Item Title	Supporting document FDE – Encryption Engine-V0 11	**Reviewer**	*German Scheme (BSI Germany)*
Item Identifier	*FDE-SD-EE*	**Review Date**	2014-11-28
Version; Date:	*0.11; 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.	FDE-SD	The relation between the Evaluation Activities and the CEM is unclear. Following statements were found: 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.” 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’.” 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. 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. 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. 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	Please see text below.

No.	Location	Comment	Suggested Change	Severity	Action
2.	Chapter 3	The role of this chapter is unclear. For some CC/CEM aspects there equivalent requirements defined (ALC_CMC.1), for some aspects there seem to be less requirements defined (ALC_CMS.1 – no configuration list needed), for some aspects refined requirements are defined (e.g. ADV, AGD, ATE) and for ASE there is no statement (cf. NDPP-SD)).	Clarify the relevance of the evaluation activities and provide a clear statement that CC/CEM are still the basis for each evaluation (see comment 1).	Significant	This chapter is intended to describe the activities the evaluator is expected to perform to determine if the applicable SARs are satisfied. The activities contained here are intended to "interpret" the activities that would be captured in the CEM work units. The cPP states for the Security Target, the CEM work units are to be applied, so there are no interpreted activities contained in the SD. For ALC, you are correct, we have modified the documents so that the evaluator simply performs the CEM work units. After thinking more about it, the ALC requirements used in the cPP do not have any technology specific aspects. The intent is that the AGD_OPE and AGD_PRE satisfy the requirements levied by ADV_FSP (see explanation for comment 1). What this section attempts to do for the AGD and ATE requirements is provide evaluation activities that are not associated with an SFR. Chapter 2 states what the evaluator is supposed to do in the context of AGD and ATE for each applicable SFR. Chapter 3 describes the overarching activities – e.g., prepare a test plan, test report - which the evaluator performs. While these are not necessarily technology dependent (that is really covered in Chapter 2), we wanted to avoid picking out certain work units. While that is done conceptually, we don't carry the numbers and specific wording.

No.	Location	Comment	Suggested Change	Severity	Action
3.	Chapter 3.5, Appendix A	The descriptions seem to be incomplete especially with regard to the "[VAWP] Draft vulnerability whitepaper" (cf NDPP_SD). The explanations concerning the "narrow usecase" and "normal types of testing" in Appendix A are not traceable.	Provide instructions for conducting a vulnerability assessment according to the [VAWP] (not only for the inclusion of newly found vulnerabilities in a future version of the cPP/SD but also for the real doing in an evaluation).	Significant	The iTC adhered to the spirit of the VAWP. The iTC focused on what vulnerability analysis made sense give the technology type and use case. The iTC does not understand what is meant by "not traceable". We agree that "normal types of testing" may be an unclear choice of words and we will be more specific in future versions of the cPP. The premise of the threat model is that an attacker only has the ability to attack the interface that is presented by the encrypted drive. CVEs for this technology do not currently exist for our use case. If any CVEs do appear that apply to our operational scenarios, we will construct assurance activities and submit them as part of the SD to the CMDB for approval.
4.	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." The meaning of "if suitable" is unclear. 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	You are correct, that there must be some resolution to any identified potential vulnerability. How the potential vulnerability is resolved will rest with the Scheme performing oversight. Testing in most cases will not be effective or appropriate, in that case the developer should offer other evidence to make the case to the evaluator that the flaw was sufficiently remedied.

No.	Location	Comment	Suggested Change	Severity	Action
5.	Chapter 2	The evaluation activities for most of the crypto related SFRs are not sufficient. E.g.: • FCS_CKM.4/FCS_CMK_EXT.4 Do you think that it is really possible to delete the DEK for each and every type of drive? What about SSDs? • FDP_DSK_EXT.1 The evaluation of the TSFI for requesting the crypto services from the environment seems to be incomplete. General Note: According the title of the cPP it is very strange and new for the German scheme that the main functionality "encryption" can be shifted to the environment of the TOE. • FPT_TUD_EXT.1 The whole description of this mechanism in the cPP and the respective evaluation activities in the SD are unclear. What about downgrade to old, possibly insecure versions? What about incremental or full updates? What is the scope of the signature e.g. is the version number part of the signature? • FCS_RBG_EXT.1	Provide more detailed evaluation activities, preferably agreed in the CCDB cryptoWG.	Significant	As far as the description for the FCS requirements, the intent was to cover what is currently done as part of a NIST CAVP validation. The iTC would welcome any direction from the CCDB Crypto WG. As for the examples contained within the comment: • FCS_CKM.4/FCS_CMK_EXT.4- yes, the DEK is "eraseable or can be deleted in SSDs". There was some detailed discussion on how keys are stored in such devices and what one might have to do to confirm all instances of the DEK have been removed, but at this time it was felt the activity was adequate for now, and the iTC will continue to explore what methods might be used to provide a higher degree of assurance that the DEK has been completely removed. • FDP_DSK_EXT.1 – Understand the commenter's position. While the implementation of cryptography can be provided by an underlying platform, the TOE must ensure that no data are stored on the device without first being encrypted. Obviously, it is a tougher argument to make if the OS is providing the cryptographic services rather than the drive itself. This is really necessary to support some of the software only products that don't do the actual encryption themselves. The iTC believes as long as it is clear to end-users where the encryption takes place, the user can determine if that is a solution that is suitable for their use-case. • FPT_TUD_EXT.1 – discussed downgrading to an older version and it was decided at this time, it would not be prevented – sometimes operationally one may need to fall back due to new version breaking something. • FCS_RBG_EXT.1 – need more direction from CCDB WG on this one.

Comment #1 Response:

We thank you for your comment, it has caused us to re-evaluate the Evaluation Activities we have specified. While we felt some activities were implicitly covered, in some instances it is better to make it explicit to ensure certain activities are fully performed.

We have a different view on what paragraph 57 of the CEM states. The referenced paragraph contains the following text: “The overall verdict is pass if and only if all the constituent verdicts are also pass. In the example illustrated in Figure 3, if the verdict for one evaluator action element is fail then the verdicts for the corresponding assurance component, assurance class, and overall verdict are also fail.” In our opinion, this paragraph is not describing verdicts of work units, rather it is discussing Evaluator Action elements, which are CC requirements designated with the E suffix. In essence, the CEM is an interpretation of the E elements contained within the CC Security Assurance Requirements. What we are attempting to do, is to interpret those E elements on a technology specific basis where it makes sense. There are cases where the technology being evaluated makes no difference in the evaluation activities, and in those instances, we attempt to rely on the agreed upon CEM work units.

ASE

For instance, the ST evaluation is not technology dependent, and we require that the CEM work units be applied when evaluating the ST. So the updated version of the Supporting document makes it clear that the CEM work units associated with the ST evaluation are to be applied. In addition, the evaluation activities were added for the elements for determining exact conformance (ASE_CCL.1.8C, ASE_CCL.1.9C, and ASE_CCL.1.10C).If the evaluator cannot perform an pass verdict for each EA defined in the SD, as well as the Evaluator Action elements

ALC

For the ALC SARs, the evaluator is instructed to perform the CEM work units associated with the applicable Evaluator Actions.

ADV_FSP

For the ADV_FSP SAR, two new Evaluator Activities were added to address CEM work units that while we believe were implicitly covered (e.g., one cannot perform the required analysis unless the necessary information is present), were not explicitly covered:

- The evaluator shall check the interface documentation to ensure it describes the purpose and method of use for each TSFI that is identified as being security relevant.
- 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.

We believe these map to the CEM Work Units ADV_FSP.1-1, ADV_FSP.1-2, and ADV_FSP.1-3. The only difference being we are not requiring the developer to categorize interfaces as SFR-enforcing or SFR-supporting. In our view, since Section 2 of the Supporting Document requires the evaluator to examine the interface documentation in the context of an SFR, the evaluator by definition, albeit implicit, is determining the interfaces that are relevant to the SFRs. The work unit 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.” is not addressed by our Evaluation Activities, as we feel this categorization provides no value. As stated, the SFR-enforcing and SFR-supporting interfaces are implicitly understood by the evaluator. SFR-non-interfering interfaces, by definition, have no bearing on compliance with an SFR, and the only place they might be considered would be during the vulnerability analysis activity, which is described elsewhere.

The work units ADV_FSP.1-5 “The evaluator shall check that the tracing links the SFRs to the corresponding TSFIs” and ADV_FSP.1-6 “The evaluator shall examine the functional specification to determine that it is a complete instantiation of the SFRs.”, we believe are covered implicitly, since the Evaluator Activities require the evaluator to examine the interfaces in the context of a given SFR.

We believe the work unit ADV_FSP.1-7 “The evaluator shall examine the functional specification to determine that it is an accurate instantiation of the SFRs.” Is covered by the Evaluation Activities, since the evaluator is instructed to perform the action in the context of a given SFR and how it applies to the technology at hand.

AGD_OPE

For the operation guidance, the Evaluator Activities (EAs) in Section 2 of the Supporting Document describe what the evaluator checks in the context of the technology and the applicable SFR – e.g., making sure that for the security function being required by the SFR, that the administrative guidance is clear in how to configure/manage the TOE.

So for the work unit 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 TOE does not currently specify the notion of roles, So the EAs for applicable SFRs require the guidance documentation to describe the functions that are configurable and any warnings that are appropriate. Work unit 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.” is addressed, where applicable by the EAs associated with appropriate SFRs. Work units 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.”, 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.” and 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." are also covered by the EA under the appropriate SFRs. In this instance, the users are the administrators – i.e., there are no untrusted user roles.

We believe work unit 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." is covered within the EAs per SFRs (Section 2) and the EA contained within AGD_OPE.1 in Section 3.

Finally, we believe the work units AGD_OPE.1-7 "The evaluator ***shall examine*** the operational user guidance to determine that it is clear." and AGD_OPE.1-8 "The evaluator shall examine the operational user guidance to determine that it is reasonable." are addressed implicitly - i.e., the evaluator would not be able to perform the EAs unless the guidance was clear and reasonable.

AGD_PRE

This SAR is interesting, since it appears to levy requirements that are captured in another SAR – ALC_DEL. Currently the EAs in the SD do not require the evaluator to examine the delivery procedures as specified by AGD_PRE.1-1 "The evaluator shall check that the procedures necessary for the secure acceptance of the delivered TOE have been provided." and AGD_PRE.1-2 "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." We believe these work units are misplaced and if ALC_DEL is required, then the PP author should include that SAR.

We do believe the work units AGD_PRE.1-3 "The evaluator shall check that the procedures necessary for the secure installation of the TOE have been provided.", AGD_PRE.1-4 "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." and AGD_PRE.1-5 "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 user guidance." are cover by the EA specified in the AGD_PRE SAR in Section 3.

ATE_IND

EAs were added to the SD to cover the work units ATE_IND.1-1 "The evaluator shall examine the TOE to determine that the test configuration is consistent with the configuration under evaluation as specified in the ST." and ATE_IND.1-2 "The evaluator shall examine the TOE to determine that it has been installed properly and is in a known state.".

We believe work units ATE_IND.1-3 “The evaluator shall devise a test subset.”, ATE_IND.1-5 “The evaluator shall conduct testing.” and ATE_IND.1-7 “The evaluator shall check that all actual test results are consistent with the expected test results.” are covered by test activities the evaluator is to perform as part of the EAs in Section 2.

Work unit ATE_IND.1-4 “The evaluator shall produce test documentation for the test subset that is sufficiently detailed to enable the tests to be reproducible.” ATE_IND.1-6 “The evaluator shall record the following information about the tests that compose the test subset: …” and ATE_IND.1-8 “The evaluator shall report in the ETR the evaluator testing effort, outlining the testing approach, configuration, depth and results.” are covered by the EA specified in Section 3 under ATE_IND.

AVA_VAN

Appendix A of the AA SD indicates the sources for vulnerability information, based on the use cases defined in the cPP. There is a process defined for proposing new vulnerability analysis activities that involves collaboration with the international Technical Community. We anticipate vulnerability analysis activities will evolve as the PP is applied during evaluations and as the iTC updates the PP to broaden the use case.