1 Evaluation Activity: *The evaluator shall examine the interface documentation to ensure it describes the purpose and method of use for each TSFI that is identified as being security relevant.* |
| ADV_FSP.1-2 The evaluator ***shall examine*** the functional specification to determine that the method of use for each SFR-supporting and SFR-enforcing TSFI is given. | 5.2.1.2 Evaluation Activity: *The evaluator shall examine the interface documentation to ensure it describes the purpose and method of use for each TSFI that is identified as being security relevant.* |
| ADV_FSP.1-3 The evaluator ***shall examine*** the presentation of the TSFI to determine that it identifies all parameters associated with each SFR-enforcing and SFR supporting TSFI. | 5.2.1.3 Evaluation Activity: *The evaluator shall check the interface documentation to ensure it identifies and describes the parameters for each TSFI that is identified as being security relevant.* |
| ADV_FSP.1-4 The evaluator ***shall examine*** the rationale provided by the developer for the implicit categorisation of interfaces as SFR-non-interfering to determine that it is accurate. | Paragraph 561 from the CEM: "In the case where the developer has provided adequate documentation to perform the analysis called for by the rest of the work units for this component without explicitly identifying SFR-enforcing and SFR-supporting interfaces, this work unit should |

| | |
|---|---|
| | be considered satisfied."<br>Since the rest of the ADV_FSP.1 work units will have been satisfied upon completion of the EAs, it follows that this work unit is satisfied as well. |
| ADV_FSP.1-5 The evaluator ***shall check*** that the tracing links the SFRs to the corresponding TSFIs. | 5.2.1.4 Evaluation Activity: *The evaluator shall examine the interface documentation to develop a mapping of the interfaces to SFRs.* |
| ADV_FSP.1-6 The evaluator ***shall examine*** the functional specification to determine that it is a complete instantiation of the SFRs. | EAs that are associated with the SFRs in Section **Error! Reference source not found.**, and, if applicable, Sections **Error! Reference source not found.** and **Error! Reference source not found.**, are performed to ensure that all the SFRs where the security functionality is externally visible (i.e., at the TSFI) are covered. Therefore, the intent of this work unit is covered. |
| ADV_FSP.1-7 The evaluator ***shall examine*** the functional specification to determine that it is an accurate instantiation of the SFRs. | EAs that are associated with the SFRs in Section **Error! Reference source not found.**, and, if applicable, Sections **Error! Reference source not found.** and **Error! Reference source not found.**, are performed to ensure that all the SFRs where the security functionality is externally visible (i.e., at the TSFI) are addressed, and that the description of the interfaces is accurate with respect to the specification captured in the SFRs. Therefore, the intent of this work unit is |

| | |
|---|---|
| | covered. |