Public Review Draft 1 of the DSC iTC cPP & Supporting Document v2.0 Overview

Table of Contents

Introduction

This is an announcement of a public review period for the cPP and Supporting Document from the DSC-iTC.

This document will provide information about where to find the documents, how to provide feedback and information about the current status of the documents.

Please email iTC-DSC@niap-ccevs.org if there are any questions about the Review process.

The latest status of the Review Period, including the latest copies of any documents, can be found at the DSC iTC page.

Review Status Phase

The documents listed here are in the v2.0 **Public Review Draft 1** phase.

Publication Date

October 31, 2023

End of Comment Period

December 15, 2023

Documents for Review

The following are the documents included in this v2.0 Public Review Draft 1 Period:

Table 1. Review Documents

Title	Version	Link
collaborative PP for Dedicated Security Components	2.0-PRD-1	Download cPP
Supporting Document for Dedicated Security Components	2.0-PRD-1	Download Supporting Document

The following are the documents to use in support of the Public Review Draft 1 Period.

Table 2. Supporting Documents

Title	Link
Comment Matrix	Download Comment Matrix

Document Release Process

The BIO-iTC follows the document release process below for the publication of documents. Generally the PP (PP-Module and PP-Configuration) and SD would be released at the same time.

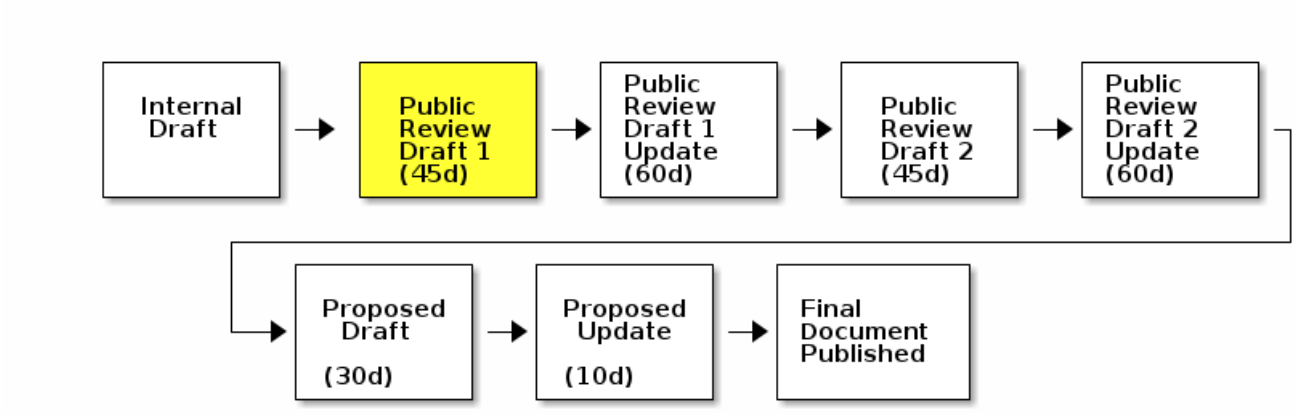

Table 3. Review Timeline

Phase	Time	Description
Internal Draft		The normal, pre-release process for creating the documents

Phase	Time	Description
Public Review Draft 1	45 days	iTC has voted according to Terms of Reference to release this version for public review. Public (i.e. from non-iTC participants) comments are accepted during this period
Public Review Draft 1 Update	Up to 60 days	The iTC will review all received comments and update the documents accordingly
Public Review Draft 2	45 days	iTC has voted according to Terms of Reference to release this version for public review. Public (i.e. from non-iTC participants) comments are accepted during this period PAD Toolbox drafts will be published with this review (final review on toolboxes may proceed independently from rest of documents).
Public Review Draft 2 Update	Up to 60 days	The iTC will review all received comments and update the documents accordingly
Public Review Draft 3 (Optional, not shown)	45 days	iTC has voted according to Terms of Reference to release this version for public review. Public (i.e. from non-iTC participants) comments are accepted during this period
Public Review Draft 3 Update (Optional, not shown)	Up to 60 days	The iTC will review all received comments and update the documents accordingly
Proposed Draft	30 days	iTC has voted according to Terms of Reference to propose this as the final document. Public (i.e. from non-iTC participants) comments are accepted during this period
Proposed Update	10 days	iTC reviews any further comments and prepares the document for final publishing (updating all dates, producing official versions for publication)
Final Document Published		Documents are posted to Common Criteria Portal

The iTC may decide, based on the comments received during the Public Review Draft 1 period, that a Public Review Draft 2 period is needed. Public announcement of a second review draft or a proposed draft will be made once all comments have been addressed.

Review Process

There are two ways to contribute comments and suggestions to the iTC. The first is through GitHub, the second by spreadsheet. It should be noted however that comments that are received via the spreadsheet will be added to the GitHub platform to allow for a comprehensive discussion. Also, feedback for comments is only provided via the answers in the GitHub comments.

Each comment should have a suggested resolution be proposed if a change is needed to the document.

GitHub Review Process

To use GitHub to submit comments, you must have a GitHub account (and it is assumed you know how to use GitHub). Each comment should be submitted as an individual Issue with the Label "Public Review" assigned. Pull Requests created for any issues will be linked to these Issues for traceability.

Comment Matrix Spreadsheet Review Process

In the Table 2, “Supporting Documents” table there is a link to the Comment Matrix spreadsheet. There are instructions for using the Matrix on the second worksheet. Please create a separate copy of the spreadsheet for each document.

Email the spreadsheets to iTC-DSC@niap-ccevs.org.

Additional Notes

This new version of the cPP is targeting to be compliant with CC:2022 since the expected time for completion of the review process will be summer of 2024 at which point CC3.1R5 makes no sense. As such, the version of this document will be v2.0 instead of v1.1 as originally planned.

The areas noted below should be considered when making comments.

Cryptographic Updates

The v2.0 cPP will utilize the Crypto Catalog that has been under development by the CCDB for some time. The current release is based on the v0.1 document that was provided. As the catalog is scheduled for release at the same time as the public review for the cPP is starting, the main concerns expected in the review related to cryptographic requirements is how they link together properly. The Public Review Draft 2 (PRD-2) will have all the changes integrated.

Importantly, note that no changes were made in the SD related to cryptographic requirements as the v0.1 of the crypto catalog did not include any Evaluations Activities. Any comments about cryptographic requirements in the SD will be automatically rejected during this review as no work was done in that section for this reason.

PBKDF Specific Question

One issue that has not yet been fully resolved in this update is the question about PBKDF integration. While a TD has been issued for this, the changes to the crypto catalog and discussions about whether PBKDF is the only acceptable method for preventing brute force-style attacks has meant this question is not yet resolved. The discussion about the possible approaches can be seen in Pull Request #124. Specific ideas about how to approach this during the review period can be made directly to the Issue or via a submission.

CC:2022 Changes

While the cPP has been reviewed for CC:2022 compliance, this is not yet complete. As this is still new, additional review related to this topic would be appreciated (and hopefully be able to be spread to other iTCs as lessons learned).

Formatting

As this is the first version published for public review using the asciidoc source, please take special note of any formatting problems in the resulting PDF or HTML output and report them for review. No problems are expected, but may appear based on how the document is processed.