# Editor's Note: Verified Login Component

**Pan-Canadian Trust Framework**

5 July 2019
Version 0.2

# 1 About This Document

This document provides a summary of comments received during the open review period of the Pan-Canadian Trust Framework Verified Login Component. **This review included the Verified Login Overview V0.06 and Verified Login Conformance Profile V0.03 Discussion Drafts**. DIACC conducted this review from 15 May to 17 June 2019.

225 comments were submitted during the review period. Of these:

- 81 related to the overview document and 140 related to the conformance profile
- The editing team reviewed each comment, identifying 105 as editorial in nature. However, these are self-assessed by reviewers in most cases. Many suggested items flagged as "editorial' changes are actually "substantive" in nature and have been referred to the design team for resolution.
- The editing team referred 117 comments to the design team for resolution.

# 2 Major Themes

The editing team noted the following as significant themes running throughout the comments received.

As this note is based on provisional responses to comments, details concerning resolution to these themes are not yet provided.

| Approaches to authentication | |
|---|---|
| While most reviewers accept, implicitly at least, that usernames-passwords and associated two-factor authentication will continue to be in use over the short to medium term, multiple comments suggest this component should consider, in the words of one reviewer, "legitimate successor[s] to traditional seals, autographs , and text-passwords." Self-sovereign identity models were | As we have seen with other components, there is modest but distinct urging of TFEC to address emergent issues and technologies. |

| | |
|---|---|
| specifically called out as being absent in this version of the document. Biometrics (and their treatment in the current version) are also of interest to reviewers. | |
| **Examples and external references** | |
| This component makes multiple references external standards – primarily as examples of industry standards with which organizations should/must adhere to as part of compliance with a given conformance criterion (e.g., BASE-5, BASE-11, CRAU-15). In some cases, reviewers ask about rationale for using or referencing specific standards. Others request that additional items be added to the conformance criteria. In one case, reviewers recommend removing reference to NIST 800-63 in its entirety on the basis of its being based on "older belies" and it "does not account for emerging technology". | Taken together, the comments suggest that component overview documents could include a note concerning the rationale for including (or in some cases, excluding) other standards that are incorporated into conformance criteria by reference. |
| **Conformance criteria for specific LOAs** | |
| The conformance criteria of this component are structured around 4 levels of assurance (LOA). The editors note that:<br>• A number of comments concern details in or changes to requirements specified for a given LOA or differences in requirements between LOAs. For instance, a reviewer may ask why a given criterion is identified as MAY rather MUST for LOA1 and suggest the change be made. | To prevent similar comments from a broader audience, the editors recommend including a note that LOA4 requirements are not specified in the current version -or- removing reference to this LOA entirely. |

| | |
|---|---|
| • Multiple reviewers note that there are no conformance criteria defined for LOA-4. | |
| **Trusted process descriptions** | |
| Reviewers identify what they regard as gaps, inconsistencies, and unclear descriptions for Verified Login trusted process descriptions and associated "inputs" and "outputs" descriptions. Multiple comments suggest additions, clarifications, or request clarifications for improvement. | Terminology and textual clarifications will address many of the comments. However, a closer look at additions to these process definitions is warranted given the potential to affect multiple conformance criteria. |
| **Overview content and editorial revisions** | |
| Reviewers submitted a high number of comments tagged as "editorial" in nature. Of these comments, the following items are most frequently raised:<br>▪ Overlaps, inconsistencies, or questions about content provided by the overview and conformance profile documents.<br>▪ Requests for terminology usage and clarifications.<br>▪ Consistent use of terminology or use of one preferred term.<br>▪ Requests for examples when referring to terms or processes/events.<br><br>On a related noted, at least one commenter recommended selecting one term to define priority of requirements (e.g., MUST and SHALL were used in the reviewed documents). | These comments reiterate the need to revisit overview and conformance criteria content – arguably for all components. This is a planned task for the editing team.<br><br>Regarding the repeated requests for terminology clarification, the comments received thus far suggest that design teams should identify key terms in their content and flag them for inclusion in either a local glossary section or the PCTF glossary. Moreover, they beg questions of what TFEC considers a reasonable level of technical awareness among the audience for these documents. |
| **Conformance criteria for specific LOAs** | |

| | |
|---|---|
| The conformance criteria of this component are structured around 4 levels of assurance (LOA). The editors note that a number of comments concern details in or changes to requirements specified for a given LOA or differences in requirements between LOAs. Reviewers also noted that there are no conformance criteria defined for LOA-4. | To prevent similar comments from a broader audience, the editors recommend including a note that LOA4 requirements are not specified in the current version -or- removing reference to this LOA entirely. |
| Sessions | |
| Reviewers note several issues with terminology and conformance criteria related to "sessions", including:<br>• Difficulty differentiating between "authenticated" and "authentication" sessions.<br>• The appearance of a tight-coupling between participants.<br>• Level of authentication of a session. | Terminology and textual clarifications will address many of the comments. In some cases, a closer look at requirements specified in certain conformance criteria is needed. |

# 3 Other Items

Other items noted by the editing team:

1. Authentication factors – The concepts of "something you know", "something you have", and "something you are" are core to this subject matter domain and properly included in this PCTF component. However, a brief description of these concepts in the overview document may make the component more accessible to a wider audience.
2. Privacy – A limited number of reviewers wonder if some conformance criteria go against PIPEDA (principle 7 – safeguards). While not a general concern, the subject is highlighted here given DIACC's commitment to privacy in all of its work.
3. Stylistic assumptions – Most comments address very specific items in the component documents. When considered together, however, it is apparent that reviewers have general stylistic assumptions about these documents – primarily as standards

documents. Stylistic assumptions may include capitalization of certain terms (depending on usage), the introduction of new terms, how external references are noted, when to use inline notes, etc.