CCDB Work Group for USB Portable Storage Devices

DOC. TYPE: Disposition of comments

TITLE: Disposition of comments on 'Establishing International Technical Communities and collaborative Protection Profiles development', v0.4, 130221

SOURCE: Responders to publication of initial public draft v0.4

DATE: 2013-12-13

STATUS: Responses from CCDB USB cPP Working Group. These responses describe actions taken in internal drafts, and these are published in order to capture the intended nature of responses, However, a substantial rewrite of the paper is about to be undertaken following other discussions in the expanded Working Group, and this document describes the responses *prior* to that rewrite. The intention of these responses is expected to be preserved in the rewrite, but the detail may differ.

           This document is an output of the CCDB USB cPP WG. It does not represent the formal position of any of the CCRA Committees.

DISTRIBUTION: Public

NO. OF PAGES: 31

Disposition of comments on 'Establishing International Technical Communities and collaborative Protection Profiles development', v0.4, 130221

Date: 2013-12-13

Document: 'Establishing International Technical Communities and collaborative Protection Profiles development', v0.4, 130221

1	2	(3)	4	5	(6)	(7)
NB[1]	Clause No./ Subclause No./ Annex)	Paragraph/ Figure/ Table/Note)	Type of com-ment[2]	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
FMV1	Purpose	Last sentence	S	Current text: "The CCDB will provide separate guidelines for the development of a ToR, including a ToR template, which will incorporate work performed by the Common Criteria Users Forum (CCUF" There is no formal task in accordance to above defined in the CCDB	Either send in a proposal to the CCDB to establish such a work item, or rephrase the text to something that can be regarded as accurate,	Accept (to be addressed outside the document in the WG workplan)
FMV2	Background	2nd but last para	S	Current text: "The document in the current form is a proposal from the CCDB USB cPP WG and does not represent the official position of the CCRA committees." WG agreed to extend the scope to also accommodate draft CCDB process.	This part must be updated. Doc now to be CCDB and USB process doc, edited by USB group. Still not feflecting formal view of CCRA at this stage.	Accept (to be addressed by creating both documents, ideally using one source and two 'views'; initiated at London workshop)
FMV3	Background	Last para	S	Current text: "The World Trade Organization (WTO) has faced and managed many challenges that are similar to those confronting the CCRA in the development of cPPs. Since the WTO model has proven successful in many of these areas, this document leverages their work and contains text that is based on text that originates from the WTO - Technical Barriers to Trade (TBT) Agreement web site."	WG agreed to move WTO stuff to other doc. But we should include the requirement on iTC that they should adhere to the six principles also in this doc, with a reference to the definition of these principles.here.	Accept (to be addressed by removing the WTO section and adding a summary of the 6 principles)
FMV4	Level of Committment	all	S	Current text use the term "Committed Nation". This is not a good term since it makes other believe that they have to commit in a very formal and "hard" way. That is not the intention.	Find another term. Perhaps "declared?" But that is not very good either.	Accept (we decided to use "Endorsing Nation", but have more recently removed this concept completely: a nation's stance is defined by its Position Statement & Endorsement Statement contents)
FMV5	Level of Committment	all	S	The current term "Committed Nation" may be actually be connected to the term CCDB "Contributing Nation, at least for the ESR part of the process.	WG need to discuss if we should make a relation in the process between the CCDB project model, and the "Committed" and "uncommitted nation" terms in the	Accept in principle (the existing sections on Committed Nations in the White Paper are to be updated as noted above). However, the iTC process is viewed as separate and no linkage is

[1] NB = Notifying Body – the organisation submitting the comment

[2] Type of comment: C = critical; S = substantial; A = administrative

Disposition of comments on 'Establishing International Technical Communities and collaborative Protection Profiles development', v0.4, 130221

Date: 2013-12-13

Document: 'Establishing International Technical Communities and collaborative Protection Profiles development', v0.4, 130221

1	2	(3)	4	5	(6)	(7)
NB[1]	Clause No./ Subclause No./ Annex)	Paragraph/ Figure/ Table/Note)	Type of com-ment[2]	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
					WP.	being made to the CCDB project model.
FMV6	Level of Committment xaa	Third para	S	Current text: "The description of how the commitment will be realized by the nation forms a part of its statement of commitment,…" We need to be more clear about the format and the content of a commitment statement	Add some more text about the intent, format and content of a commitment statement.	Accept (the existing sections on Committed Nations in the White Paper are to be updated as noted above; in particular there is now a separate section on Position Statements & Endorsement Statements).
FMV7	Block 1	all	S	Current text. "Sponsor". The use of the term Sponsor in the context of the process has by some been confused by the use of the same term in scope of certifications. The term lead many to believe that the sponsor is responsible for funding of resources. That is also misleading.	We should probably find another term or perhaps systematically use the term cPP sponsor.	Accept (we will use "initiator")
FMV8	Block 2/3	2nd para	A	Current text: "If a cPP does not exist, the CCDB consults the CCRA to gauge the community's interest in the development of such a cPP." What is meant by "community" in this sentence? I think it means any relevant stakeholder. But by using this word, it could be confused with the iTC itself.	Change word "community" to something else.	Accept (rewritten text just talks about consulting CCRA Participants)
FMV9	Block 2/3	2nd para	S	Current text: "If there is insufficient interest, the CCDB informs the Sponsor" What are the grounds for CCDB to deem there are "insufficient interest"? What is insufficient interest? Less than simple majority in CCDB? Or the MC? Should not two interested nations enough? Should two nations have to get the approval from the others to establish a cPP if they have a need, and there are no other cPP:s established in the area?	Adjust the text and make clear in what ground the CCDB can reject a proposal to establish a cPP/ESR/iTC	Accept (to be addressed outside the document in the CCDB Role Guidance)

[1] NB = Notifying Body – the organisation submitting the comment

[2] Type of comment: C = critical; S = substantial; A = administrative

1	2	(3)	4	5	(6)	(7)
NB[1]	Clause No./ Subclause No./ Annex)	Paragraph/ Figure/ Table/Note)	Type of com-ment[2]	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
				I think that the only reason for having to oblige for CCDB approval is if CCDB do not have resources to adminstrate the supporting documents that follows. But as soon as there are at least two contributing and committed nations, there should be no problem to move ahead?		
FMV10	Block 5	First para, all	S	Current text: "The creation of the ESR is the primary role of the WG" I think the WG also should do the work to establish the iTC, but ensuring that CCRA DB and MC is invited to participate in the process	Update the WP accordingly.	Accept.
FMV11	Block 5		S	Current text: "However, it should be expected that for many technical domains, one or several other governmental authorities from the CCRA participant may need to be involved in the work to establish such harmonized security requirements." Should be made clearer that we really understand that also other gov entities need to be involved.	Change sentence to: "However, it should be expected that for many technical domains, one or several other governmental authoritiesfrom the CCRA participant, than those represented within the CCRA, may need to be involved in the work to establish such harmonized security requirements." "than those represented in tje CCRA committees."	Accept in principle
FMV12	Block 6/7/8	first para, all	S	Current text: "Here the WG distributes the draft ESR to the CCRA members to solicit comments" We need to clarify the status of the ESR. The ESR should be a public document. The WG will look for comments and deal with comments from CCRA members (and their various agencys). The WG should accommodate for such comments to try to reach broad agreement. But other may also comment (like vendors or other	Update the text to clarify that the ESR is a public document. The WG will work with comments from CCRA members to seek consensus, and may at its own discretion also accommodate for comments received from others.	Accept in principle (important not to commit to *respond* to all comments from non-CCRA Participants – responding to all could undermine realistic timescales)

[1] NB = Notifying Body – the organisation submitting the comment
[2] Type of comment: C = critical; S = substantial; A = administrative

Date: 2013-12-13	Document: 'Establishing International Technical Communities and collaborative Protection Profiles development', v0.4, 130221

1	2	(3)	4	5	(6)	(7)
NB[1]	Clause No./ Subclause No./ Annex)	Paragraph/ Figure/ Table/Note)	Type of com-ment[2]	Comment (justification for change) by the NB	Proposed change by the NB	Resolution[1] on each comment
				stakeholder) and such comments may be accommodated for too, if the WG find them relevant.		
FMV13	Block 9/10/11	First para,all	S	The responsibility to establish the iTC need to be refined. The only *formal* role the CCDB will have, is to liaise with the iTC and (together with the MC) approve the ToR. The iTC should be able to be established by any entity and the establishment of an iTC should not have to be on the initative of the CCDB. It *could* be established on initative of the CCDB, but also by others. It is of course strongly advisable, that any party that enters the process to establish an itC, should inform the CCDB of such activites.	Update the text in the whole doc accordingly.	Accept in principle (WG has agreed that the WG itself will be the one to initiate contact with the iTC)
FMV14	Block 9/10/11	First para	S	Current text: "a TC may exist and is willing and able to take on the responsibility of creating a cPP and operating under the constraints levied by the CCRA and [Vision]" This text is saying that the iTC operating under some kind of authority of the CCRA and need to follow its directions. It also say that the cPP is made by the iTC as a task assigned by the CCRA. This should nuanced. The iTC is an independent group that is selfsuffiecient and establish a liaison with the CCRA.The liaison is established between two "equals". The iTC is not "assigned the task" to establish the cPP. Rather, the iTC volonters to write the cPP that meets the requested needs stated in the ESR.	Change the wording and provide a better description of the relation between the CCRA and the iTC.	Accept in principle (will add explanation that the iTC is *endorsed* by the MC; it may then be more appropriate to describe the iTC as working under the constraints of the documented process (and related CCDB/MC Operating procedures) except where separately agreed as part of its approval by CCDB and endorsement by MC)
FMV15	Block 9/10/11	First para,	A	Current text: "In this case the CCDB may agree with the existing iTC that it will take on responsibility for the new cPP (which)" Similar as above. The text should rather say "the CCDB	Update text.	Accept in principle

[1] NB = Notifying Body – the organisation submitting the comment

[2] Type of comment: C = critical; S = substantial; A = administrative

Disposition of comments on 'Establishing International Technical Communities and collaborative Protection Profiles development', v0.4, 130221

Date: 2013-12-13

Document: 'Establishing International Technical Communities and collaborative Protection Profiles development', v0.4, 130221

1	2	(3)	4	5	(6)	(7)
NB[1]	Clause No./ Subclause No./ Annex)	Paragraph/ Figure/ Table/Note)	Type of com- ment[2]	Comment (justification for change) by the NB	Proposed change by the NB	Resolution[1] on each comment
				may liaise with an already existing iTC who volenteers to develop an cPP that meets an ESR.		
FMV16	Block 9/10/11	2nd para	S	Current text: "It is envisioned that Committed Nations would participate in the iTC at some level, and potential iTC participants from the relevant technology domain would be solicited for participation by CCRA members and other recognized groups such as the CCUF." What is a recognized group? How and by whom are they recognized on what grounds?	Either explain the word recognized, or change or remove this word.	Accept (remove "recognized")
FMV17	Block 12	First sentence	S	Current text "When the iTC initial membership has been constituted, then a ToR template (see [ToR Temp]) This is what we have been calling the "interim group" in the WG.	Consider to use the term "interim iTC group" or something like that, to be consistent with the term we use in the WG.	Accept in principle (but latest rewrite still uses the term initial membership, subject to ongoing discussion of any better term to use here)
FMV18	Block 12	Whole section	S	In the WG we now have some more detailed understanding of what needs to be considered when the interim group is being approached and established, what their task would be, and what their obligations and limitations should be. We should add that text into the WG	Add relevant part of WG meeting agenda and meeting notes about how the interim group is being setup.B	Accept in Principle (action/update to be decided later based on how much there is to say about this, and whether it will unbalance the paper or delay production of the next version. A separate document for this (or later update to USB-specific text in the paper) may be considered.)
FMV19	Block 12	First para	S	Current text: "The only explicit constraint levied by the CCRA on the iTC is that it encourages fair and open competition, and otherwise supports [Vision]." We should point to the six principles	Add text (with a reference) to the WTO TBT six principles.	Accept (put in a single discussion of the 6 principles)
FMV20	Block 13		S	Current text: "Once the iTC is formally created the CCDB	Update text accordingly.	Accept (Public review now included in

1	2	(3)	4	5	(6)	(7)
NB[1]	Clause No./ Subclause No./ Annex)	Paragraph/ Figure/ Table/Note)	Type of com-ment[2]	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
				passes to it the ESR .. " The ESR should be made available to the iTC, vendors and others before that. This is necessary to ensure that we give all stakeholders on the market access to the same information at the same time.		block 6/7/8)
FMV21	Block 13		S	Current text: "and any additional constraints the CCDB feels are necessary. These constraints may further limit the scope in ways that the ESR did not consider, based on the CCDB's broader view of on-going activities. An example might be where an ESR is provided for a firewall application-level proxy; the CCDB might convey to the iTC that virus scanning of incoming traffic is outside the scope, since that is included in another iTC's charter." This whole section is problematic in my view for all sorts of reasons. The CCDB should probably not overrule or interpret the request on the content on the cPP the Committed Nations are doing in the ESR. The only comment I would recon that the CCDB does in this context is to recommend the iTC to consider to use certain supporting documents, or other aspects in relation to CC, CEM, Supporting document and/or the vision statement (latter to be replaced by reference to new CCRA).	Update the role of the CCDB to not intervene in the ESR. That belongs to the Committed Nations.	Reject (Will make sure it is clear that CCDB performs a review to ensure no overlapping domains/requirements. The example clarifies why it is important that in a few cases the CCDB might need to intervene)
FMV22	Block 13		S	Current text: "levels of commitment from CCRA nations" Clarify that this comes with the commitment statements.	New text: "levels of commitment from CCRA nations, with accompanied commitment statements."	Accept (included in changes above)
FMV23	Block 13		S	Current text:"Changes to the CC portal entry for an iTC will be reviewed by the Liaison CCRA Participant, as well as CCDB to ensure the [Vision] is being maintained."	Update in accordance with comment.	Accept

[1] NB = Notifying Body – the organisation submitting the comment

[2] Type of comment: C = critical; S = substantial; A = administrative

Date: 2013-12-13	Document: 'Establishing International Technical Communities and collaborative Protection Profiles development', v0.4, 130221

1	2	(3)	4	5	(6)	(7)
NB[1]	Clause No./ Subclause No./ Annex)	Paragraph/ Figure/ Table/Note)	Type of com-ment[2]	Comment (justification for change) by the NB	Proposed change by the NB	Resolution[1] on each comment
				I think rather that it is the liaison CCRA participant that ask the CCRA portal admin direcrly for the changes in the portal, and that the CCDB oversee this.		
FMV24	Block 13		S	Current text: "with the exception that the supporting documents must be approved by the CCDB." This is as we have agreed. How can it be avoided that supprting docs are not approved by the CCDB in the end? We need to avoid suprises for the iTC. It would be veeery bad if the whole time schedule of getting the cPP and supporting documents finalized by late negative feedback from the CCDB.	We need to develop some mechanism that avoid that the	Accept in principle (have made a note that the workplan needs to include an appropriate approach to oversight/review of SD development as agreed with the CCDB chair. The iTC/cPP process document is likely to address only cases where full visibility of the cPP/SD development is available: further updates may be needed in future if a less visible situation arises)
FMV25	Block 14		S	Current text: "Assurance Requirements (SARs) that are contained in the cPP template (see [cPP Temp])." There is no such doc in the workplan or the AI-list. This needd to be put into the WG workplan, AI-list or be removed. This kind of guidance is needed. But it need to be coordinated with other guidance on how to write PPs that is already established. Maybe this guide should be yet another Supporting Document?	WG need to agree in what form guidance and mandatory rules for how to create cPP should be documented. Probably supporting documents. (in that case such docs should established by theCCDB on request of the WG. The WP should be updated accordingly.	Accept in principle (to be incorporated in WG workplan – no change to iTC/cPP Process document)
FMV26	Block 14		S	Current text: "and any deviation from the baseline SARs will require a justification, which includes a rationale as to how the [Vision] is maintained." What are "baseline sar:s"? Where are they described?	Clarify or remove.	Accept in principle (no change to document: text says they are defined in [cPP Temp] and this is to be produced as noted for the comment above)
FMV27	Block 15/16/17		S	Current text: "Although the iTC retains ownership of the cPP, and therefore decides how to respond to both internal comments (from members of the iTC) and	Update accordingly.	Accept

[1] NB = Notifying Body – the organisation submitting the comment

[2] Type of comment: C = critical; S = substantial; A = administrative

1	2	(3)	4	5	(6)	(7)
NB[1]	Clause No./ Subclause No./ Annex)	Paragraph/ Figure/ Table/Note)	Type of com-ment[2]	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
				external comments, the goal for a cPP remains to achieve consensus among as many nations as possble" Not only nations, but actually among all relevant stakeholder(like banks, NATO etc)		
FMV28	Block 15/16/17		S	Current text: "However, if there are changes in the content of statements of commitment (i.e. the actions that embody a nation's commitment), or if a nation moves to some other (non-Committed) status, then the reasons for this will be gathered from the nation by the iTC and notified to the CCDB via the Liaison CCRA Participant. Who is responsible to keep Committment status etc uptodate on the portal? The iTC? The CCRA liaison rep? The WG? The CCDB? This process of asking and re-affirming committment status back and forth may become difficult to manage. We may need to change the mechanism for how this achieved with our limited resources.	Discuss in the WG. After conclusion, update accordingly.	Accept (this situation is now managed through updates to PS/ES, which the author will send to the iTC for publication, so the iTC has the responsibility for maintaining this status and this will form a required part of the iTC ToR)
FMV29	Block 19/20/21		S	Current text: "then the reasons for this will be gathered from the nation by the iTC and notified to the CCDB via the Liaison CCRA Participant." What is the liaison CCRA participant expected to do with this	Clarify or remove.	Accept (clarify)
FMV30	Block 23/24/25		S	Current text: "at this stage the CCDB will review the cPP for consistency with the 'Baseline requirements' in [Vision]." The cPP should be consistent with the CC, CEM and supporting docs. That is verified by the scheme during the certification of the cPP. The CCDB has no say about the cPP as such, until some scheme calls for an discussion in the CCDB due to that it found that the cPP is not consistent with the CC, CEM or sup docs and	Need to be discussed in the WG, and text to be updated accordingly.	Accept (agreed at London workshop to require certification, but to allow it either before *or at* first use of the cPP)

[1] NB = Notifying Body – the organisation submitting the comment

[2] Type of comment: C = critical; S = substantial; A = administrative

1	2	(3)	4	5	(6)	(7)
NB[1]	Clause No./ Subclause No./ Annex)	Paragraph/ Figure/ Table/Note)	Type of com- ment[2]	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
				therefor wants this to be tested by the CCDB. And in such cases I think it is the CCMB that deals with such matters. And what are the "Baseline requirements"? There is not such work item in the CCDB or the WG.		
FMV31	Block 27		S	Current text: "The exception to the other reviews is that a formal CCDB review of the Supporting Documents and CCDB approval of these documents is required before they can be published for use in evaluations." Maybe rather than approving the sup docs, the CCDB can ask for changes in next release? Hmm... Want to avoid late suprises for the iTC. Very very important.	To be discussed in WG and updated accordingly.	Reject (due to the importance of positive CCDB approval of SD)
FMV32	Annex A		A	The whole Annex need to be updated to be consistent with other things. Below are some examples.		Accept (individual notes below)
FMV33	Annex A			Current text: "Approving the creation of iTCs for new technology areas requested by the CCDB" MC will not approve creation of new iTCs. MC will approve ToRs of iTCs and tech domains were supporting docs will be developed.		Updated
FMV34	Annex A			Current text: "Approving requests for new cPPs and allocating approved cPPs to iTCs; " Dont think this is correct. The CCDB does not approv individual cPP:s. It approves if we should establish WGs to create ESR:s. It suggest new tech domains to the MC, and approves supporting docs.		Updated (to be consistent with latest CCDB role statements)
FMV35	Annex A			Current text: "Seeking approval from the CCRA Management Committee for the creation of new iTCs; " Don't think this is correct. iTC can be established many ways and with involvement of the MC or even the DB.		Updated (to be consistent with latest CCDB role statements)

[1] NB = Notifying Body – the organisation submitting the comment

[2] Type of comment: C = critical; S = substantial; A = administrative

Disposition of comments on 'Establishing International Technical Communities and collaborative Protection Profiles development', v0.4, 130221

Date: 2013-12-13

Document: 'Establishing International Technical Communities and collaborative Protection Profiles development', v0.4, 130221

1	2	(3)	4	5	(6)	(7)
NB[1]	Clause No./ Subclause No./ Annex)	Paragraph/ Figure/ Table/Note)	Type of com-ment[2]	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
				But their ToR need to be approved by DB/MC.		
FMV36	Annex A			Current text: "the Working Group to define the ESR for a cPP" Correct, but the WG may do other things too. Like establish the iTC.		Updated (to be consistent with latest WG role statements)
FMV37	Annex A			Current text: "Seeking members for each iTC, and determining when the proposed membership of an iTC is sufficiently representative" I think itnis up to the iTC to prove themselces, rather than having the CCDB to staff the iTC (formally).		Updated (to be consistent with latest CCDB role statements)
FMV38	Annex A			Current text: "Providing the template ToR to a potential new iTC, and approving the completed" ToR to be approved by DB and endorsed by the MC (see language from draft of new CCRA v14.		Accept in principle (next version of the paper will be reviewed for consistency with the new CCRA, probably v15)
FMV39	Annex A			Current text: "Reviewing the cPP for consistency with the 'Baseline requirements' in [Vision], during its public review stage"; I think this is the certifying schemes responsibility to very against CC, CEM and supporting docs. The CCDB will not intervene in that. Issues a scheme may have, can be raised to the CCDB and/or CCMB.		Accept in principle (see response on certification of cPPs under FMV30)
SG1	All		C	Similar to the comment from GEE on what is 'CCRA member' and 'CCRA participant', it should be considered what 'nation' means.	Proposed change: Replace all occurannces referring to CCRA from 'member' and 'nation' to 'participant'.	Accept. CCRA Participants and CCRA Members are intended to be the same thing. 'Nation' then means the nation that a CCRA Participant represents. In iTC paper: change all "CCRA member" and "CCRA participant" references to "CCRA Participant" and

[1] NB = Notifying Body – the organisation submitting the comment

[2] Type of comment: C = critical; S = substantial; A = administrative

1	2	(3)	4	5	(6)	(7)
NB[1]	Clause No./ Subclause No./ Annex)	Paragraph/ Figure/ Table/Note)	Type of com-ment[2]	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
						add a note that this means the signatories to the CCRA (since many other entities, such as developers and labs, may see themselves as CCRA participants!).
SG2	All		S	The terms 'technial domain', 'techinal type', and 'technological domain' appear to have idenitical meaning,a dn should be stanardised or clearly defined.	Proposed change: Use 'technololgical domain' as single term and replace 'techinal type', 'technology domain', 'technical domain' etc.	Accept in principle Align to use of 'technology type' throughout iTC paper. Also make clear distinction with Technical Domain used in Supporting Documents
SG3	All		S	CC and the definition of PP refer to a term 'TOE type'. It is assumed that TOE type is basically identical to 'technological domain'. However, CC does not define TOE type, it only gives examples.	Proposed change: Provide a glossary of terms, and clarify that 'technological domain' (or whatever term is chosen) is identical to 'TOE type' in CC, or provide a definition of what a domain is. Also clarify if domains must exist or must be reflected int he CPL categoeries of the CC portal.	Accept in principle. The authors agree that there is some looseness of terminology here, but believe that the intention in the process is clear enough for the present, and will address individual comments as they arise. A tighter definition may be needed in future if and when examples have arisen where the question of technology type causes a significant problem in the process – linked to comment above. No further change to document.
SG4	All		C	There is no flow or reference d3fined, if and how a cPP can be maintained. Does it always start at sponsor and must undergo all stages?	Define the conditions and permitteed scope of maintenance for a cPP.	Accept in principle (to be addressed in a separate item covering cPP maintenance in the WG workplan)
SG5	Process for cPP Development	Block 12 iTC ToR Created/C CDB Approval/Li	A	Block 12 in flow diagram does not state who approved ToR an who approved iTC, which accroding to Annex A is done for iTC by CCMC and for ToR by CCDB.	Add the respective approving entity for 'iTC generation' and 'ToR approval' into diagram in accordance with the other blocks.	Reject. This is stated in the description of blocks 9-11 and 12: " the CCDB determines the best course of action with respect to engaging or creating an

[1] NB = Notifying Body – the organisation submitting the comment

[2] Type of comment: C = critical; S = substantial; A = administrative

Disposition of comments on 'Establishing International Technical Communities and collaborative Protection Profiles development', v0.4, 130221

Date: 2013-12-13

Document: 'Establishing International Technical Communities and collaborative Protection Profiles development', v0.4, 130221

1	2	(3)	4	5	(6)	(7)
NB[1]	Clause No./ Subclause No./ Annex)	Paragraph/ Figure/ Table/Note)	Type of com-ment[2]	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
		aison CCRA Participant Appointed				iTC to develop the new cPP"; " ToR must be submitted by the candidate iTC and approved by the CCDB". It is not the authors' intention to include all of the text information in the block diagram.
SG6	Process for cPP Development	Block 18 iTC Requireme nts Created	S	The document uses the term 'minimal security functionality' in two cases: one time during ES creation, and another time during the SFR definition. This seems to imply that 'more could be done', as it only states the 'minimum'. However, the vision statement has an explicit bullet point, stating that 'CCRA certificates claiming conformance to the cPP shall not include additonal security fucntionality besides those specified by the cPP'. As such, a CPP doesnot have 'minimum' security requirements, but 'exact' requirements.	Remove the term 'minimum' for requirements and clarify in alingment with the vision statement, that a iTC must be careful to define the suitable set of requirements, as no extensions are acceptable.	Accept in principle. (Deleted occurrence of "minimal" in block 4, and clarified with some extra discussion in Annex B.)
SG7	Process for cPP Development	Block 23/24/25 iTC/Public cPP Finalized and Published	S	A cPP is supposed to be approved by the CCRA, but for certification conformance claim and recognition of a IT product, the cPP must be certified and not only approved by the CCDB. Will the CCDB publish the cPP before or after certification? Secondly, can a participating Scheme in the development of a cPP be the Scheme to certify the cPP, or is ther conflit of interest? If later, then the process shouls at stage 1 immediately identify a Scheme a certifying scheme, and the Scheme then may not contribute to the actual PP writing stage (hile it may contribute to ESR, SPD, and Supporting document).	Define the certificatin rrequirements for a cPP.	Accept in principle (see response on certification of cPPs under FMV30)
SG8	Level of Commitment		S	The bullet point of defining commited nation has a different connotation from the expantion, ione using 'recommend' and the other 'strongly advise'	Propsed change from 'or strongly advice in their national..' to 'or recommend in their national...'	Accept (wording changed as part of change of terminology to 'Level of Endorsement')

[1] NB = Notifying Body – the organisation submitting the comment

[2] Type of comment: C = critical; S = substantial; A = administrative

1	2	(3)	4	5	(6)	(7)
NB[1]	Clause No./ Subclause No./ Annex)	Paragraph/ Figure/ Table/Note)	Type of com-ment[2]	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
SG9	Level of Commitment		S	This paragraph does not appear to be in line with the other descriptions in several manners and might need to be fully revised, as a) defiing the level of commitment is only expected around block 6, by which time e.g. ESR is already completed. b) it creates a difference in 'voting' or contribution capability, which may not be fulfilling the common practices, c) is not reflected in any subsequent blocks, where each such block clearly states that all comments shall be taken qually serious from all sources. d) for SPD, SFR, Suporting documents, which are all under the control of the iTC (and its ToR), the actual commitment status of a participant is assumed to be irrelevant	Proposed change: Remove the "but their uncommited status may weigh on the effort expended to address their comments'	Accept in principle (clarified text as part of general change of terminology to 'Level of Endorsement')
SG10	Level of Commitment		S	The paragrpah states that there are 'several places' wher a level of commitmentt can be reviewed, the diagram only shows one stage (block 16), the description include a few stages (e.g. 6), and text n block 6/7/8 states 'can be reevaluated at each milestone in the process'. However, milestone may not be identical to 'block', so the actual term should be used.	Proposed change from 'at several reveiw stages' to 'at each stage/block in the process by informing the CCDB chair'	Accept in principle (clarified text as part of general change of terminology to 'Level of Endorsement'; have specifically identified the formal reconfirmation/update stages, but note that the change is expressed by updating the statement of endorsement rather than by informing CCDB chair)
SG11	Level of Commitment		S	The document states that it is 'the ultimate goal for all CCRA members to be committed nations', but it is not clear if this is indeed a CCRA goaal, or a goal of a cPP, or (as expressed in later stage) a goal for the iTC. Additonally, if this remains a ultimate goal, it would entail a mandatory statement by every CCRA particpant on its commitemtn, which does not seem to be agreed upon.	Propsed change to remove the section 'the ultimate goal is for all CCRA...'	Reject. This is a goal of the process, and it is to be achieved by creating a suitable process, and by iTCs taking a constructive approach to widening the set of Endorsing Nations whenever possible. The fact that we have this goal does not impose any other obligation on CCRA Participants – this would be

[1] NB = Notifying Body – the organisation submitting the comment
[2] Type of comment: C = critical; S = substantial; A = administrative

Date: 2013-12-13	Document: 'Establishing International Technical Communities and collaborative Protection Profiles development', v0.4, 130221

1	2	(3)	4	5	(6)	(7)
NB[1]	Clause No./ Subclause No./ Annex)	Paragraph/ Figure/ Table/Note)	Type of com-ment[2]	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
						beyond the scope of the process or the WG. But it is important to state that we do hope to (one day) be writing such useful and relevant cPPs that every CCRA Participant will endorse them.
SG12	Block 1		A	The context and implication of the plain fact of a request may be misunderstood with the required content.	Proposed change from 'This request justifies the need' to 'This request should contain a justification for'	Accept
SG13	Block 1		A	The term 'sponsor' commonly bears connotation with funding, but this does not seem to be the case that a sponsor for a cPP must make any monetary commitment.	Propsed change from 'sponsor' to 'Initiator'	Accept
SG14	Block 2 & 3		A	There may be a substantial difference between 'interest' and 'need', which should be avoided, and based on fairness 'interest' may noot be objective enough as a criteria.		Accept in principle (clarified that interest would be based on identification of current or future need)
SG15	Block 2 & 3		A	Block 2 and 3 describe the scenario that a need is identified and an existing cPP can be changed, but the flow chart does not provide any idea if any of the stes (e.g. ESR) can be skippeed in such a case		Reject

There is no indication that steps can be skipped, because they cannot. In fact latest draft makes clear that the steps must be followed even if a complete ESR (or in later stages a complete PP) exists. |
| SG16 | Block 2 & 3 | | S | Is the sponsor automatically the lead nation for the WG, or how is this determined? | | Accept in principle

The answer is 'no'.

To be clarified in iTC paper |
| SG17 | Block 5 | | A | There has been no description of a commitment requirement so far, and it is only stated int he subsequent | Proposed change from 'CCRA representative of a commited | Accept in principle (changed to 'each |

[1] NB = Notifying Body – the organisation submitting the comment

[2] Type of comment: C = critical; S = substantial; A = administrative

Date: 2013-12-13	Document: 'Establishing International Technical Communities and collaborative Protection Profiles development', v0.4, 130221

1	2	(3)	4	5	(6)	(7)
NB[1]	Clause No./ Subclause No./ Annex)	Paragraph/ Figure/ Table/Note)	Type of com-ment[2]	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
				section for he first time, yet this section requires a commited nation to be known to act as CCRA representative.	nation' to 'CCRA representative of a authorising participant under the CCRA'	CCRA Participant in the WG ')
SG18	Block 9-11		S	The description seems to indicate that any existing TC (not necessarily an iTC) can be assigned to create the cPP, without then the need to create a separate iTC. This does not seem to be possible in all cases, as e.g. an existing TC may not be open to admit new members required for an iTC under their terms and conditions. Secondly, the scope of such a TC is not clear: Is it fully replacing a iTC, or is is only for the cPP development. If fact, the term 'cPP development is ambigous in the document, as it can refer to al stages of the flow, only to the responsibility of an iTC (starting in block 13, or restricted to blcoks 21 to 24.	Proposed change: Make it mandatory for a creation of an iTC, but clarify that an iTC may liase or outsource work to a suitable existing TC.	Reject If an existing TC is used, then it is the intention that it will be delegated responsibility for the cPP, with the usual level of CCDB oversight via the Liaison Representative.
SG19	Block 9-11		A	The paragraph states twice that 'CCDB would announce a call for participation in the creation of iTC'. The context appears to be identical, and so once metioning should be enough	Propsed change is to remove the last part of the section, re-stating again 'CCDB would announce a call for participation in the creation of iTC on the CC portal'.	Accept (redundancy removed as part of a wider change)
SG20	Block 9-11		C	The description seems to indicate that the creation of iTC is a matter of CCDB, but the Annex A states that CCMC is the entity to approve the creation of iTC. Depending on the first issue raised, it may need to be clarified if the CCMC also needs to be consulted if no iTC is created, but a TC be appointed?		Accept in principle (these responsibilities have been generally revised)
SG21	Block 12		S	The description seems to indicate that ToR and the development of the cPP 'belong' to the iTC, but does this include the copyright to the cPP itself? If so, how can maintence etc. be managed? Also block 13 explicit states that iTC is intended to 'have a justified sense of ownership' of the cPP content, and block 15 repeats that	Proposed adddtion: "While ToR belong to the iTC and the iTC is responsible for the creation of the cPP, the final cPP, suporting documents, SPD remain the copyright	Accept in principle (to be addressed in the iTC ToR template; no change to the iTC/cPP Process paper)

[1] NB = Notifying Body – the organisation submitting the comment

[2] Type of comment: C = critical; S = substantial; A = administrative

1	2	(3)	4	5	(6)	(7)
NB[1]	Clause No./ Subclause No./ Annex)	Paragraph/ Figure/ Table/Note)	Type of com-ment[2]	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
				iTC 'retains ownership' of the cPP.	of the CCRA'	
SG22	Block 13		S	The description seems to indicate that the CCDB may have some addtional criteria to the ESR, but it is the CCDB WG which creates the EST. As such it is not clear what CCDB could have as 'additonal constraints', which the WG for the ESR would not already have?Can't it be assumed that the development being under CCDB, the final ESR will already incorporate all CCDB constraints?		Reject Agree that mostly likely to have been covered by WG but, as the example shows, there may be other cases.
SG23	Role of CCDB		S	In the last but one paragrpah , it states that a cPP may undego a 'sunset' if a iTC is inactive. Thsisr aises a few questions: 1) What does it mean for a iTC to be inactive after the cPP has been published? 2) Does CCDB have any means to stop an iTC during any stage? 3) If a cPP is finsihed, it cannot be used for certification unless the cPP itself has been certified. As CCRA is discussing anyway to create a validity period for all certifcates, would that not address this issue more directly?		Accept in principle (to be addressed in separate paper on cPP maintenance – cf. response to SG4)
SG24	Pages 2 & 15	second para, 1st sentence	A		Proposed change from 'may have fiffering reasons for not committing or opposing a cPP' to 'may have differening reasons for neither commiting nor opposing a cPP'.	Accept (but note that this sentence has now been deleted!)
SG25	Page 4	last but on eparagraph	A		Proposed change from 'SPD and requirements are recast' to 'SPD and requirements be recast'	Accept (but note that this sentence has now been deleted!)
SG26	Page 5	paragraph	A		Align flowchart for block 22.	Accept in principle (much of this

[1] NB = Notifying Body – the organisation submitting the comment

[2] Type of comment: C = critical; S = substantial; A = administrative

Date: 2013-12-13	Document: 'Establishing International Technical Communities and collaborative Protection Profiles development', v0.4, 130221

1	2	(3)	4	5	(6)	(7)
NB[1]	Clause No./ Subclause No./ Annex)	Paragraph/ Figure/ Table/Note)	Type of com-ment[2]	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
		before block 1				paragraph has been rewritten)
SG27	Page 12	title of block22	A		align flochart with description and connect block 18 with blcok 26.	Reject (believe that the block 22 title reflects the description – note that the titles are not in general the same asthe flowchart labels. Block 18 only connects with block 26 via the other blocks as currently shown, so no change)
SG28			A		Proposed change from 'and allocating approved cPP to iTC' to 'and allocating the development of accepted cPP proposals to iTC'	Accept
SG29	Page 15	CCDB	A		Proposed change from 'may have fiffering reasons for not committing or opposing a cPP' to 'may have differening reasons for neither commiting nor opposing a cPP'.	Accept in principle (but affected text no longer present)
BSI1	All		S	From BSI point of view text concerning WTO should be removed, because the certification scheme does not have sufficient knowledge to judge the implications by the references to the WTO regulations. If there are useful passages in the WTO regulations they might be copied into our document, if possible.		Accept in principle (to be addressed by removing the WTO section and adding a summary of the 6 principles, although the latter remain criteria for accepting iTC ToRs)
BSI2	All		C	There should be kept a strong distinction between "recognition of certificates" and procurement – BSI (as example for also other CC schemes) does not have the competence to mandate a cPP for governmental procurement.		Accept in principle (This is intended to be clarified and resolved by the updated details of Levels of Endorsement)

[1] NB = Notifying Body – the organisation submitting the comment
[2] Type of comment: C = critical; S = substantial; A = administrative

Disposition of comments on 'Establishing International Technical Communities and collaborative Protection Profiles development', v0.4, 130221

Date: 2013-12-13

Document: 'Establishing International Technical Communities and collaborative Protection Profiles development', v0.4, 130221

1	2	(3)	4	5	(6)	(7)
NB[1]	Clause No./ Subclause No./ Annex)	Paragraph/ Figure/ Table/Note)	Type of com-ment[2]	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
BSI3	The MC Vision Statement in relation to the WTO – TBT Agreement	Page 3, first paragraph	S	What will be the content of the supporting documents? Assurance activities?		Accept in principle. An important part of the supporting documents will be the assurance activities, but we do not intend to limit the content here. The supporting documents should contain whatever is necessary or useful for the interpretation of CC to the relevant technology domain. Update iTC paper to note that assurance activities are a main part of the supporting documents.
BSI4	Level of Commitment		S	What is meant with "The description of how the commitment will be realized by the nation forms a part of its statement of commitment,"?		Accept. This means that, when expressing the 'Committed' level of commitment, a nation does not simply state the level, but also states the actions that it will take to express that commitment in practice (e.g. adding the product to an 'approved' list). This is noted in 'Block 15/16/17 iTC/Public SPD Finalized' where it mentions "the content of statements of commitment (i.e. the actions that embody a nation's commitment)", but this should be made clearer. This section has been superseded by the replacement of statements of commitment by Position Statements

[1] NB = Notifying Body – the organisation submitting the comment
[2] Type of comment: C = critical; S = substantial; A = administrative

1	2	(3)	4	5	(6)	(7)
NB[1]	Clause No./ Subclause No./ Annex)	Paragraph/ Figure/ Table/Note)	Type of com-ment[2]	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
						and Endorsement Statements.
BSI5	Process for cPP Development	Block 1 Sponsor Request cPP	A	What is meant with CCRA participant? What is meant with CCRA member? What is meant with "entity outside the CCRA"? What are the differences between the three terms?		Accept. CCRA Participants and CCRA Members are intended to be the same thing. Entities outside the CCRA are any other entity – e.g. industry bodies. In iTC paper: change all "CCRA member" and "CCRA participant" references to "CCRA Participant" and add a note that this means the signatories to the CCRA (since many other entities, such as developers and labs, may see themselves as CCRA participants!).
BSI6	Process for cPP Development	Block 2/3 CCDB/Spo nsor cPP Need Determined	C	In which way the CCDB will deal with requests? When will the requests be discussed? During CCDB meetings, in CCDB conf calls, per email discussion? Who will be involved in the discussions about the requests? In which way the CCDB will come to the decision about a request? Simple majority vote, two-thirds majority? Does anyone have the power of veto? What will be the timeframe for the CCDB to answer to a request?		Accept in principle (to be addressed outside the document in the CCDB Role Guidance)
BSI7	Process for cPP Development	Block 2/3 CCDB/Spo nsor cPP Need Determined	S	What about competing sponsors? Who will get the positive response?		Accept (to be addressed outside the document in the CCDB Role Guidance)
BSI8	Process for cPP Development	Block 2/3 CCDB/Spo nsor cPP Need	A	"The CCDB consults the CCRA". What is meant with "CCRA" here?		Accept Add "Participants" after "CCRA" in iTC paper.

[1] NB = Notifying Body – the organisation submitting the comment
[2] Type of comment: C = critical; S = substantial; A = administrative

Date: 2013-12-13	Document: 'Establishing International Technical Communities and collaborative Protection Profiles development', v0.4, 130221

1	2	(3)	4	5	(6)	(7)
NB[1]	Clause No./ Subclause No./ Annex)	Paragraph/ Figure/ Table/Note)	Type of com- ment[2]	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
		Determined				
BSI9	Process for cPP Development	Block 2/3 CCDB/Spo nsor cPP Need Determined	S	Who will decide about the members of the working group?		Accept (to be addressed outside the document in the CCDB Role Guidance, since it is the CCDB that creates the WG)
BSI10	Process for cPP Development	Block 12 iTC ToR Created/C CDB Approval/Li aison CCRA Participant Appointed	S	What are the regulations for the CCDB approval of the ToR?		Accept (to be addressed outside the document in the CCDB Role Guidance, although the reference to the 6 principles in the next version of the document is also related to this)
BSI11	Process for cPP Development	Block 13 iTC Workplan Creation/Li aison CCRA Participant	S	Who will formulate the CCDB constraints? In which timely manner?		Accept (to be addressed outside the document in the CCDB Role Guidance, since this is a CCDB responsibility)
BSI12	Process for cPP Development	Block 14 iTC SPD Creation	S	What is the cPP template? Who will create this document?		Accept in principle (to be resolved via a separate USB WG workplan item – no change to iTC/cPP paper)
BSI13	Process for cPP Development	Block 14 iTC SPD Creation	A	What is meant with "general rules"?		Accept in principle. The "general rules" are those represented by the text of the Vision Statement. No change to iTC paper.

[1] NB = Notifying Body – the organisation submitting the comment
[2] Type of comment: C = critical; S = substantial; A = administrative

1	2	(3)	4	5	(6)	(7)
NB[1]	Clause No./ Subclause No./ Annex)	Paragraph/ Figure/ Table/Note)	Type of com-ment[2]	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
BSI14	Process for cPP Development	Block 15/16/17 iTC/Public SPD Finalized	S	Shouldn't the external comments be channeled by the schemes? Otherwise it might be possible to receive contradictory statements from one nation and no one is able to weigh them.		Reject. The iTC will be responsible for weighting comments and resolving any conflicts.
BSI15	Process for cPP Development	Block 15/16/17 iTC/Public SPD Finalized	S	What is meant with "changes in the content of statements of commitment (i.e. the actions that embody a nation's commitment),"?		Accept in principle. This means that nations may change their statements of commitment, either to change their level of commitment or to change the actions that the commitment implies. In any such case (particularly where this represents a reduction in the commitment or the strength of the actions) the nation will be asked to explain the reasons for the change. The iTC paper has been updated extensively in this area, but it is still possible for nations to withdraw or update statements at any time.
BSI16	Process for cPP Development	Block 18 iTC Requirements Created	S	Are the assurance activities part of the requirements, i.e. part of the cPP? If yes, what is the content of the supporting documents?		Accept in principle The assurance activities are considered to be part of the supporting documents. But there may be other content for the supporting documents – e.g. to address cryptographic aspects for the technology type. Update iTC paper to note that assurance activities are a main part of the supporting documents.

[1] NB = Notifying Body – the organisation submitting the comment

[2] Type of comment: C = critical; S = substantial; A = administrative

Date: 2013-12-13	Document: 'Establishing International Technical Communities and collaborative Protection Profiles development', v0.4, 130221

1	2	(3)	4	5	(6)	(7)
NB[1]	Clause No./ Subclause No./ Annex)	Paragraph/ Figure/ Table/Note)	Type of com-ment[2]	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
BSI17	Process for cPP Development	Block 23/24/25 iTC/Public cPP Finalized and Published	S	Shouldn't the cPP undergo any formal evaluation? Should this process be implemented by the iTC in any way? The planned public review process does not substitute a real evaluation.		Accept (see response on certification of cPPs under FMV30).
BSI18	Process for cPP Development	Block 27/28/29/30 iTC/Public/ CCDB Supporting Documents Finalized and Published	C	Why do the supporting documents have to be approved by the CCDB, but the cPPs themselves do not?		Accept in principle At the reviewing stage we believe it is important that both cPP and supporting documents can be reviewed together. However, the process specifically intends to delegate responsibility for the technical content of the cPP to the iTC, where the appropriate expertise is located. Therefore there is no formal requirement for the cPP to be approved by the CCDB. Clarification added to the iTC paper that cPP may be available, but must not be used before supporting documents are agreed. (Also note certification requirement for cPP added as noted under FMV30.)
ANSSI1	The MC Vision Statement in relation to the WTO – TBT Agreement	Para starting "Some of the fundamental principles of the	S	This paragraph is completely outside the scope of CCRA an of the job of our agency. 1) The subject dealt with the WTO is generally managed by the authorities in charge of economics affairs and notgenerally by the national security agencies. . 2) The WTO does not concern private companies which use certification as a means for their own procurement.		Accept in principle (to be addressed by removing the WTO section and adding a summary of the '6 principles')

[1] NB = Notifying Body – the organisation submitting the comment

[2] Type of comment: C = critical; S = substantial; A = administrative

Date: 2013-12-13	Document: 'Establishing International Technical Communities and collaborative Protection Profiles development', v0.4, 130221

1	2	(3)	4	5	(6)	(7)
NB[1]	Clause No./ Subclause No./ Annex)	Paragraph/ Figure/ Table/Note)	Type of com-ment[2]	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
		WTO-TBT Agreement …"		3) The WTO is not the good instance to define the level of security of a product for the companies/nations which usecertified products		
ANSSI2	The MC Vision Statement in relation to the WTO – TBT Agreement	Sentence starting "But it can be noted that moving into a cPP-based approach …"	S	It is the responsibility of the nations, which may also be members of the WTO, to comply with its rules. Therefore the only thing to say about WTO is that any specific government procurement policy should be in line with the WTO-TBT, together with the sentence numbered 2) below. Further analysis of possible inconsistencies between national procurement policies and WTO-TBT is out of the scope of CCRA, which is a recognition agreement based on technical aspects (ie nations recognise the quality of the work done by a lab in another member nation for the security evaluation of a given product at a given level).		Accept in principle (see response to comment above).
ANSSI3	The MC Vision Statement in relation to the WTO – TBT Agreement	Bullet starting "Nations that are signatories of the CCRA should …"	C	In general, the development of multiple PPs answers to the expression of different security needs, that may correspond to different assurance levels, or to different functional needs (e.g. firewall, VPN client or firewall+VPN client). Therefore the sentence should be something like "Nations that are signatories of the CCRA should collaborate in order to avoid developing multiple national PPs in the same technical domain, unless these PPs correspond to particular and different security neeeds".		Accept in principle (text changed to talk about avoiding *unnecessary* overlapping cPPs).
ANSSI4	Level of Commitment	Bullet list of levels of commitment, under first paragraph	C	There are some other possibilities : Nations which use some cPP for their procurement policies (understood : some cPP will not be used because they don't agree with the content) Nations which use cPP but with some extensions		Accept in principle. Levels of commitment have now been replaced by Position Statement & Endorsement Statement contents, which allow a more flexible way for a nation to express its stance on a cPP

[1] NB = Notifying Body – the organisation submitting the comment
[2] Type of comment: C = critical; S = substantial; A = administrative

| Date: 2013-12-13 | Document: 'Establishing International Technical Communities and collaborative Protection Profiles development', v0.4, 130221 |

1	2	(3)	4	5	(6)	(7)
NB[1]	Clause No./ Subclause No./ Annex)	Paragraph/ Figure/ Table/Note)	Type of com-ment[2]	Comment (justification for change) by the NB	Proposed change by the NB	Resolution[1] on each comment
				(technical or evaluation level depending of their own risk analysis, or some local recommendations, for instance in the area of cryptography)		(including disagreements or expression of required changes to a cPP/SD). We do not deal with extensions to cPPs: this is to be covered by the definition of exact conformance (which is outside the scope of the iTC Process paper), and the use of optional packages in a cPP.
ANSSI5	Level of Commitment	Sentence ending "…but their uncommitted status may weigh on the effort expended to address their comments."	A	Or, on the contrary, may encourage participants to the TC to take such nations' needs into account in order to increase the number of procurers that may ask for this cPP. This part of the sentence is probably unnecessary.		Accept in principle. It is true that the iTC is expected to consider whether it could accommodate additional requirements of CCRA Members in the cPP, and an important part of this is the potential increase in market size for the product. The original sentence has been clarified to better express this point in the new section on Position Statements & Endorsement Statements.
ANSSI6	Process for cPP Development	Figure 1	S	The diagram could possibly highlight the role of committed/uncommitted/opposed nations throughout the entire process. It could for example be divided into several phases : - phase 1 where intially committed nations define an ESR - phase 2 where all CCRA nations can interact with the TC, and eventually change their status based on the achievements of the TC (e.g. move from uncommitted to committed or from committed to opposed etc.). - phase 3 where CCRA nations make public their final		Accept in principle. A high-level diagram has been added to summarise the process and to highlight the place of Position Statements & Endorsement Statements (which replace levels of commitment).

[1] NB = Notifying Body – the organisation submitting the comment

[2] Type of comment: C = critical; S = substantial; A = administrative

Date: 2013-12-13	Document: 'Establishing International Technical Communities and collaborative Protection Profiles development', v0.4, 130221

1	2	(3)	4	5	(6)	(7)
NB[1]	Clause No./ Subclause No./ Annex)	Paragraph/ Figure/ Table/Note)	Type of comment[2]	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
				position on the cPP - phase 4 where the cPP is "in use", and where committed/uncommitted nations recognise the cPP at its own level and for the formers, recommend it, and where opposed nations may only recognise it under the EAL2 limitation or simply recommend not to use it.		
ANSSI7	Process for cPP Development	Figure 1, block 24-25	S	According to the foreseen modification of the CCRA, a cPP can be recognised above the EAL2 limitation if appropriate supporting documentation is available. Therefore a cPP shall not be published unless the associated supporting documents are approved, or its recognition should come under the EAL2 limitation.		Accept in principle (more explanation has been added about the connection between a cPP and its Supporting Documents).
ANSSI8	Process for cPP Development	Figure 1, block 29	S	Since consuming nations are likely to use cPPs through evaluations done in other schemes, it seems that the MC level would be more appropriate for the approval of such documents. One may find difficult to recognise technical results based on a methodology they have not reviewed and approved for "high" levels of assurance (i.e. for components above the EAL2 level).		Accept in principle. The revised CCRA will cover some of this, and Supporting Documents will continue to be approved in the normal way (a reference to the operating procedure on Supporting Documents has been added). Also, as noted above, more explanation has been added about the connection between a cPP and its Supporting Documents. A note has also been added to note the requirement for certification of cPPs either before *or at* first use of the cPP.
ANSSI9	Process for cPP Development	Block 14 iTC SPD Creation, sentence ending "…any deviation	S	contradiction with VS that states "any deviation from the baseline SARs will be outside CCRA recognition"		Accept in principle. The authors believe this comment relates to bullet 5 in the ' Baseline requirements' section of the vision statement, which states that " cPPs shall define the achievable common

[1] NB = Notifying Body – the organisation submitting the comment

[2] Type of comment: C = critical; S = substantial; A = administrative

Disposition of comments on 'Establishing International Technical Communities and collaborative Protection Profiles development', v0.4, 130221

Date: 2013-12-13

Document: 'Establishing International Technical Communities and collaborative Protection Profiles development', v0.4, 130221

1	2	(3)	4	5	(6)	(7)
NB[1]	Clause No./ Subclause No./ Annex)	Paragraph/ Figure/ Table/Note)	Type of com-ment[2]	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
		from the baseline SARs will require a justification, which includes a rationale as to how the [Vision] is maintained."				level of security assurance and will address vulnerability analysis requirements to ensure certified products achieve an expected level of security. Assurance activities not defined in the cPP will not be recognised under the CCRA and certificates claiming conformance to the cPP shall not include higher level and/or additional assurance requirements." This part of the vision statement is referring to deviations in an ST or an evaluation compared to the assurance activities in the cPP. However, the sentence in the iTC paper refers to deviations in the cPP compared to the baseline SARs *as defined in the cPP template.* So the deviations referred to in the iTC paper are about the definition of assurance activities in the cPP itself, not about subsequent deviations from the cPP in an evaluation or ST.
ANSSI10	Process for cPP Development	Block 27/28/29/30 iTC/Public/ CCDB Supporting Documents Finalized and Published	C	type ofvote: unanimity? majority? note that if countries do not agree with a supporting document means thatthis countru donot recognized the result of the evalution....		Accept in principle (to be addressed outside the iTC Process paper, in [CCDB Role] and [ToR Guide], and by revised CCRA).
ISCI1			S	ESR, SPD & requirements are created and offered to		Accept in principle

1	2	(3)	4	5	(6)	(7)
NB[1]	Clause No./ Subclause No./ Annex)	Paragraph/ Figure/ Table/Note)	Type of com-ment[2]	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
				public review in an English narrative form avoiding the CC terminology. Moreover it is advised to develop a set of English requirements in conjunction with CC SFR written in the cPP to minimize divergence with the original English prose. This approach open the door to a lot of ambiguities, misunderstanding, challenges and time lost.		The text of the iTC paper has been updated to clarify that it is not intended to be mandatory to use only natural language. In reality we expect that the natural language and CC SFRs will be developed in parallel. However, it remains the authors' recommendation that natural language is used extensively as described – indeed we believe it is a mechanism for *avoiding* ambiguities, misunderstanding, challenges and lost time, in part by making it easier to include the participation of non-CC experts.
ISCI2			S	The process for cPP development seems heavy and long with many review periods. This seems to be linked to the goal of obtaining the longest possible list of Committed Nations		Accept in principle. The authors would agree that the speed of progress is reliant on goodwill and resourcing, but do not see a lighter weight process that brings the benefits of national commitment that we are looking for here. We note that once the iTC has been established then it is largely in control of the speed of the process. The authors believe that once the process is mature (and the participants are comfortable with it), much of this could be speeded up. For example a dedicated CCDB group might be able to handle cPP requests outside of formal face-to-face meetings. But this needs to be based on confidence derived from

[1] NB = Notifying Body – the organisation submitting the comment

[2] Type of comment: C = critical; S = substantial; A = administrative

Disposition of comments on 'Establishing International Technical Communities and collaborative Protection Profiles development', v0.4, 130221

Date: 2013-12-13

Document: 'Establishing International Technical Communities and collaborative Protection Profiles development', v0.4, 130221

1	2	(3)	4	5	(6)	(7)
NB[1]	Clause No./ Subclause No./ Annex)	Paragraph/ Figure/ Table/Note)	Type of com-ment[2]	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
						evidence of the successful use of the process. No change to the iTC paper.
ISCI3	Background	"avoid several cPPs being established in the same technical domain"	S	How to manage a situation where different security needs (depending on the context of use) could be required in the same technical domain?		Accept in principle. If there are genuinely multiple different sets of security needs (e.g. based on different use cases) then more than one cPP could be created (probably by a single iTC). The paper does not intend to exclude this situation (nor does the September 2012 vision statement). However, we do believe that it is important to harmonise requirements wherever possible – hence the creation of a separate cPP in an existing technology domain would be subject to the initial CCDB approval in block 2 of the process. The paper also allows for options to be included in the ESR and cPP – this may also help to address some different security needs, but we need to ensure that this does not damage the common understanding of what certification against the cPP will mean. Current text says "avoid unnecessary overlapping cPPs".
ISCI4	Level of Commitment	"The ultimate goal is for all CCRA members	S	The described process is oriented towards Government procurement: O In particular with the level of commitment mechanism. O There is no other CC use cases mentioned		Accept in principle. It is true that the initial process is oriented towards government procurement, because this represents an area where improving the *adoption*

[1] NB = Notifying Body – the organisation submitting the comment

[2] Type of comment: C = critical; S = substantial; A = administrative

1	2	(3)	4	5	(6)	(7)
NB[1]	Clause No./ Subclause No./ Annex)	Paragraph/ Figure/ Table/Note)	Type of com-ment[2]	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
		to be Committed Nations for the cPPs of all types of technology for which their government has a national requirement."		O There is no room for other stakeholders such as an association of customers or operators to be the Sponsor and the real applicant for a cPP.		of PPs (rather than just the *recognition*) is important and has the potential for significant improvement. However, this does not exclude non-government communities from initiating a cPP request through a CCRA Participant. The paper notes (in the description of block 1) that in future requests may be accepted from other entities. Latest draft of the iTC paper is written as a more general (less USB-specific) process, and identifies that the mature process is expected to be suitable not just for government needs, but for any collaborative CC/security requirement setting.
ISCI5	Process for cPP Development	Block 9/10/11 CCDB iTC Engaged/Created	S	In the context of "If one or more potentially suitable TCs exist (e.g. an industry body with an existing security/CC remit), then a CCDB representative will be given responsibility for initiating contact to determine if a working relationship can be established" – Can we consider that such a TC exists already for the smart cards and similar devices□Technical Domain? Can ISCI expect to be contacted ? The USB token is it not such a similar device?		Accept in principle. It is likely that the communities for smart cards, payment terminals, and other existing PP-producing communities would be identified for cPPs for their corresponding technology types. There would still be a formal appointment process (blocks 10 & 12) in this case, and the adopted TC would be expected to follow the defined process for the cPPs that it produces. USB storage devices are currently considered to be a distinct technology area from smart cards, with distinct use cases and assurance requirements. The calling notice for the USB iTC will be published on the CC portal, and at

[1] NB = Notifying Body – the organisation submitting the comment

[2] Type of comment: C = critical; S = substantial; A = administrative

Disposition of comments on 'Establishing International Technical Communities and collaborative Protection Profiles development', v0.4, 130221

Date: 2013-12-13

Document: 'Establishing International Technical Communities and collaborative Protection Profiles development', v0.4, 130221

1	2	(3)	4	5	(6)	(7)
NB[1]	Clause No./ Subclause No./ Annex)	Paragraph/ Figure/ Table/Note)	Type of com- ment[2]	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
						this point ISCI WG1 would be able to participate in the iTC. No change to iTC paper.
ISCI6	Process for cPP Development	Block 23/24/25	S	The cPP will not be evaluated and the only requirement to achieve it is that comments have been processed . What are the evidence that the cPP addresses all the rules of PP construction? What is the arbitration mechanisms in front of challenge on comment?		Accept in principle (see response on certification of cPPs under FMV30)

[1] NB = Notifying Body – the organisation submitting the comment

[2] Type of comment: C = critical; S = substantial; A = administrative