Common Criteria Recognition Arrangement
Development Board

Establishing iTCs and Developing cPPs

Title: Establishing International Technical Communities and Developing collaborative Protection Profiles
Maintained by: CCDB Work Group for USB Portable Storage Devices
Unique Identifier: 015
Version: 1.0
Status: Final
Date of issue: 2023-Oct 30
Approved by: CCMC

Purpose

This document describes the preferred process for developing a collaborative Protection Profile (cPP) and related Supporting Documents (SD)[1] under the CCRA. The development of a cPP/SD is carried out by an international Technical Community (iTC) that is endorsed by the CC Management Committee, and the process therefore also covers the formation and operation of an iTC. The process is intended to enable and encourage collaborative harmonisation of security functionality and assurance requirements for IT products that will provide the grounds for procurement and policy. The intent of this paper is to convey the general principles and present a high level process flow of the milestones that take place once a request has been made for the development of a cPP for a given technical area. Many individual details are deliberately left for the iTC to develop within certain constraints (which generally arise from CCRA-related concerns or past experience of applying CC). The CCDB will provide separate guidelines for the development of Terms of Reference (ToR) describing the task and operating practices of an iTC, including a ToR template [ToR Guide], which will incorporate research into existing technical communities performed by the Common Criteria Users Forum (CCUF).

Initial Certain aspects of the initial application of the process will be more constrained than in the mature version (i.e. when experience of the process has generated confidence in its consistent application and effectiveness). For example, initially only CCRA Participants will be allowed to act as Initiators (i.e. the entities that submit requests for a cPP to the CCDB). These initial constraints are expected to be implemented in [CCDB Role] and [CCMC Role] (e.g. by making changes to CCDB decision criteria once suitable reference examples of the use of the process have been achieved). It will be announced, via a statement on the CC portal and update of the relevant documents, when the initial constraints have been relaxed.

It is expected that this process will be improved in the future by making refinements based on experience of applying it. The goal is to create a 'method of choice' for capturing and using shared security evaluation requirements, based on demonstrable examples of effective use.

[1] In general, each cPP is expected to require one or more SDs to be developed, for example to describe the specific assurance activities for the SFRs and SARs of the cPP. Most references to "cPP" in this document will also have some connection to the SDs. In many places in this document the notation "cPP/SD" is used as a reminder of this fact.

Status and History

Version	Date	Status	Comment
1.0	Oct – 30 2023	Final	Approved by CCMC
0.10	Sep – 21 2023	10th Draft	Incorporating minor changes from CCDB comment period
0.9	Feb – 8 2023	9th Draft	Updating process based on CCDB review
0.8	Oct – 14 2021	8th Draft	Simplifying process based on input from iTCs
0.7	Feb – 28 2014	7th Draft	Further changes from WG discussions; draft prepared for public comment
0.6	Dec – 19 2013	6th Draft	Incorporated changes based on comments received from WG.
0.5	Dec – 13 2013	5th Draft	Incorporated changes based on comments received from WG and other reviewers.
0.4	Feb – 21 2013	4th Draft	Incorporated changes based upon group comments. This draft will be distributed to the CCRA members and the CCUF for comments.
0.3	Feb -14 2013	3rd Draft	Incorporated suggested changes and addressed comments.
0.2	Feb-5 2013	2nd Draft	Incorporated group responses to previous editorial questions and extended content with completed draft of flowchart steps and roles.
0.1	Jan-28 2013	1st Draft	Combined the whitepapers for establishing iTCs and principles for cPP development.

Conventions

Initial Paragraphs with this style indicate text applicable to the early application of the process. Once the process has been demonstrated in practice and suitable reference examples generated, the requirements in these paragraphs may be relaxed (meaning that when the process is mature the paragraph may be ignored). Any such relaxations will be notified via an announcement on the CC portal.

USB Paragraphs with this style indicate text applicable to the initial 'prototype' process that applied to the USB Portable Storage Devices iTC. These paragraphs are intended to capture rationale or lessons that explain the generic process described in the rest of this document.

Terminology

(For general Common Criteria terminology see also Common Criteria part 1.)

Achievable Common Level of Security Assurance	SARs defined in cPPs that produce reasonable, comparable, reproducible, and cost- effective results. It is recognised that all Qualified CBs (as defined in the CCRA) have the potential to certify evaluations against cPPs /SDs. Schemes may or may not use cPPs based on their business need.
CCDB	Common Criteria Development Board – the body that manages the technical aspects of the CCRA, including development and maintenance of the Common Criteria and its associated methodology. The CCDB is also responsible for the development of cPPs by iTCs, and for providing technical advice and recommendations to the CCMC (see the description of the Development Board in the CCRA document).
CCMC	Common Criteria Management Committee – the body that administers the CCRA (as defined in the CCRA document).
CCRA	Common Criteria Recognition Arrangement – see details (including the arrangement document itself) on the Common Criteria portal at www.commoncriteriaportal.org.
CCRA Participant	A signatory to the CCRA.
cPP	Collaborative Protection Profile: a Protection Profile collaboratively developed by an iTC endorsed by the CCMC. A cPP (and related SDs) defines the minimum set of common SFRs and the achievable common level of security assurance. It addresses vulnerability analysis requirements to ensure certified products reach an Achievable Common Level of Security Assurance.

ES	Endorsement Statement (see 'Position Statements and Endorsement Statements').
ESR	Essential Security Requirement (see 'Block 5 CCDB WG ESR Creation' and 'Annex B: The Essential Security Requirements Document').
ICT	Information and Communications Technology
iTC	International Technical Community: a group of technical experts including Participants, Certification/Validation Bodies, ITSEFs, developers and users which are: a) working in manners that promote fair competition; b) working in some specific technical area in order to define cPPs; c) endorsed for this purpose by the Management Committee; and d) establishing interpretations of the application of the CC and CEM necessary for cPPs through SDs which are subject to the CCRA approval process
PS	Position Statement (see 'Position Statements and Endorsement Statements').
SAR	Security Assurance Requirement (see Common Criteria part 1).
SD	Supporting Document: a document that specifies the use of the Common Criteria or Common Methodology for Information Technology Security Evaluation in a particular field or domain of technology. Such documents may be either Mandatory or Guidance and generally specify the interpretations of the CC and/or CEM when necessary. (see the CCMC operating procedure on Supporting documents, MC 2006- 09-003 at www.commoncriteriaportal.org).
SFR	Security Functional Requirement (see Common Criteria part 1).
SPD	Security Problem Definition (see Common Criteria part 1).
WG	Working Group.

Background

The CCRA Management Committee (CCMC) meeting in Paris in September 2012 agreed on a vision statement [Vision] for the future direction of the application of the CC, leading to a revision of the CCRA (see [CCRA]). [Vision] includes a fundamental framework to enable proper management of cPPs intended to be used for procurement purposes in several nations.[2]

Through the vision statement the CCMC expressed the key point that the general security level of general Information and Communications Technology (ICT) COTS certified products needs to be raised without severely impacting price and timely availability of these products. To support that goal, the level of standardization has to be increased by building iTCs that develop cPPs/SDs, in order to reach reasonable, comparable, reproducible and cost-effective evaluation results. Collaboration with product vendors whose products fall within the scope of a cPP is proposed, in order to include state-of-the-art technology, promote fair competition and maximize acceptance of the cPP and the number of compliant products.

Moving to a more PP-centric way of using the CC and CCRA requires harmonization of how cPPs /SDs are developed and applied, in order to

- match the application of CC more specifically to the technical area of the cPP
  ensure that all the CCRA Participants[3] have the opportunity to state their requirements and participate in the development of cPPs that are of interest to them
- ensure that vendors, labs and other stakeholders are given access and an ability to influence the work, and
- avoid unnecessary overlapping cPPs being established for the same technical area.

This document describes the principles for how collaborative Protection Profiles may be developed to address these needs. Fundamentally this is an *enabling process*: it enables security requirements to be clearly stated, agreed amongst the stakeholders involved, and then demonstrably met during the evaluation of products. CC has, of course, always been concerned with the statement of security requirements and evaluation of products against those requirements; this new process is therefore focused on improving the collaboration aspects that lead to more extensive stakeholder agreement, and on providing direct support for implementing [Vision].

When using this process, several stages in the development of a cPP will be open for public review and it is hoped that consensus can be reached at each phase. It is important to note that cPPs/SDs will be managed by an active iTC and will therefore be able to adapt quickly to changes in the technology and its threat environment. If a cPP is unable to include security functionality matching all parties' needs in its current draft, then the iTC provides a vehicle for the evolution of the cPP to encompass more requirements over a planned series of updates. The ultimate goal is to develop the process into a method of choice so that all CCRA Participants will issue ESs (see 'Position Statements and Endorsement Statements' below) for the cPPs of all types of technology for which their government has a national requirement.

This document has been created by the CC Development Board (CCDB) Workgroup tasked to establish a cPP for USB Portable Storage Devices (CCDB USB cPP WG).

[2] Since [Vision] was published, the terminology in this area has moved on. This document distinguishes "international Technical Communities" (iTCs), which are tasked with the production of cPPs, from other general "Technical Communities" that may exist for various other purposes related to a technical area (e.g. standardisation). It should be clear from context which of these cases any particular use of "Technical Communities" in [Vision] refers to.

[3] In this document, the term "CCRA Participants" includes both the certificate-consuming and the certificate-authorising nations

High-Level Process Description

A high-level view of the process of creating an iTC and cPP is shown in Figure 1. This view is discussed below to introduce the main concepts, and then a more detailed step-wise flow is presented in the section 'Process for cPP/SD Development'.

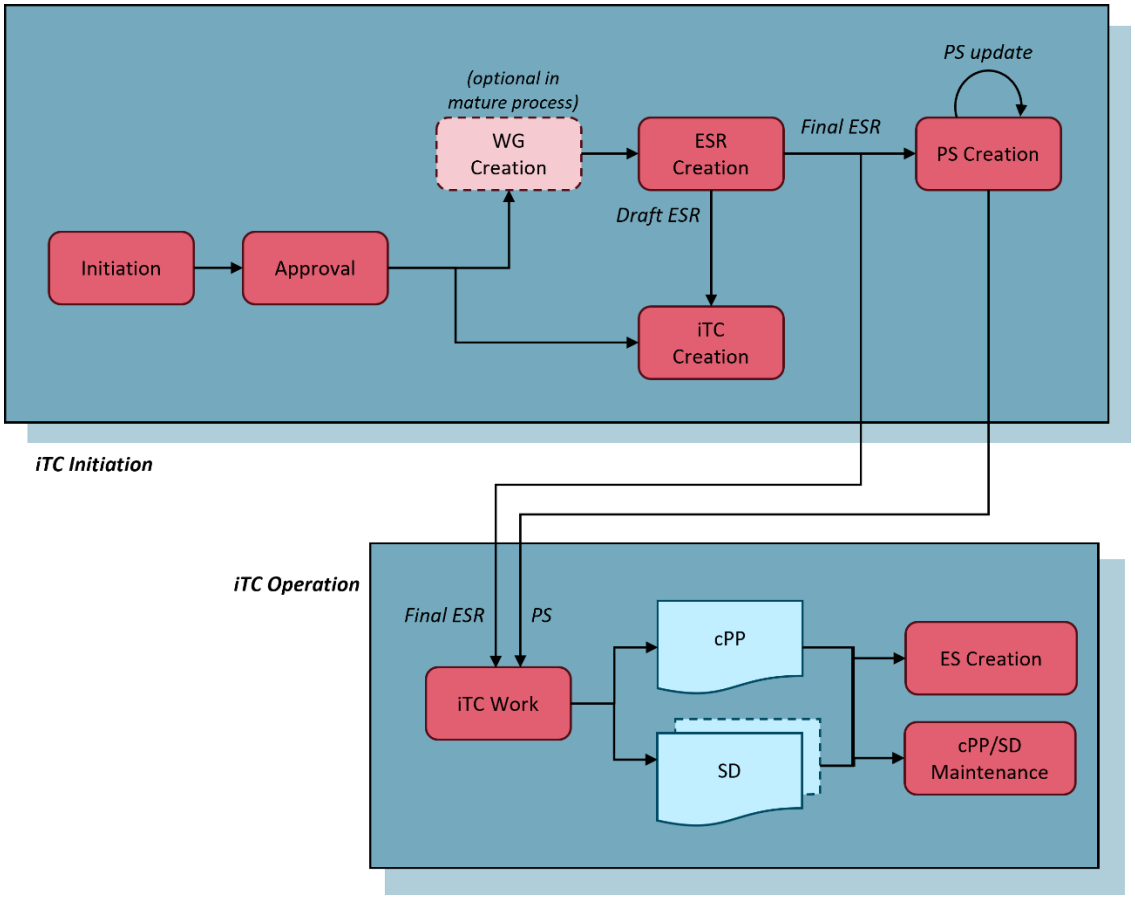

Figure 1:High-Level View of iTC Initiation & Operation[4]

At the Initiation stage, a request is received from an Initiator for the creation of a cPP covering a particular technical area (such as a USB portable storage device). This leads to an Approval stage at which the CCDB determines whether to approve the request (on the basis of criteria as indicated in [CCDB Role]).

The Initiator may be a CCRA participant, or other entities such as an existing Technical Community (TC) may act as Initiators and send requests directly to the CCDB. Assuming that CCDB approval is granted, and the Initiator may carry out the ESR Creation stage.

The ESR Creation stage first produces a draft ESR (see 'Block 4 ESR Creation') that is distributed for comment, and gives an initial basis on which to gather members for an iTC. This in turn leads to the iTC Creation stage in which the Initiator establishes a group with suitable membership, infrastructure, Terms of Reference, and workplan. The iTC is approved by the CCDB, and endorsed by the CCRA Management Committee[5] (both subject to meeting the relevant approval and endorsement criteria).

[4] See 'Terminology' for definition of abbreviations used in the diagrams.

[5] This endorsement of the iTC by the Management Committee is required under Article 2 of the new CCRA in order for cPPs developed by the iTC to be mutually recognised under CCRA.

After addressing comments on the draft ESR, a final ESR is issued, and this forms the main input to the iTC Work stage in which the cPP and one or more SDs for the technical area (abbreviated as "cPP/SD") are created.[6] The final ESR is also the basis for the PS Creation stage in which entities send Position Statements (PS) to the iTC as a way of expressing formal views on the ESR that are also a basis for the iTC to make judgements about the content of the cPP. A PS may be updated by its author at any time.

After a number of detailed steps, involving public review of the emerging cPP content as described in the section 'Process for cPP/SD Development', the iTC publishes its cPP/SD and enters the cPP/SD Maintenance stage. A cPP that has been published in a final form along with its matching SDs is referred to as a 'finalized cPP' (or 'finalized cPP/SD'), and the creation of ESs is requested for the cPP at this point (see the section 'Position Statements and Endorsement Statements' below). In the Maintenance stage the iTC supports the use of the cPP/SD in evaluations, and updates the cPP/SD on the basis of experience with their use and changes in the security context for the technical area (e.g. the appearance of new threats and improved attack methods). Activities in the Maintenance stage are described in [cPP Maint].

Position Statements and Endorsement Statements

An important aspect of the cPP development process is that it encourages each CCRA Participant and other entities involved in policy making, standardization, or procurement (not limited to national government requirements) to make a public statement about their interest in the development and use of each cPP, through the creation of a PS and, after the publication of the cPP/SD, an ES. These statements are intended to make clear the views of the author on the need for the relevant cPP, and the suitability of the the ESR to match their requirements. This enables iTC members to make an informed estimate of the benefits that will justify their participation in the iTC.

At its most general level, a PS allows free-format comment on a cPP/SD, or the interim deliverables from an iTC, but does not represent a formal commitment by its author. By contrast, an ES is a formal statement of commitment to a finalized cPP, with a description of how that commitment is realized (e.g. by listing conformance with the cPP as a mandatory, preferred or recommended procurement requirement for certain types of equipment and/or placing conformant products on an 'approved product list').

Both PSs and ESs may relate to one or more cPPs, in which case the content of the statement must identify to which cPPs it relates.

Initial The precise form and content of PSs and ESs is not specified at present, but it is likely that templates will be created in future (at least for ESs), after initial experiences have indicated the most useful and efficient content.

Both types of statement are public, and at the initial ESR stage (before an iTC has been given responsibility for the cPP) they are sent by their author to the CCDB, which will publish them on the CC portal. In later stages, when the iTC has been established and approved, PS and ES are sent directly to the iTC, which will manage the publication of the statements on the CC portal or an iTC website (indeed it is expected to be a requirement in the iTC ToRs that it will provide timely publication of all statements received) as well as determining whether any further action should be taken in response.

[6] See the CCMC operating procedure on Supporting documents, MC 2006- 09-003.

Initial The initial USB PS/ES have been published on the CC portal, and this is likely to remain the case for *any* PS/ES that are issued on an ESR before the relevant iTC has been formed. Initially all PS/ES will be published on the CC portal (with the iTC taking responsibility for receiving them and requesting their publication), but at a later stage it is possible that the preferred approach will be for the iTC to maintain its own website (linked from the CC portal), and to publish the PS/ES itself.

Because the point of a PS or ES is to provide motivation to product developers and to members of an iTC to invest in the development of cPP/SD and products that conform to the cPP, achieving a significant number of PS's at an early stage (e.g. in response to the ESR) is highly desirable in order to support the formation of a suitably representative iTC. Furthermore, with this iTC-motivation aspect still in mind, the more detail and precision that is put in a PS or ES therefore, the better the iTC will understand the market demand, and thus the more likely it is that the cPP will satisfy the author's needs. Also, the stronger the commitment that can be made in a PS/ES, the more weight its author's requirements are likely to carry in the iTC.

PSs have the following characteristics:

- They can be issued by a CCRA Participant, or any other entity with an interest in adopting the cPP (the PS must therefore clearly identify which entities' views it describes)
- They can be issued at any point after the publication of the draft ESR for comment (see 'Block 4 ESR Creation' below)
- They may express a positive position of support for ESR or for a published cPP/SD, and/or may express the PS author's need for a described change to the cPP/SD
- They may indicate a technical position (e.g. expressing agreement with the content or scope of a cPP) and/or a level of intended support for the use of the cPP in procurement – for example they may include a declaration of the intent to issue an ES when the cPP/SD are published and approved (this would in general be dependent on satisfactory completion of the cPP, but gives the developer an indication of the strength of a PS author's support)
- They can be updated (or withdrawn) at any time in the cPP/SD development process and when the cPP/SD have been finalized.

As noted in the characteristics above, a PS may be 'positive' in expressing the author's support for interim deliverables or a cPP/SD, but may also be 'negative' in the sense that it may describe a need that is not currently being met by the cPP/SD. PSs that express a positive view are seen as very important during the development of a cPP, because they are a public demonstration of an expectation to support the final cPP (although of course this is not a legally binding commitment). This support is an important part of gathering visible commitment to products that conform to the cPP, and is one of the main factors that will encourage and enable developers and other potential iTC members to maintain commitment of their resources to the development of the cPP.

PSs that express a negative view are intended to allow public presentation of an alternative need, and this may result in support from other entities who have previously been silent, but whose needs may be met by a similar change, and who may therefore issue their own PSs expressing a similar need. As a result, the iTC may be made aware of a previously unrecognized need and, if the need represents a market of an appropriate size, then it provides a motivation for the iTC to find a way to accommodate the additional needs. It is not intended that the use of negative PS comments should replace the normal commenting process on interim deliverables, nor the routine discussion of any alternative needs in the iTC

itself – indeed, discussion in the iTC will be the more efficient method of reconciling different needs, and ultimately this is where any changes inspired by a PS will have to be agreed (the PS does not represent a method of commenting that is resolved by any different body: PSs are still managed by the iTC).

Once a draft ESR has been agreed (see 'Block 4 ESR Creation'), all CCRA Participants will be invited to issue a PS relating to the ESR (and the iTC will be open to receiving a PS from any other relevant entity). Updates to the PS are allowed at any points in the cPP/SD development process and when the cPP/SD have been finalized. An updated PS replaces any previous PS by the same author for the same cPP (i.e. it is intended that a reader should only have to consider one PS, or ES, in order to understand the current position of its author on the cPP), although as noted below there may be different PS/ES for each different finalized *version* of the cPP/SD.

When the finalized cPP/SD are available, all CCRA Participants are then invited to make an ES (superseding any previous PS from the same author), which is a formal, public statement of the set of steps that the CCRA Participant will take to express its endorsement of the cPP. These steps will be specific to each CCRA Participant, but examples might include listing conformance with a cPP as a mandatory, preferred or recommended procurement requirement for certain types of equipment and/or placing conformant products on an 'approved product list'. Although the normal and preferred statement on a finalized cPP is in the form of an ES, a CCRA Participant (or other entity) that cannot directly link conformance with a cPP to its procurement policy can continue to express support for a cPP by maintaining a PS. CCRA Participants may co-ordinate a variety of statements from different national policy and procurement organisations so as to capture these in a single PS/ES for the nation, but this is not mandatory (i.e. there may be PS/ES from more than one organization related to the same CCRA Participant).

An ES may include notification of specific national requirements for cryptography, or for inclusion of certain options defined in the cPP/SD. This information is important to enable vendors to understand how they will need to write their Security Target in order to satisfy their target market for a product.

It is expected that initially for each cPP being established, the set of CCRA Participants that issue an ES may be relatively small. However, as the cPP matures, and the number of products that are certified against the cPP increases, the number of nations who find the cPP useful to the extent that an ES becomes appropriate for them is expected to increase. Increasing the number of ESs (and PSs) after a cPP has been finalized is still expected to be useful, not only in making requirements clear to vendors, but also in supporting the future activity of the iTC and maintenance of the cPP.

The PS and ES lifecycle, relative to other iTC activity, is shown in Figure 2.

Initial As noted above, the PS/ES will initially be published directly on the 'CC portal' only- hence the option shown in Figure 2 to publish on an iTC website will not be used until a later stage.

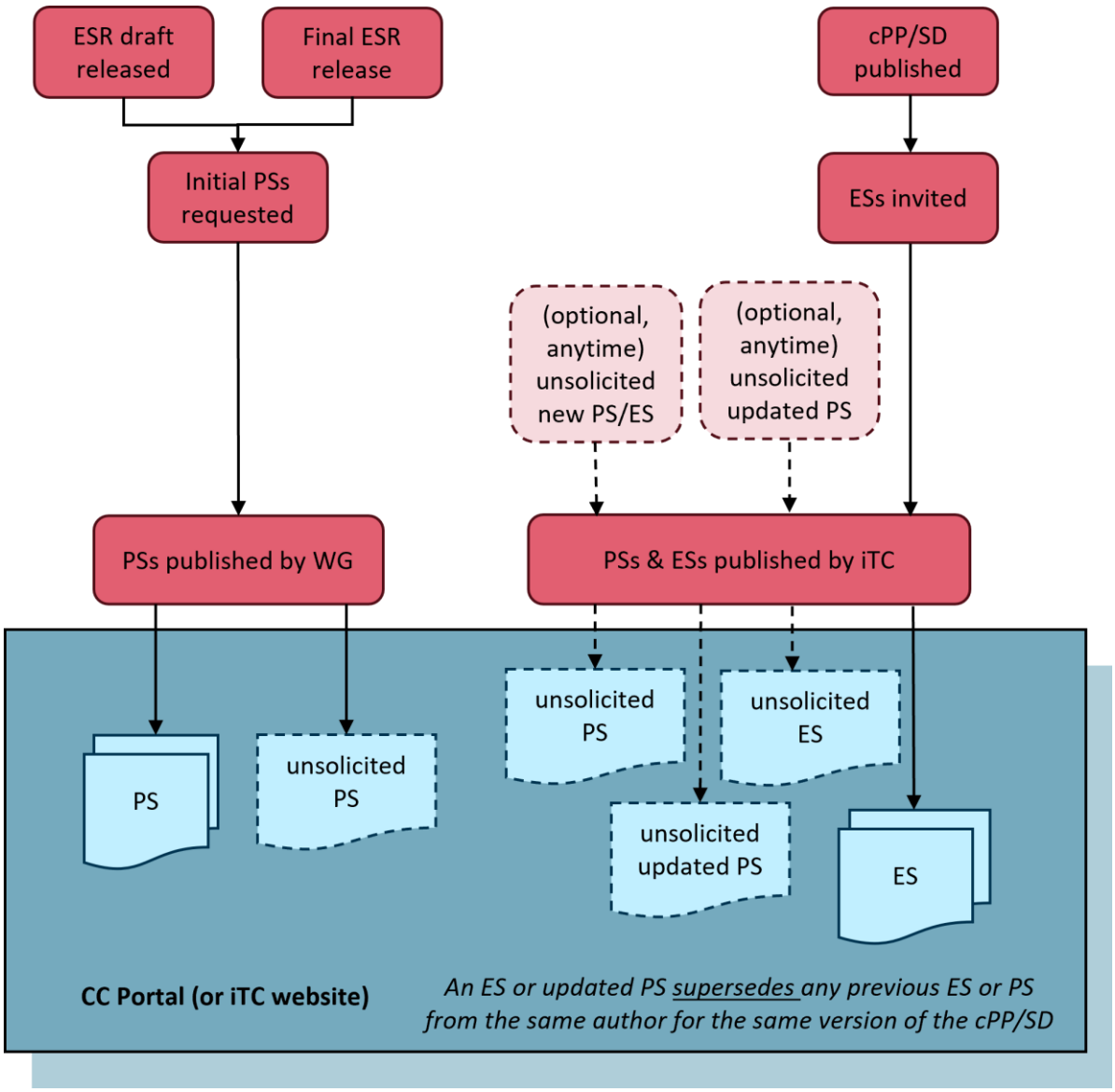

Figure 2: PS and ES lifecycle

It is intended that ESs will not need to be updated until new versions of the cPP/SD are finalized. At this point, the author may issue a new ES relating to the new version(s), and may choose to withdraw the previous ES relating to the old version(s) at any time. Although undesirable, it is also recognized that there may be circumstances where an ES author finds that they need to withdraw an ES (perhaps because the cPP/SD have not been updated but the threat landscape for the technical area has changed). In this case the ES author notifies the iTC, who are responsible for promptly arranging removal of the ES from the CC portal.[7] When an ES is withdrawn, the preferred practice is that it is replaced at the same time with a PS expressing the reason for withdrawal.

In summary:

- A PS will be sought from each CCRA Participant when a new ESR is issued; other entities may also issue PSs at this time; new PSs may be added at any time
- A PS may be updated by its author at any time
- When a cPP/SD are published, then CCRA Participants will be asked to issue an ES.

[7] If the iTC is has become inactive, then the Liaison CCRA Participant should be the point of contact for removal of the ES; failing this, as a last resort the ES author would contact the CCDB directly

USB The USB process initially defined only an ES (originally named "commitment statements") that would be updated as the creation of the cPP progressed.
However, it subsequently became clear that there was a benefit in (a) separating an ability to express less formal 'positions' from recording of more formal 'endorsements' with a stronger link to procurement activities; (b) providing a vehicle for the expression of technical comments that express a desire for changes in the current state of cPP interim deliverables (hence PSs can be 'positive' or 'negative'); and (c) enabling entities other than CCRA Participants to express the same range of views, in both PSs and ESs.

USB A separate Level of Endorsement was also defined for earlier versions of the USB process, in order to capture at an early stage each CCRA Participant's basic attitude to the cPP, and as a simpler, quicker way to express this attitude (i.e. without the need to draft the text for a formal statement). However, it was decided that this was unnecessary when the use of free-format separate PS & ES was defined.

Process for cPP/SD Development

The previous section stated the guiding principles behind the process outlined in the remainder of the document. Figure 3 provides a flow diagram of the process, with the detail of each of the blocks described in the following text. For the sake of clarity Figure 3 does not show all the possible paths through the stages: it represents the main path in which a new iTC is created to create a new cPP.[8]

USB The process described in this paper has evolved from the initial process defined by the CCDB Work Group for USB Portable Storage Devices, and is therefore different from the approach actually followed for the USB iTC.

The iTC is free to decide the details of how they wish to create the cPP and its components (SPD, requirements, etc.) to best suit their needs. The steps described below suggest preferred ways of working that are based on making extensive use of natural language in preference to, or at least as an accompaniment to, CC language. This reflects the importance of achieving a common understanding of the meaning and intended application of the CC language amongst an iTC that is likely to include end-users and/or risk-owners who may not be so familiar with the CC language but have an important contribution to make in ensuring that the cPP will be appropriate for use. However, beyond following the sequence of process steps, the use of natural language in this way is guidance and is not mandatory.

Block 1 Initiator Requests cPP

To begin the process an entity, referred to as the "Initiator", submits a request to the CCDB for the development of a cPP for a specific technical area. This request should contain a justification of the need for a cPP and provides a high level description (a paragraph or two) of the security problem the resulting cPP would address. The request should also contain an approximate time-frame in which the Initiator would like to see a cPP completed so that their expectations are known. Where there is an apparently similar cPP already in existence or in development, then the cPP Initiator should provide a rationale that demonstrates the need for an additional cPP (as opposed to updating the existing cPP).

The Initiator does not have to be a CCRA Participant. Other entities such as existing TCs

[8] So, for example, the path where the cPP is assigned to an existing iTC at the ESR stage is described in the text but not indicated by arrows between the relevant blocks in Figure 3.

may act as Initiators and send requests directly to the CCDB.

Although the security problem description required at this stage is not a complete ESR, Initiators may nevertheless choose to submit a draft ESR as part of their request. Assuming that the request is approved, this may enable process steps up to the creation of the ESR (block 4) to be completed more quickly, but an ESR will only be accepted in this way on the understanding that it is a draft and is subject to revision. This follows from the role of the ESR as a consensus-forming document that is open to as wide a range of procurement and risk owners as possible.

Block 2/3 CCDB Determines cPP Need

When the CCDB receives the request, it checks whether a cPP currently exists (or has already been initiated under this process) that would address the security problem presented by the Initiator (this is discussed further in [CCDB Role]). If the CCDB determines that such a cPP exists, the CCDB would inform the Initiator that they feel the existing (or already initiated) cPP is suitable to address the Initiator's needs. The Initiator would have an opportunity to respond and either convince the CCDB otherwise or find an alternative approach. If the CCDB then agrees that the other cPP does not adequately address the Initiator's needs, they may nonetheless believe that those needs could be accommodated by an extension of scope or maintenance cycle of the other cPP. In this case the CCDB would contact the iTC responsible for the cPP to propose the extension of their scope, and the Initiator would then directly engage with the iTC (typically by joining the iTC).[9] As part of this discussion, the CCDB may agree additional liaison activities and representatives with the existing iTC to cover the new cPP (this may also require some changes to the membership and ToR of the iTC in order to meet the requirements for authority and openness – see the discussion under 'Block 11 iTC ToR Created/CCDB Approval and CCMC Endorsement/Liaison CCRA Participant Appointed' below).

If a relevant cPP cannot be identified at the time, the CCDB consults the CCRA Participants to determine interest in the development of such a cPP (where interest would be based on an identification of a current or future need by each CCRA Participant). If there is insufficient interest then the CCDB informs the Initiator, who then is left to find an alternative solution. Alternatives could include redefining the security problem to generate more interest, developing a National Scheme PP instead of a cPP, or simply abandoning the request for the time being.

[9] If the iTC rejects the proposed extension then this will be addressed on a case-by-case basis by the CCDB, who may of course then decide to form a new iTC for the new cPP, but the CCDB will also have to consider how to manage any expected overlap in SDs (for example, the SD for the existing iTC might need to be split to allow a generic shared SD for applying evaluation requirements to the common areas and separate SDs for more detailed aspects that are specific to each of the two cPPs).

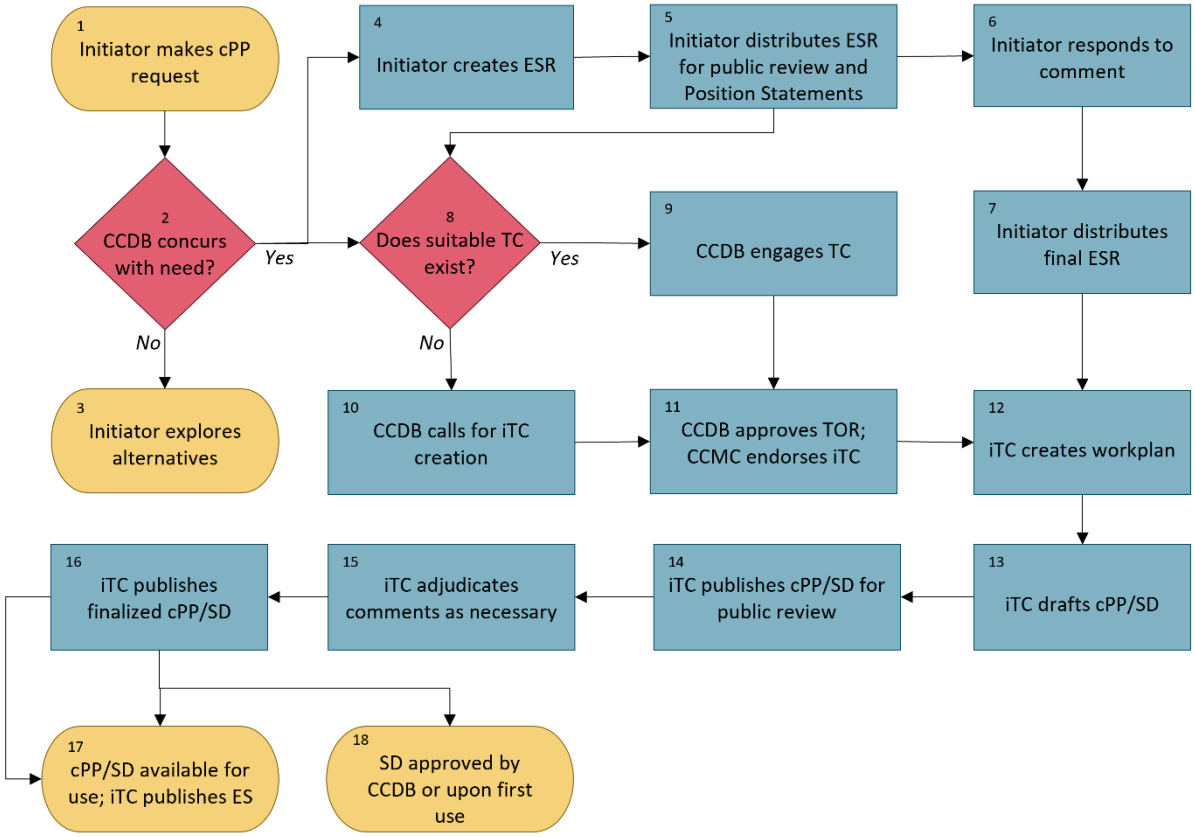

Figure 3: Process Flow Diagram for cPP Development

When the CCDB has determined that there is a need for a cPP, it directs the Initiator to create an ESR document.

Block 4 Initiator Creates ESR

The Initiator (typically an existing TC) creates the ESR and requests membership to help establish the iTC. The description below summarizes the principles behind the ESR, as well as giving a rationale for its need (more details of the ESR are given in Annex B). In order to allow creation of cPPs that are used for procurement purposes in several (ultimately all) nations that are signatories of the CCRA, it is necessary for appropriate government authorities of those nations to provide a common set of harmonized security requirements for products that are to be procured. Such appropriate government authorities may be the same as the ones representing the respective nation as their CCRA Participants (i.e. those that participate directly in CCRA management and execution activities). However, it should be expected that for many technical areas, other governmental authorities from the CCRA Participant's nation may need to be involved in the work. Each CCRA Participant is therefore expected to inform other appropriate government authorities about the work on particular cPPs that may be relevant.

Each Initiator member is encouraged to coordinate the positions of its own government authorities in order to present a unified national view in the international discussions for harmonizing the security requirements for each particular cPP. Similar principles apply where a Initator member represents an entity other than a nation: the Initiator member is encouraged to coordinate the positions of any of its constituents that have independent policy and procurement requirements. Coordination of independent constituencies in this way is expected to give the requirements of the Initiator member (or, in the later stages, the iTC member) more weight, because the product developers can recognize the larger market associated with the requirement.

The ESR is a natural language document (i.e. avoiding CC abbreviations and constructs) that scopes and bounds the security problem for the cPP by defining a set of use cases, assets and threats. It then identifies both general and, when appropriate, specific requirements with which an ICT product of this type must comply in order to satisfy the Initiator members' procurement guidance and/or technical regulations. The intent is that the ESR will allow the iTC flexibility to craft SFRs in a manner that makes sense to that community, given that the iTC members represent *expertise* in that technical area. In the course of creating the ESR, the Initiator members may continue to collect input from other government agencies, vendors, or other relevant parties, whilst noting that some of the contributions from these parties may be more appropriately addressed by the iTC when the cPP is developed, rather than in the creation of the ESR.

More detail on the content of an ESR is given in Annex B.

It is possible that the process of producing the ESR may indicate that the cPP would in fact be best addressed within an existing iTC rather than by creating a new iTC. In this case the Initiator may report this finding to the CCDB and the CCDB, if it agrees with the conclusion, may then contact the relevant iTC to propose an expansion of scope, as in 'Block 2/3 CCDB/Initiator cPP Need Determined' above.

Block 5/6/7 Initiator Distributes Draft ESR for Review/Initiator Finalizes ESR

At this stage the Initiator distributes the draft ESR for public review to solicit comments and to ask for PSs from at least the CCRA Participants (see 'Position Statements and Endorsement Statements' above).

USB In the USB case, initial drafts of the ESR were distributed to all CCRA Participants and provided a useful way of increasing the WG membership. Comments and PSs on the ESR were solicited only from the CCRA Participants, although the ESR was also distributed more widely through the CCUF.

CCRA Participants are not *required* to respond to the draft ESR, but it is hoped that all will provide a PS at least by the time the ESR is finalized. The Initiator adjudicates the comments received, in a way that arrives at a consensus among the Initiator members (according to the decision process defined in the terms of reference). While the comment resolution process can be a lengthy and time consuming process, the Initiator nevertheless attempts to respond to all comments against the ESR. This is encouraged as at least a courtesy, acknowledging the time and effort taken to review a document and submit comments. The ultimate goal of the comment resolution process is to reach consensus among as many potential supporters of the cPP (nations and others) as possible.

There may be some comments that are not adequately resolved in the eyes of the body that submitted the comments, but where the commenting body feels that it cannot use the expected cPP in its policy and procurement. Any such formal comments and/or opposition to the contents of the ESR may be recorded by the commenting body in a PS that it sends to the Initiator, and which the Initiator is then required to provide to the iTC along with the ESR. It is then left to the iTC to determine how they wish to proceed. It is important to note that entities expressing such comments in a PS are not excluded from participation in the iTC and its work – indeed, it is hoped that their participation may enable the iTC to identify ways to address their additional or alternative requirements in the cPP in future, even if they cannot be agreed at the ESR stage.

Before finalization, the ESR must also be released into the public domain, allowing a wider range of comments to be received (including from entities such as vendors and evaluation laboratories, who may later form part of the iTC). This review may be combined with the review by CCRA Participants described above, or may be carried out after the CCRA

Participants' review. The Initiator is not required to accommodate or respond formally to comments from this wider review audience, although of course it may choose to do so. As noted above for residual comments from CCRA Participants, the Initiator may decide that most or all of the public comments would be better addressed subsequently within the wider membership of the iTC. The finalized version of the ESR should then be released into the public domain.

The finalization of the ESR is the next stage at which PSs are actively sought from CCRA Participants (and possibly other entities).

Block 8/9/10 CCDB Engages iTC

These stages represent the activity sequence that results in an iTC that is ready to take on the cPP development. The activity sequence is carried out mainly by the Initiator, and takes place in parallel with the ESR development. The Initiator determines the best course of action with respect to engaging an existing TC or creating a new iTC to develop the new cPP. The Initiator should consult with the CCDB chair (who will decide as to what wider consultation within the CCDB and CCMC is appropriate for the particular cPP), and with vendors of the relevant technical area, to help in this determination. The Initiator should also consider the potential for involvement of any relevant standards bodies for the technical area. The general approach will be for the Initiator to identify an initial group of suitable iTC members and to carry out some initial discussions, and for the CCDB to issue a formal invitation to the relevant bodies to create (or become) an iTC.

If one or more potentially suitable TCs already exist (e.g. an industry body with an existing security/CC remit), then the Initiator (or CCDB representative) will be given responsibility for initiating contact to determine whether a working relationship can be established. In some cases, an existing TC may be neither willing nor able to engage with the Initiator and CCDB[10] at the necessary time to construct a cPP. In this case, the Initiator (possibly with CCDB assistance) may have to create a new iTC, and members from an existing TC may then also elect to participate in the iTC. In other cases, the TC may be willing and able to take on the responsibility of creating a cPP and operating under the constraints levied by the CCRA and [Vision], and so the CCDB will formally invite the TC (subject to approval by the CCDB and endorsement by the CCMC as in block 11) to take on the cPP creation task, in which case the TC will therefore be recognized as an iTC for these purposes.

Another possibility is that the Initiator or CCDB may decide that the new cPP would be suitably developed under an existing iTC that was previously formed to develop some other cPP, but that also volunteers to develop the new cPP. In this case the CCDB will contact the iTC to propose an expansion of its scope, as discussed in 'Block 2/3 CCDB/Initiator cPP Need Determined' above.

If a suitable TC cannot be found to develop a cPP, then the Initiator assists the CCDB in creating a new iTC. The Initiator may contact potential iTC members in order to bring together a suitable initial group of members, who can then take on the task of forming the iTC. Care must be taken at this stage to balance the number of initial members that can reasonably be involved in forming the iTC against the number of members intended for the full iTC. The need to communicate with an initial group, before it has formed a single iTC identity with suitable points of contact (such as a Chair and a Liaison CCRA Participant) means that the initial group may have to be significantly smaller than is intended for the full iTC. The Initiator shall therefore seek to ensure that the later members will not be significantly disadvantaged, for example in terms of influence over the cPP/SD or the iTC

[10] Although initial contact with the iTC may be made by the Initiator, there will usually be an ongoing relationship with the CCDB to allow monitoring of iTC progress against its workplan.

terms of reference, accrues to the initial members but not to the other members of the fully formed iTC. Although it is a defining characteristic of the initial members that they are willing to put in place an infrastructure on which to base a full iTC, the initial members should not be allowed to start formally recognized work on the cPP until a suitably representative iTC membership has been achieved. The criterion of a suitably representative membership will be part of the CCDB review of the iTC proposed ToR in 'Block 11 iTC ToR Created/CCDB Approval and CCMC Endorsement/Liaison CCRA Participant Appointed'.


In the USB case, an initial group of 3 developers were contacted. This group established a developer organization (the Secure USB Alliance) with a web presence from which to further develop the iTC.

Although the Initiator carries out many of the tasks involved in bringing together the initial iTC members, the formal invitation to form an iTC is issued by the CCDB. The invitation is published on the Common Criteria portal as well as distributed to all CCRA Participants and other groups such as the CCUF, with the intention that these recipients will help to find further candidates for membership of the iTC. It is also envisioned of course that some CCRA Participants would participate in the iTC.

Block 11 CCDB Approves iTC ToR/CCMC Endorses iTC/iTC Appoints Liaison CCRA Participant

When the iTC initial membership has been established, then a ToR guidance document (see [ToR Guide]) will be used by the iTC to generate a ToR specific to that iTC. Before the iTC can be formally invited to create the cPP/SD by the CCDB, the ToR must be submitted by the candidate iTC and reviewed by the CCDB until they meet the criteria set down in [CCDB Role], at which point the CCDB will approve the ToR and recommend to the CCMC that it endorse the iTC. This endorsement of the iTC by the CCMC is a critical requirement for international recognition of products claiming conformance to the cPP under CCRA (see footnote 5), and it is therefore important to note that such endorsement must therefore be maintained by the iTC (see [CCMC Role] for further information on what is necessary to maintain CCMC endorsement).

The iTC will also need to follow the general requirements on cPPs that are defined in Annex K of the CCRA and, in accordance with the CCRA definition of an iTC (see [CCRA, Annex A]), to work in a way that is open and promotes fair competition. This means that the iTC's terms of reference must implement the '6 principles' in [WTO6], which are summarized as follows:

- Transparency: making the essential information relating to the creation of the cPP available to all interested parties, along with adequate time and opportunity to provide written comments
- Openness: making membership of the iTC open to all relevant bodies
- Impartiality and Consensus: providing all relevant bodies with meaningful opportunities to contribute to the cPP, such that the process avoids giving privilege or favour to some members over others
- Effectiveness and Relevance: the cPP to be developed needs to be relevant and to effectively respond to regulatory and market needs (as indicated by the ESR), without distorting the global market, having adverse effects on fair competition, or stifling innovation and technological development
- Coherence: the cPP to be developed needs to avoid unnecessary duplication of, or overlap with, other cPPs
- Development Dimension: constraints on developing countries, in particular, to effectively participate in cPP development, should be taken into consideration in the development process.

In practice, as part of the commitment to openness and impartiality, it will also be a requirement that the iTC should have the participation of at least two vendors of the technical area.

As another part of the formal recognition of the iTC, a Liaison CCRA Participant is appointed by the CCDB to act as a formal point of contact between the iTC and CCDB.

Block 12 iTC Creates Workplan

Once the iTC has been formally approved the CCDB formally passes to it the ESR, any PS received so far, and any additional constraints the CCDB feels are necessary. An example of such a constraint might be to identify certain existing or emerging SDs that should be adopted by the new cPP. It is also possible that the constraints may further limit the scope of the cPP 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 supports the objective of avoiding overlapping cPPs.

At this point the approval of the iTC is recognised by creating an entry for the iTC (or expanding the entry of an existing iTC) on the CC portal including the name of the iTC, its contact details, its initial membership, the ESR, and any PS received. Changes to the CC portal entry for an iTC will be requested from the CC portal administrator by the Liaison CCRA Participant.

It is noted that, although it receives the ESR and other initial inputs from the CCDB, the iTC is responsible for the cPP(s) that it establishes. All decisions about the ultimate content of a cPP belong to the iTC, although the associated SDs (which include the assurance activities for the cPP) must be approved by the CCDB.[11] The iTC is expected to fulfill the ESR provided by the Initiator, or else the cPP may have little value as products evaluated against it may not have widespread endorsement for procurement. However, there will be no need for formal approval of the cPP from the CCDB, nor from the CCRA committees. This is intended to ensure that the iTC members have a justified sense of ownership of the cPP content, and to avoid a situation where various interactions and approvals from CCRA bodies could hinder the iTC's ability to develop the cPPs in a timely manner.

The primary objective at this step in the process is to construct a workplan giving the schedule for producing the cPP/SD and identifying critical milestones. The iTC should, in particular, address the need to avoid rejection of SDs at a late stage, by agreeing with the CCDB chair an appropriate set of monitoring and/or review steps.

Block 13 iTC Creates Draft cPP/SD

The cPP is based off of the SPD and iTC requirements, but these do not need to be released for separate formal comment periods.

The SPD for the cPP is created by the members of the iTC, according to the workplan. As noted above, this is intended to be based on the ESR and other initial inputs from the CCDB, but the cPP content is now the responsibility of the iTC, with no further formal approval required from the CCDB .

[11] The *need* for any *mandatory* SD is first approved by the CCMC; the content of the SD is then approved by the CCDB, as described in the CCMC operating procedure on Supporting documents, MC 2006- 09-003, or certified upon first use.

It is expected that the SPD will be written largely in a natural language prose style and will avoid relying solely on CC formalisms (such as implicit definition of the threat detail via its mapping to security objectives). The goal is that the SPD will be readable to a wide audience and that extensive experience with the CC is not necessary to understand and review the problem being addressed by the cPP.

CCRA Participants are able to present their detailed views and requirements (refining the high-level requirements that were put into the ESR) to the iTC during cPP development. This will include any specific national requirements that need to be accommodated in the cPP (e.g. via optional packages, or constraints on how SFR assignments and selections are specified in the cPP).[12] Ideally this would be done by direct participation in iTC activities, but less resource-intensive opportunities are available via any other review stages that the iTC may decide to offer. Since the iTC is intended to be a technical forum, CCRA Participants may delegate their attendance at the iTC to other relevant organisations more directly concerned with the technical area.

The CCDB (and CCMC) will keep the scope of the iTC and its cPP(s) under continuous review, and may intervene if this scope has expanded from the original remit and/or has developed overlap with another cPP without CCDB approval and CCMC endorsement. This could potentially lead to CCMC endorsement of the iTC for one or more of its cPPs being withdrawn. However, it is also recognized that there will be cases where authorization for expansion of the iTC remit needs to be approved and endorsed. The preferred course is therefore for the iTC itself to request any such expansion through the CCDB.

The security objectives and SFRs for the cPP are created from the previous SPD definition, once again applying the principles in [Vision]. As with the SPD, when crafting the requirements, it is important that the iTC make as much use as possible of natural language, in order to make the requirements intelligible to readers who are not CC experts. Natural language should be used, for example, to make the scope and application of SFRs clear (e.g. the use of different SFRs for different types of user or connection, or the types of user data that an SFR is expected to apply to). When crafting the requirements care should be taken to be as specific as possible and consider what would constitute not only the pass or fail *criteria*, but what *activities* would be performed to determine whether a product satisfies, or fails to meet, a requirement – these will ultimately lead to the assurance activities that are included in SDs associated with the cPP.

One hazard in developing a natural language version of the requirements and gaining consensus among a wide audience – many of whom may not be CC experts – is that when the translation to SFRs is made, the original intent is lost. The iTC should take this into consideration and determine the proper approach for the cPP development. They may decide to develop a set of natural language requirements in conjunction with CC SFRs to have them examined together to minimize potential divergence.

It is also important that the requirements capture the minimum set of requirements that are agreed as necessary by users and risk owners for the technical area and that can gain a consensus among the iTC members (acknowledging of course that the iTC may apply decision and voting criteria as in its ToR where unanimity cannot be achieved). However, consistent with the approach described for the ESR in Annex B, the iTC also has the ability to specify requirements that are optional because they are considered beyond the minimum set of necessary security functionality.

[12] It is noted that any such national requirements will need to conform to the requirement (in CCRA annex K) that cPPs shall not contain requirements that have a dependency on national conformity assessment schemes if mutual recognition is to be achieved.

This stage will also see the drafting of SDs to describe the evaluation methodology and application of the CC SARs to the specific technical area in determining conformance with the cPP – these include the assurance activities for SFRs and SARs in the cPP. The iTC considers the SARs that are contained in the cPP guidance (see [cPP Guide]), which are considered the baseline level of assurance that the methodology in the SDs is intended to satisfy. The iTC has the authority to modify this baseline as necessary to address the SPD and what makes sense for the given technical area. However, it must be noted that the CCDB is the ultimate approval authority for any SDs generated in conjunction with the cPP, and any deviation from the baseline SARs will require a justification, which includes a rationale as to how [Vision] and [CCRA, Article 2] are maintained.

Since writing the assurance activities that an evaluator is expected to perform in order to determine compliance with an SFR may also cause the expression of the SFR to be reconsidered, it is important that the iTC attempt to write the assurance activities in parallel with requirement/SFR creation.

Once the SPD and requirements are finalized and stable, the iTC completes the initial draft of the cPP by taking the natural language prose expression of requirements and creating a CC-compliant protection profile. This will require the cPP to address all the rules of PP construction (as defined in CC part 1 and the APE criteria in CEM) and includes the appropriate mapping and rationale sections.

When specifying the requirements in the appropriate CC language, care must be taken to limit the use of open assignments in SFRs whenever possible. Limiting the scope of an SFR is important when specifying the objective and repeatable evaluation activities to be performed when determining product compliance with an SFR. If a completely open assignment is included then it is challenging to address the variety of potential implementation choices that might be made by an ST author; it is preferable to use a selection, where the scope of options is constrained and assurance activities can address each potential selection made by the ST author, or at least to include in the assignment a rule that narrows the ‘variable’ to a predictable and recognisable range of values.

As stated earlier, there will be a baseline set of SARs that will form the basis for the evaluation methodology that will be expressed in the SDs. The SDs or at least the assurance activities dealing with evaluator actions to assess the product against the requirements should be drafted in parallel with functional requirement development. However, after the SFRs are completed, the SDs are finalized. It is likely that many of the interpretations and assurance activities will have emerged during the creation of the SFRs themselves, but this stage represents the preparation of a complete draft CC SD to contain them and put them into the context of the cPP.

The SDs define interpretations and refinements of CC and the CEM that are to be used in evaluating products that claim conformance with the cPP. The objective in all cases will be to interpret and refine the CC requirements and methodology to be appropriate for the technical area. The SDs are a vital part of achieving the reasonable, comparable, reproducible and cost-effective evaluation results referred to in [Vision].

Block 14/15/16 iTC/Public cPP/SD Finalized and Published

The iTC makes completed cPP/SD versions available for public review on the CC portal, with a defined deadline for receipt of comments. This release of the draft cPP typically is made at the same time as the release of the draft SDs. The intention is that the draft cPP and the draft SDs can each be reviewed with reference to the other.

Although there is no formal approval of the cPP required by the CCDB, comments regarding the consistency of the cPP with the ‘Baseline requirements’ in [Vision] are important at this

stage.

The iTC should respond to all authors of comments received, acknowledging receipt and indicating the results of processing the comments.

Note that the cPP will only be available for use in evaluations after the related SDs have also been finalized and published

Block 17/18 iTC/Public/CCDB Supporting Documents Finalized and Published

When the cPP/SD have been finalized and published, they are available for use and the iTC will ask for ESs for the cPP/SDs. The SDs undergo a formal CCDB review and approval, but they do not have to wait for CCDB approval to be available for use.. The CCDB review of the SDs will be concerned with establishing that the content of the documents supports the objectives of [Vision], and that they are consistent with other SDs.

In addition to this process, the cPP/SD is also to be evaluated and certified against the CC APE criteria. This can be done either before the first use of the cPP in a TOE evaluation, or may be carried out during the first use of the cPP.

At this stage the iTC is expected to continue to exist, and to provide support for the use of the cPP in TOE evaluations (e.g. by supporting and collating interpretations that are found necessary in TOE evaluations, and producing updated versions of the cPP/SD to reflect experience of their use, and changes in the technical area and threats). This maintenance activity is addressed in [cPP Maint].

References

[CCDB Role]	***[*Reference to a document that describes the details regarding the CCDB's participation in this process. Note that in some areas this may overlap with [ToR Guide] below. It is likely that [CCDB Role] will take the form of an Operating Procedure which will initially include more restrictions than expected for the mature process. These restrictions will be relaxed as good examples of mature cPPs and iTCs appear.]***
[CCMC Role]	***[*Reference to a document that describes the details regarding the CCMC's participation in this process. Like [CCDB Role], this is likely to take the form of an Operating Procedure.]***
[CCRA]	Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security, 2 July 2014
[cPP Maint]	***[*Reference to a document that describes the details of cPP/SD maintenance activities.]***
[cPP Guide]	***[*Reference to another new guidance document to be created. This is likely to be a CC SD, and it is expected that it will provide the structure of a cPP and provide guidance concerning the contents of each section. The reference document will also provide the baseline SARs, that in conjunction with the SFRs, will guide the development of the assurance activities specified in the SDs to be created for the new cPP.]***
[ESR Temp]	***[*Reference to the ESR Template, which currently exists as the file 'ESR-Template v0.2.docx']***

[ToR Guide]	***[*Reference to a new guidance document to be created, probably in the form of a CCRA Operating Procedure. This guidance will reference the CCUF ToR guidelines, and will note certain requirements for applying this to iTCs. For example, it will be required to reference the WTO 6 principles, and to establish sufficient representation in the iTC membership both in terms of types of participant (CCRA Participants, labs, developers, risk owners/relying-parties) and the numbers of each (relative to the technical area). The CCRA Operating Procedure will be subject to CCDB review and CCMC approval.]***
	[*It is also intended to create a library of iTC ToR, to help new iTCs to quickly establish a set of approved ToR.]
[Vision]	Vision statement for the future direction of the application of the CC and the CCRA, 2012-09-001, v2.0, September 2012
[WTO6]	G/TBT/1/Rev.9 (8 September 2008) "DECISIONS AND RECOMMENDATIONS ADOPTED BY THE WTO COMMITTEE ON TECHNICAL BARRIERS TO TRADE SINCE 1 JANUARY 1995"

Annex A Roles and Responsibilities

The roles and responsibilities of each active entity are described above throughout the process flow description. The intent of this Annex is to succinctly capture the roles and responsibilities for each group in one place.

The role of the CCRA Management Committee

The CCRA Management Committee is responsible for:

- Oversight of the iTC and cPP process according to [Vision] and [CCRA]
- Endorsing an iTC (following approval of the iTC and its ToR by the CCDB)
- Approving the need for new mandatory SDs for technical areas or domains requested by the CCDB (cf. CCMC operating procedure on Supporting documents, MC 2006- 09-003).

The role of the CC Development Board

The CCDB is responsible for:

- Approving requests for new cPPs and allocating the development of approved cPPs to iTCs (block 2/3 & block 8/9/10)
- (CCDB chair) Responding to Initiator consultations regarding engaging or creating an iTC (block 8/9/10)
- Suggesting to the CCMC the establishment of new technical domains for mandatory SDs, and providing an appropriate rationale (when the need for SD is identified as a result of activities in other blocks)
- Issuing the formal call for members and invitation to form an iTC (block 8/9/10)
- Providing the ToR guidance [ToR Guide] that is given to a potential new iTC (block 11)
- Reviewing and approving iTC ToR and, when appropriate, recommending to the CCMC that the iTC should be endorsed (block 11)
- Providing the ESR to the iTC to enable work to start on the cPP (block 12)
- Appointing a Liaison CCRA Participant for each iTC
- Monitoring the progress of each cPP against its workplan, via reports from the Liaison CCRA Participant in each iTC (block 11) (block 12)
- Reviewing and approving the content of SDs drafted by iTCs (block 18).

Although it does not control or direct the iTC, the CCDB may also attempt to resolve issues arising during the development of a cPP that threaten to lower the level of cPP/SD support from a CCRA nation.

In cases where an iTC has become inactive and its cPP is not being used, the CCDB may also decide to set a sunset date for the cPP, after which it will be withdrawn (i.e. it will no longer be recognized and accepted for use in evaluations).

Another document [CCDB Role] describes in more detail the responsibility of the CCDB in this process, as well as formalizing the communications that are necessary to ensure that the CCDB is kept informed of the material activities being performed by the iTC and that the iTC is fully aware of its standing with the CCDB (e.g., the iTC is made aware of any issues the CCDB may have with the progress or stances taken by the iTC, or is made aware that the CCDB is comfortable with the status and progress being made towards the cPP).

The role of the Initiator

The Initiator is responsible for:

- Submitting a request that rationalizes a need for a cPP, in which there may be multiple CCRA Participants or other entities that work together to submit a joint request (block 1)
- Following up on the initial request if asked by the CCDB (block 2)
- Examining alternatives if the CCDB does not concur with the need (block 3)
- Creating the ESR for a cPP as indicated in Annex B, distributing it for public comment, responding to comments, and distributing the final ESR (blocks 4/5/6/7)
- Making the initial contact with potential members of the iTC that will develop the cPP (as described for block 8/9/10/11)

The role of the Liaison CCRA Participant

The Liaison CCRA Participant is responsible for ensuring that liaison activities with the CCDB (such as reporting) take place, and for receiving and executing instructions from the CCDB. In general the liaison activities will be:

- Communication of the workplan from the iTC to the CCDB
- 6-monthly written report (possibly including a presentation) to the CCDB on the activities, level of participation, and progress against objectives and the workplan. The report should also include key topics of debate/dissent, changes in ToR or membership of the iTC (identifying any concerns that this may raise over whether membership is still sufficiently representative, or deviation from other requirements in [ToR Guide]) and any other notable inputs
- Solicitation and gathering of comments on documents or answers to questions that require wider CCDB/CCMC input (i.e. those documents/questions that include matters outside the remit of the iTC and its member CCRA Participants alone)
- Notifying to the CC portal administrator any changes in information presented for the iTC on the CC portal
- Notifying to the CCDB any changes in support for the cPP/SD (mainly as represented in PSs) arising from iTC work
- Transfer of formal deliverables from iTC level to CCDB/CCMC level (e.g. SDs that need to be formally issued)
- Gathering requirements for future cPP updates from CCRA Participants.

The Liaison CCRA Participant also acts as the point of contact for an iTC that has become inactive. Inactivity would be notified to the CCDB in the routine reporting from the Liaison CCRA Participant, and the Liaison CCRA Participant will then be the formal point of contact for the iTC until a decision on the actions required is taken by the CCDB.

The role of the iTC

Ultimately, the role of the iTC is to create a cPP that minimizes the number of negative PSs, and maximizes the number of ESs and positive PSs. This, of course, is operating within the constraints levied by the CCDB (e.g., ESR, approved ToR, SD). The role of the iTC is to:

- Create a ToR and submit to the CCDB for approval
- Follow the principles and procedures described in this document, and the conditions

for iTC described in the Vision statement and the CCRA
- Create a Workplan that provides a schedule and identifies critical milestones
- Support the Liaison CCRA Participant (or their representative) in their interactions with the CCDB
- Create a cPP/SDs, submit for public review, and resolve comments
- Carry out maintenance activities to support cPP usage and to create updates to the cPP/SD.

Annex B The Essential Security Requirements Document

The ESR for a cPP is developed by the Initiator once a need for the cPP has been established. Its main purpose is to provide an iTC with a consensus statement of security requirements from customers and risk owners, on which a set of PSs have been based. A draft ESR may be used by an Initiator to describe the requirement for a new proposed cPP at step 1 of the process, but this would be more than is required for initiation, and in such a case it would be necessary that the ESR is adopted only as a draft that is subject to revision by the initial members of the potential iTC in order to achieve the necessary consensus. The role and the high-level characteristics of an ESR are described as part of the 'ESR Creation' block in the main document. This annex gives more detail about the content of an ESR – a template [ESR Temp] is also available.

Note that the text below describes the ESR as representing mainly the views of the initial potential iTC members who create it. However, this should be understood to include also those views that may be expressed by other entities *through* an initial potential iTC member, and those views that arise from feedback obtained from outside comments on ESR drafts.

Some of the following text reflected the initial limitation that initial members would be composed only of CCRA Participants. However, the statements are more generally applicable now that this requirement is removed, at least when taking into account that CCRA Participants (representing their national governments) will usually be a significant part of the user community for most cPPs.

Harmonizing security requirements on a detailed technical level between several initial potential iTC members is obviously difficult, and risks delaying the cPP progress, for two reasons. First: the work will become highly technical and the CCRA Participants may not have enough resources to work through the requirements for a large set of cPPs concurrently. Second: the adoption of the security requirement should be based on achieving as near unanimity of the initial potential iTC members as possible. Hence the text representing the harmonized security requirements of the initial potential iTC members needs to be expressed in a way that will allow a general consensus on the high level requirements, whilst deferring the detail to expert discussion in the iTC. Both problems are therefore addressed by defining the characteristics of a document needed to present the *high level* cPP requirements to the iTC. The document ensures that the detail that gives rise to the first problem is deferred to the iTC discussions, and that its contents are capable of describing all of the critical national requirements related to the second problem. This document is called the ESR.

The ESR scopes and bounds the initial potential iTC members' view of the security problem for the cPP. This is accomplished by defining the use cases, the assets to be protected and the threats to be countered. The ESR may also specify exclusion of certain aspects from the cPP. This may be done by explicitly stating the exclusion of a threat, such as "Resistance against physical attacks of the device, where the device is compromised and returned to the user, are not to be considered." The ESR should in general avoid specifying or predicting the technical solutions for doing so. This flexibility is intended to allow the iTC to choose the way to meet the requirements, and to make the ESR stable over time.

The requirements listed in the ESR should be core requirements that are common to all the initial potential iTC members (and other parties that can reasonably be accommodated at this stage). The ESR may identify requirements that apply only to *some* use cases or initial potential iTC members as optional extensions for the iTC to consider including (as options) in the cPP, but these should not be included as core requirements in the ESR. This approach therefore encourages a focus on the core requirements (at least for the initial version of the

cPP), but recognizes that there may be particular situations that justify the presence of optional requirements in a cPP. The iTC will then be responsible for balancing the urgency of need for an initial cPP against the benefits of providing identified options.

The ESR should constitute both the general and, when appropriate, specific requirements with which an ICT product must comply in order to satisfy the initial potential iTC members' procurement guidance and/or technical regulations. The intent is that the ESR will allow the iTC flexibility to craft SFRs in a manner that makes sense to that community, given that the iTC members (rather than the initial potential iTC members) represent *expertise* in that technical area. An example of a general requirement in an ESR would be "A user must be authorized by the device before accessing (reading/writing) any user data on the device". This high level requirement offers multiple ways in which an SFR could be expressed. However, there are also instances where initial potential iTC members may see no alternative other than to provide specific requirements. An example of a specific requirement would be "The expectation is that the device will employ cryptographic means to provide the necessary protection of user data, the strength of which lies in the quality of the cryptographic algorithms and the entropy of the authorization factor (e.g., password, passphrase)." While this statement still allows for some flexibility on the part of the iTC, it is clear that cryptography must be the primary method used to provide a solution.

The ESR is to be expressed in natural language - CC abbreviations and constructs should be avoided, in order to make the document more accessible to a wide range of readers (e.g. technical experts and risk owners, as opposed to CC experts).

The degree of detail of the wording will depend on the subject matter. General constructs should be used to capture the requirements as much as possible. Wherever appropriate, the ESR shall specify security functionality, rather than design and/or implementation characteristics.

It is understood that there may be technical and assurance aspects that it is critical to cover in certain ways in a cPP in order to allow for a CCRA Participant to be able to support the finalized cPP. However, detailed aspects of the construction of the cPP should be dealt with through discussion in the iTC, where CCRA Participants are expected to participate at an appropriate level in order to cover their interest in the cPP (as compared to the initial potential iTC where they are concerned only with high-level requirements for the ESR). The main goal for the ESR is to describe the essential security requirements for a particular cPP that has been harmonized at a high level among the CCRA Participants.

An ESR shall contain:

- A statement of the status of the ESR
- A description of use cases (defines the primary use of user data, often not directly related to security aspects)
- Resources to be protected
- The attacker's access to the TOE (this identifies the threat paths to be covered and may identify attack vectors *not* to be covered)
- The boundary of the cPP target product (e.g. in terms of logical and physical parts included or excluded)
- The list of essential security requirements.

An ESR may contain:

- Optional extensions that the iTC should consider
- Assumptions
- Items to be placed outside the scope of evaluation (e.g. threats, functionality, or other product capabilities)

- Notes or guidance to aid in interpretation of the requirements.

An ESR shall not contain:

- Policies (since it is expected that policies are difficult to harmonize among various government authorities, and would therefore make ESR production timescales too long to be useful).