Item Title	Supporting document FDE - Authorization Acquistion-V0 13	**Reviewer**	*Eunkyoung Yi*
Item Identifier	*FDE-SD-AA*	**Review Date**	*2014-11-27*
Version; Date:	*0.13; 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
1.	<SD> 2. Evaluation Activities for SFRs	Based upon SARs defined in the related cPP, we consider all evaluation activities for SFRs are interpretations to the CEM because there is no extended SAR in the cPP. It is obvious that the SD can provide interpretations to the CEM in accordance with the baseline requirements defined in the Vision Statement. In accordance with the CEM section	We suggest that all of the proposed evaluation activities for SFRs need to be referenced using related work units in the CEM so that the evaluator applies them to his/her pass/fail verdict decision.	moderate	*Please see the text below for how the iTC believes the CEM is being addressed.*

No.	Location	Comment	Suggested Change	Severity	Action
		8.2.5, the evaluator assigns verdicts to every evaluator action element, assurance component, and assurance class. Also, 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. The proposed evaluation activities for the SFRs are mandatory because they are using auxiliary verb 'shall', but there is no reference to the origin work unit which can be examined or checked together with. This will lead to a situation that the evaluator has a difficulty to assigns pass/fail verdict.			
2.	<SD> 2. Evaluation Activities for SFRs	To apply evaluation activities for SFRs, first of all the evaluator needs evaluation deliverables provided by the sponsor or developer. And the sponsor or developer provides their evaluation deliverables based upon SARs claimed for the evaluation. In the related cPP, SARs from EAL1 are claimed. It is unclear that the necessary evaluation deliverables for the proposed evaluation activities for SFRs are consistent with Developer Action Elements and Content & Presentation of Evidence Elements for each SARs	We suggest that all of the proposed evaluation activities for SFRs need to be referenced using related work units in the CEM so that the sponsor or developer determines they are consistent with SARs claimed.	moderate	*Please see the text below for how the iTC believes the CEM is being addressed.*

No.	Location	Comment	Suggested Change	Severity	Action
		claimed in the cPP.			
3.	<cPP> 2. CC Conformance	The current version of the CC/CEM doesn't provide 'Exact Compliance' as subset of strict conformance.	The CCMB is now under reviewing process to incorporate 'Exact conformance' into the CC/CEM, so we expect that this comment will be resolved sooner or later.	Significant	*We added the elements for determining exact conformance to the SD.*

Comment 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.