International Technical Communities formation process – FAQ

FAQ to accompany 'Establishing International Technical Communities and collaborative Protection Profiles development', v0.4.

1. *What are the main priorities of the cPP and iTC development process proposed by the CCDB USB Working Group?*

   The fundamental aim for the process has been to take the intentions in the CCMC's 'Vision statement for the future direction of the application of the CC and the CCRA' of September 2012, and to develop a more detailed process for forming iTCs and developing cPPs. The main priority for the process is that it should build support for each cPP from as many CCRA Participants as possible so that the cPP will not only be *recognised* by the member nations, but also *adopted* for use.

   The next level priorities are to minimise the level of CCDB involvement required, and to give the iTC as much ownership of the cPP as possible. Finally, the process is intended to enable cPP development to be as fast as possible, once support has been given for the other priorities.

   We are conscious of the suggestion that speed of cPP development could be a higher priority. However, we make the following observations about this:

   - We believe that getting support for a cPP at an early stage is important, and that this support will take a certain amount of time to build, especially for the first few times that the process is applied. The prize for the patience and effort involved is a set of iTCs and cPPs that will not just make small improvements to the traditional approach to PPs, but that will give cPPs a role in harmonising national requirements wherever possible, and that will emphasise the adoption (i.e. the *use*) of cPPs rather than just their development. The process supports harmonisation by deliberately putting in steps to encourage widespread participation amongst CCRA Participants, and to start cPP development in a context where these harmonised requirements can be clearly understood. It supports adoption by encouraging the submission of Position Statements from the point at which the ESR is made available, which therefore enables industry participants to more clearly see the benefits of participation in an iTC, and encourages vendors to make available products that meet the cPP (because there is a clearer and cleaner path to achieving a certified product with known benefits in a known group of nations)
   - Several of the early steps do not have to be repeated once the iTC has been formed – so for example, we would not expect ESRs to change frequently, nor would the iTC selection and ToR review need to be repeated for updates to the cPP.
   - The current process is expected to evolve to streamline the process in the light of experience in applying it.

2. *What do a CCRA Participant's Position Statements and Endorsement Statements mean?*

   Position Statements and Endorsement Statements are about related to how CCRA Participants intend to *adopt* a cPP, and therefore represent a level of support beyond simply *recognising* a certificate.

   In the early stages of cPP development a Position Statement indicates the support of a CCRA Participant for the development of a cPP. CCRA Participants cannot express a binding commitment to a cPP that they have not yet been seen, but at an early stage a CCRA Participant will use a Position Statement to indicate support for the direction a cPP is taking as indicated in the published interim deliverables at that point (e.g. the ESR and the SPD). In some cases, a CCRA Participant may use a Position Statement to formally record a requirement that the cPP does not currently seem to address. Although such a Position Statement may not indicate support for the cPP[1], it indicates what would be necessary in order to gain the additional support from the PS author. This enables the iTC to make judgements about how, and when, it would be best to update the cPP in order to make it more widely adopted.

   An Endorsement Statement is issued when a CCRA Participant has been able to review a cPP and enables the author to set out the specific ways in which that CCRA Participant expects to recognise the benefits of products that are certified against the cPP (and that therefore are shown to meet its national requirements as embodied in the cPP). Typically this would include making some sort of recommendation for the use of such products – perhaps by adopting the cPP as a procurement requirement, or placing conformant products on an 'approved' list.

3. *How is a CCRA Participant's Position Statement maintained during the development of the cPP?*

   Updates to a CCRA Participant's Position Statement are requested at various points during the cPP development: when the SPD is completed, and when the security functional requirements are completed. We note that one of the purposes of recommending more extensive use of natural language at the requirements stage is to make it easier for CCRA Participants to confirm their support at this stage (which may involve them in consulting beyond their CC-expert group). This re-confirmation process is a more *engaged* way of ensuring that there are no hidden, delayed, or misunderstood objections to the cPP, and therefore a means of sustaining confidence and commitment to the iTC work.

   If a CCRA Participant reduces its level of support during cPP development then we expect that the iTC would be motivated to try and address this; however, there can be no absolute obligation for the iTC to do this. Although we believe that the process generally aligns the incentives for all parties towards collaboration and creation of a cPP that accommodates a variety of member requirements, ultimately it may not be possible to satisfy all CCRA Participants. However, the use of Position Statements will at least prevent this from happening by accident or inattention. Over time, we believe that successful use of the process and of the resulting cPPs will demonstrate the benefits to CCRA Participants (as well as to other bodies) of

[1] A PS could indicate support for the current cPP, but could also indicate a future requirement beyond the scope of the current cPP.

making a strong effort to present their requirements and to make a strong statement of support in their Position Statements, and ultimately of issuing Endorsement Statements.

4. *How are SFRs in a cPP to be standardised between CCRA Participants, especially where there are different national requirements?*

   We do not underestimate the challenges here, but fundamentally we believe that there is significant scope for agreeing requirements amongst members, even at the SFR level. Our intention here is to move away from a position where PPs tend to be developed without strong engagement of all the CCRA Participants who are intended to use them. The main parts of the process that support our belief that we can achieve greater harmonisation are:

   - making the process more focussed on getting early inputs to define a cPP scope (in the ESR) that will maximise support from CCRA Participants
   - encouraging participation in iTCs, and supporting the authority of iTCs by giving them strong ownership of the cPP and its development, including the resolution of issues (so there is a 'one-stop' place where issues can be resolved, instead of a 'propose then ratify at CCDB' model)
   - encouraging involvement of CCRA Participants in cPP reviewing, even if the CCRA Participant is not an active or regular participant in the iTC activities
   - encouraging the use of extensive amounts of natural (non-CC) language in the cPP development to make the early stages of the cPP more accessible to non-CC specialists who may be supporting CCRA Participants for particular technology types; in addition, if this non-CC language is retained as supporting text in the final cPP then a CCRA Participant can have more confidence that they understand the cPP and that it will be applied consistently.

5. *Why is there so much deliberation and approval in the early stages of the process to approve an iTC and cPP?*

   Obtaining significant levels of consensus and support amongst CCRA Participants will depend on getting clarity and understanding about the cPPs and iTCs that are being proposed. The support that we are seeking from CCRA Participants will often require them to discuss and consult with national bodies, and we believe it is important to be clear about both the expectations on CCRA Participants and also the fact that this process needs certain steps if it is to be meaningful over the longer term of cPP development.

6. *Why are vendors not involved earlier in the process, at the point where the ESR is created?*

   The ESR is all about establishing requirements across multiple CCRA Participants (and hence multiple nations). Ideally vendors and others (such as labs) would be involved all the way through, but we believe that the process we have defined is the best way of breaking down steps that progressively build confidence and support for the cPP (without an overloading bureaucracy of consensus) and then progressively build detail within a context of support. This seems to be the key thing, as opposed to having fully correct technical detail from the very start. Also note that there is provision for the ESR to be updated later by the iTC if necessary.

There is no reason why CCRA Participants should not consult vendors during the ESR creation, but this is not mandatory, and the ESR will be available for public review before its final adoption (although the decision as to how to respond to review comments will remain with the ESR authors and the relevant Working Group).

7. *Why are there no limits on the size of iTC membership?*

   It is fundamental to the aim of increasing *adoption* (rather than just *recognition*) of cPPs that we should make the process as inclusive as possible. Recent experience has suggested that even where a technical community becomes large, there will be relatively few active members, and this will still enable progress to be made. Once an ESR has established the parameters for the cPP, and gathered a base of support, then we would expect that many CCRA Participants will be content to review the outputs from a suitably technically competent iTC working from the ESR.

   The expectations for routine operation of an iTC will be that it will make suitable efforts to enable the active membership to participate, but this need not inhibit measures to ensure the group can make suitable progress against its workplan. If significant problems arise from the size of the membership, then the iTC would generally be free to work out its own techniques for managing these (based, for example, on its workplan and the demographics of its active membership).

8. *Why does the process emphasise so much use of natural language?*

   Firstly it should be noted that the process does not intend that it should be *mandatory* to *replace* CC language with natural language at any point. However, we do believe that jumping too early into CC constructs (a) diminishes the level and effectiveness of participation by non-CC participants who may be important for technical and/or risk-owner input; (b) brings risks that because the language and structures are now not expected to be 'everyday' then there is an interpretation layer when reading them, and different participants may do this step in different ways without the differences being obvious; (c) largely as a result of (b) this can lead to differences of opinion being hidden until they become fatal cracks in the support and endorsement at a later stage, rather than being addressed at a time when they could be accommodated in some way.

   Even experienced CC people will tend to carry expectations based on their previous use and interpretation of SFRs forwards into a new PP, and we know that this is not always consistent. Starting in natural language is intended to reduce the 'hidden expectations', or at least make them explicit in the natural language that surrounds the SFRs and can be adopted to make a more usable and consistently applied cPP by building the text into SFR refinements, SFR completion, assurance activities and/or application notes. The natural language gives us a comprehensive shared staring point and we can then more easily ask 'do the SFRs actually say that?' as a reviewing question.

9. *What level of consensus is required in Working Groups and iTCs?*

   We note firstly that consensus need not imply unanimity. In particular, there is not intended to be any suggestion that an iTC's decision making process should be based on unanimity (nor indeed on unanimity of any particular subset of its membership, such as CCRA Participants). As

discussed for other questions, the process has been designed to enable consensus and support to be built, and it is obviously important that consensus and collaboration remain the dominant state of mind within the iTC. Mechanisms also exist for dealing with disagreements and unreconciled views at various stages in the process, without having to resolve them in favour of one view and to the detriment of the other. For example: an iTC can be given an ESR with notes about additional comments and opposition to the ESR, a Position Statement can be used to formally record a requirement that the cPP is not currently addressing, and there is the possibility of defining optional packages within the cPP.

10. *What Supporting Documents are required to accompany a cPP?*

    It will be for the iTC to define the detail of what supporting document content is needed, depending on the technology that the cPP addresses, but based primarily on the idea that the Supporting Documents "describe the evaluation methodology and application of the Common Criteria Security Assurance Requirements to the specific technology type in determining conformance with the cPP" (see the description of block 18 in the iTC paper). There is no requirement that all cPPs should have a certain set of supporting documents, although it will be expected that *some* supporting documents will exist to describe the assurance activities for the cPP.

11. *How will the CCDB gauge the level of CCRA Participants' interest , and how much interest is sufficient (in terms of number of members or other criteria) before an iTC can be created?*

    This is a deliberately non-formal part of the process. It basically requires each CCRA Participant to establish whether it has a need for that type of technology. The actions and criteria for this are up to the relevant nation. It should not be confused with a rigorous assessment of whether the technology is "worthy" – it is much more pragmatic than that. Roughly speaking: if there is sufficient interest in a future technology then it will get an iTC anyway. If not, then this does not kill the technology! It just means that CC will have to catch up when the technology has developed enough to capture the interest. The technology types under consideration are expected to be on the CC portal website and so will be visible for interested parties to discuss with national representatives.

12. *What happens if two vendors cannot be found to participate in the iTC?*

    Two is the intended minimum ("at least two vendors"), and it is important that the iTC membership is sufficiently representative. We recognise that in a very few cases there could be only one vendor making CC-evaluated products of the relevant type. This would be handled as an exception to the iTC process.

13. *What is the lifecycle of a cPP and an iTC after the initial cPP has been completed?*

    More detail needs to be given for the post-completion lifecycle of a cPP and its iTC and this will be addressed in a future paper. However, an outline of the current expectation is as follows:

    - The iTC would usually continue to exist, and would respond to questions that may arise in early uses of the cPP, as well as being responsible for making updates to the cPP or its

supporting documents as a result of lessons learned, changes in the technology, and changes in the attack and threat status

- Because the ESR is at a high level, it is not expected to need frequent changes, however…
- …the ESR can be updated if a technology changes significantly, or if CCRA Participant national requirements change (including in some cases perhaps to accommodate a new Participant)
- Updates to the cPP would be reviewed in a similar way to the initial development, with a public review period for the draft updated cPP. Review and release steps for Supporting Documents may have to vary according to the type of document, in order to balance the need to ensure that assurance activities remain consistent with the Vision Statement and CCRA, but also that changes in the threat or attack situation can be accommodated sufficiently rapidly
- Additional CCRA Participants can issue a Position or Endorsement Statement and join the iTC at any time
- Existing Endorsement and Position Statements on the cPP would normally be expected to remain in place, but can be revised at any time.