From:
To: [piv_comments] Comments on SP 800-217
Subject: Monday, March 27, 2023 3:10:15 PM
Date:

My comments are the following.

_____

Line 234: Insert a comma after "account".

Line 451" Need to more clearly describe the difference between the PIV Idp and the home IdP.

Lines 473-475: Elaborate a bit more. Because the info about the non-PKI-based derived credentials is only available at the home IdP?

Lines 480-484: This is hard to understand. Since this is discussed in different documents, some reminder of what's going on here and why would be helpful.

Lines 485-487: This is hard to understand. Since this is discussed in different documents, some reminder of what's going on here and why would be helpful.

Lines 507-510: Expand on this. Remind the reader of what's going on here.

Line 518: The use of SHALL ss kind of a strong word for use with "trust". How does one mandate trust? This could be reworded to something like "The RA SHALL NOT have an agreement with a specific IdP unless the IdP is trusted...

Line 542: Change to "...attributes that can be provided"?

Lines 551-553: Could the RP have established trust agreements for Agency X with both IdP A and IdP B? Maybe change "a" in line 517 to "one" (or "only one") to be more specific?

Line 595: Change to "...attributes that can be provided"?

Line 702: Define/describe "injection".

Line 716: Define "static process".

Line 718 (and elsewhere): Provide a definition in this document for "bound authenticator"(the reader may not remember what it means). Look for other terms to include as definitions as well. There are at least 5-6 documents to "remember" terms from. However, keeping definitions in sync is difficult. Maybe this is not a useful idea, but what about having all the definitions in one document, with links to that definition document?

Line 725: Change "of" to "in"?

Lines 739-742: This is very complicated; explain a bit more.

Line 776: Delete "on".

Lines 802-804 (cryptographically...identifier): Don't think this is quite right. Maybe something like "an approved random-be generator or a value derived from an approved derivation

method for the subject..."?

Lines 817-818 (for only...event): Don't understand. Provide an example?

Lines 924 and 937: Change to "At a minimum".

Line 929 (which is IAL3): I think the intent here is that the IdP needs to provide the IAL for the account and the RP only accepts IAL3 (it doesn't read quite that way). Can the account have something less than IAL3?

Line 992: Change "to" to "using".

Appendix A: The example could use pictures for clarity.

Line 1057" Change to "information to be consumed by the RPs"?