Comment Template for: NIST SP 800-217 (Initial Public Draft)

Please submit responses to piv_comments@nist.gov by March 24, 2023

Organization: CertiPath, Inc

Name of Submitter/POC:

Email Address of Submitter/POC:

Comment #	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
1	General			This document tries too hard to provide non-PKI federation solutions to Federal agencies. If this is about credentials from one Federal agency being accepted by another Federal agency, which it most certainly appears to be then it should take full advantage of the PIV credential and the PKI Certificates associated with the PIV credential for establishing trust. I am hard pressed to think of a scenario where "attributes" would need to be exchanged between one Federal agency and another. The PKI certificates provide employing organization and full name of the individual. Agencies generally don't need information such as DOB or age at run-time for access to systems and the sorts of information they do need would likely be exchanged out-of-band beforehand (security clearance etc.). The implications of the "home IDP" are equally concerning. Establishing an 'external' mechanism that can reach back into the organization's personal identity records database is fraught with security risks, particularly as this capability may actually be outsourced to a third party vendor. The concept of the "home IDP" also has the effect of limiting competition and innovation in the field, while 'other' IDPs are not prohibited, they are limited to AAL1, which will result in their scarcity if not complete extinction. A federation assurance capability available in the market today leverages PIV credentials and their PKI certificates to establish accounts at the IDP, and allows the addition of other authenticators to that same account. Each authenticator in the account has an assigned AAL and the account holder's account log in process established the IAL. Relying Parties are able to set their minimum IAL/AAL criteria and accept authentication from the IDP that meets these needs. Interaction with a Personal Identity Account is unnecessary because the IDP can continually authenticate the PIV credentials and the account holder can add or remove additional authenticators through the portal. Our recommendation is that this Special Publication be withdrawn for a complete review and revision. We recommend a series of public forums to better understand the needs of the agencies and the capabilities of the industry.	Consider withdrawing this document and holding public hearings on how Federation can be utilized in a PIV-based government environment.
2	1.3	2	284-285	Organizational Affiliation - How does this differ from Issuing Organization? Not in glossary. Needs more explanation. Why does the RP need this information	Recommend additional discussion of what a "home agency" is up front. i.e. The Federal Agency issuing the PIV card and setting up the PIV Identity Account - and move the explanatory language from Section 2.2 here. Use the term consistently as needed throughout the document (e.g., replace "issuer of a PIV Identity Account" with "home agency".)
3	1.3.1	3	319-320	Makes the statement that the subscriber "only has to manage one set of credentials." Does this mean that all PIV and DPIV credentials are being lumped into "one set"? While technically true, it can still be a challenge to determine which of these is appropriate for which RP. Will the IDP handle this and tell the subscriber to authenticate with credential X?	Check this statement for accuracy. Add more 'color' to improve understanding.
4	1.5	4	352	This is a Special Publication, it's title indicates it is a "Guideline" but it calls itself a "Standard" here. Is it NIST's intention that this Guideline be considered a Standard? Seems to send mixed messages.	Revise this introduction for accuracy. For example: "This Guideline contains requirements that are mandatory for Federal organizations and uses the following typographical conventions in text:" Alternatively, the mandatory nature of the document could be made clear in Section 1.2 Purpose and Scope and the change here limited to replacing "Standard" with "Guideline".
5	2.2	8	440 & 446	The term "issuer" is used here in the context of the entity issuing the PIV Identity Account, which is assumably the "home agency" (previously identified). Everywhere else in the document, "issuer" is used to refer to the PIV IDP.	Recommend replacing "issuer" here(2 locations as identified by line #) with "home agency" to avoid confusion.
6	2.2	8	448-453	I fail to see the value of a PIV IDP that is not the home IDP, particularly when the home IDP is mandatory. Other than a proxy, why would an RP choose anything else? Particularly if it is only valid to FAL1.	Recommend additional detail on the nature of a non-home IDP.

7	2.2.2	9	480-484	This entire paragraph is confusing. It is referring to PIV IDPs as if they are distinct from home IDPs (the establishment of a subsection on home IDPs and then a second subsection on PIV IDPs suggests they're distinct from each other as does the fact that it doesn't state that home IDPs are a subset. Given this, the entire discussion about choosing the IDP either for a set of subscribers or for a specific subscriber. Still trying to ascertain why an RP would ever need to contact any but the home IDP (or its proxy). What advantage could there be in designating a non-home IDP for any account?	Recommend review/revision of this paragraph. At a minimum the relationship between the home IDP and the PIV IDP should be made clear. One thing that might work is reversing the order. Put PIV IDP first and then Home IDP follows and identifies itself as a subset of the PIV IDP definition.
8	2.3	9	489-490	"PIV identity accounts are protected using one or more PIV credentials that are bound to the account." Is this correct? Are they "protected" by the PIV credentials, or are they "linked to" the PIV credentials. As written it makes it sound like the only access to the PIV Identity Account is via the PIV credential (presumably the PIV credential identified by the Identity Account) when in actuality, the Identity Account and its contents are managed by the home agency.	Consider revising this sentence for accuracy. For example: PIV identity accounts are ~~protected using~~ linked to one or more PIV credentials that are bound to the account."
9	3	11	533	"Authorized Party" is not defined in SP 800-63C. It is defined in the Baseline document SP 800-63.	Revise, correct this reference.
10	3	11	539	How is mapping the PIV Identity Account to the IDP an RP function? - doesn't the RP just get the result from the IDP? - the IDP would be the one mapping the PIV identity account to the authenticator. Or are we talking about RP subscriber accounts? Should be clearer.	Review/revise this requirement as appropriate.
11	3.1	12	567	"An RP MAY establish the PIV IdP directly with the IdP in a bilateral fashion". Shouldn't the underlined be "trust agreement'	Revise sentence for accuracy
12	3.1	12	566-574	This entire section is confusing. What does the 2nd paragraph have to do with bilateral agreements? Nor does the 2nd paragraph seem completely accurate. "When the PIV IdP is the home IdP for an agency, the PIV IdP operator SHALL make available its home IdP record to the connected RP" - what is "home IDP record"? Is this a proof that it is the home IDP for a specific set of accounts? Is it the home IDP publication record from line #661? If so, it should refer to it as the "home IDP publication record." "The RP operator SHALL make the home IdP record available to authenticated subscribers from that IdP, upon request." Why is the RP making the home IDP publication record available to the subscribers? Wouldn't that be the IDP's job? Or is this talking about the attributes pertaining to the specific subscriber that it collects?	Consider whether the 2nd paragraph belongs in a paragraph about bilateral agreements. Also, whether it stays or moves, clarify its intent.
13	3.2	12	576-577	"An RP MAY establish the PIV IdP through the use of a trusted third party known as a federation authority, . . ." RPs don't establish PIV IdPs. It would seem a reference to the trust agreement is missing here.	Revise for accuracy. For example: "An RP MAY establish a trust relationship with the PIV IdP through the use of a trusted third party known as a federation authority,. . ."
14	3.2	12-13	579-580	"In such systems, the federation authority decides which PIV IdPs and RPs are allowed to participate based on the trust agreement provided by the authority." The Federation authority decides based on the trust agreement it provides??? Or based on its community needs and resources? This feels a little bit like cart before the horse. I could see it being the community it serves or the federation charter/by-laws but trust agreement with whom?	Review/revise this requirement as appropriate for accuracy.
15	3.2	13	582-583	"The federation authority SHALL establish and declare whether each PIV IdP is the home IdP for any given PIV identity account within the trust agreement." What is the meaning of "establish in this context?	Recommend replacing "establish" with "determine" in this sentence.
16	3.2	13	584-585	"The federation authority SHALL vet all PIV IdPs and RPs within the federation to ensure that all parties are acting within the terms of the agreements." Is this a once for all, or is there periodic re-evaluation?	Revise to add more detail concerning the expectations for refreshing the relationship between the federation authority and the IDPs and RPs.
17	3.2	13	586-587	"The federation authority SHALL disclose to all connected RPs whether a particular IdP is the home IdP for an agency in question." Isn't the RP more interested in whether this is the home IDP for a particular subscriber population?	Consider revising this sentence to replace "agency" with "subscriber population" or "PIV Identity Record"
18	3.2	13	587-588	"Federation authorities SHALL make all home IdP records available. . ." As witten it sounds like the PIV IDP records pertaining to all subscribers will be dumped to the RPs.	Recommend adding "publication" here. i.e., "home IdP publication records."
19	3.2	13	596-598	Why does the RP have to justify itself to the federation authority? if the attributes requested are available, then an RP should be permitted to request them based on their own processes and SORs.	Recommend removing this requirement for the RP to justify itself to the federation authority or IdP.
20	3.3 - 3.5	13-15	599-	Section 3 is Trust Agreements. Begins with Bi-lateral and Multi-lateral. Begs the question whether Proxy, Shared Signaling and Home IDP are types of Trust Agreements. In other words, do these sections belong here or is there a more appropriate location/section for them.	Revise the language in Sections 3.3-3.5 to more closely align with the Trust Agreement topic or move the contents here to another section (Architecture, perhaps).
21	3.3	13	606-607	"However, bilateral agreements are still possible and allowable through a proxy, with each IdP and RP making a pairwise agreement to the proxy itself." This feels internally contradictory. Aren't all agreements between an IDP/RP and the proxy (as federation authority)? How does this differ?	Review/revise as necessary for clarity.
22	3.3	13	608-610	"For each federated transaction with an RP, the proxy SHALL determine the appropriate upstream PIV IdP that is appropriate for each PIV identity account it proxies to a downstream RP." Too many "appropriates." Is "proxies" the right word here? What does it mean "to proxy"? Simply put "the proxy proxies" Would it be better to say "presents" here?	Consider revising this sentence as follows: "For each federated transaction with an RP, the proxy SHALL determine the ~~appropriate~~ upstream PIV IdP that is appropriate for each PIV identity account it ~~proxies~~ presents to a downstream RP."

23	3.3	14	614	"The proxy's nature as a proxy". So the proxy is disclosing the fact that it's a proxy? Perhaps there is a clearer way to state this.	Consider revising this bullet to more clearly state what is expected here. For example: "Its status as a proxy".
24	3.4	14	637	Surprised this isn't a "MUST". If an RP is seeing suspicious behavior on a subscriber account, wouldn't that be an indicator that the IDP may have been compromised? Generally, the value of shoulds and mays in this entire section is questionable. If it is the right thing to do for security and privacy, they should be required to do it, otherwise, don't talk about it.	Consider reviewing revising these mays and shoulds. Maybe take a different approach to the discussion.
25	3.4	14	643-644	"When the IdP receives such status changes, the IdP SHOULD terminate, disable, or update . . ." Not investigate? Contact subscriber to let him know his account may be compromised? A unilateral termination or disablement could cause consternation for the subscriber who doesn't understand why access has been pulled.	Consider reviewing/revising the IDP responsibilities when notified by RPs of problems with subscriber accounts.
26	3.5	15	646	What portion of this instruction to the home IdP also pertains to a non-home PIV IdP?	Perhaps revise the title to idicate "any" IdP. Or add anohter section for PIV IdP (non-home).
27	4.1.3	17	739-740	Very confusing paragraph. Not sure what the sentence "In their use as bound authenticators at FAL3, authenticators from PIV credentials do not function as PIV credentials at the RP." is trying to convey. It seems to be talking about PIVAuth certificates, but then begins to refer to DPIV as if that was the intent all along. And if so, it seems self-contradictory.	Review/revise this paragraph as appropriate.
28	5.1.1	20	776	Typographic error: The word 'on' should not be here - was it intended to be 'only'? If so, don't split the verb with it, place it after the verb "can be verified only"	"However, becausenon-PKI-based derived PIV credentials can ~~on~~ be verified only by the issuing home agency, . . ."
29	5.1.1	20	780	What is 'recent' in this context. If a live session has to be reauthenticated every 12 hours, is that sufficient or is this intended to be more recent than that and, if so, why, if the session is still valid? 'SHOULD' means it is a suggestion - but why make the suggestion? It is understandable if the RP requests it, but doesn't make sense as a general requirement.	Consider removing this 'SHOULD' statement.
30	5.1.1	20	785	The parenthetical here is problemmatic as you go on to say below.	Remove the parenthetical example/
31	5.1.1	20	786-788	Home IDPs are supposed to be connected to PIV Identity accounts. Now it seems they should connect to Enterprise Identity Management Systems. Is this the intent?	review/revise this sentence for clarity
32	5.1.1	20-21	788-795	This doesn't flow from the beginning of the paragraph. Nothing there indicates that the PKI-based is being used as the only authenticators. This should be a separate paragraph. And while it is a valid point that a certificate may have been terminated while a PIV account is still valid and vice-versa. The maximum lag is 18 hours, which makes it less of an issue (not discussed here). The "Note" here applies equally to the home IDP and other IDP scenario and as a note should be set apart to be easily discernable.	Beginning with the sentence "For other PIV IDPs. . ." make this a new paragraph. Then start a new paragaph with "Note. . ."
33	5.1.3	21	816-518	This is confusing. Not sure what it is sying	review/revise this sentence.
34	5.2.1	21	823	Word usage: Recommend revising this sentence for accuracy	"The RP SHALL verify that all assertions received ~~contain~~ meet the requirements enumerated in. . ." OR "The RP SHALL verify that all assertions received contain the ~~requirements~~ specified attributes enumerated in. . ."
35	5.2.2	22	826	Need to review this sentence - the word 'that' does not seem to belong.	Revise sentence for clarity.
36	5.2.2	22	832-833	If there are two different IDPs associated with a subscriber, will that subscriber have two different accounts at the RP? How is this reconciled by the RP? Can the RP associate two separate federation identifiers with a single subscriber account? How does it know that one is not a "spoofed" identity?	Review/revise to provide clarity.
37	5.2.2	22	838-840	This seems overly restrictive on the RP which is ultimately responsible for who/how it provides access to an account.	Consider revising this "SHALL" to a "SHOULD" so it becomes a best practice not an imperative.
38	5.2.3	22	846-847	Hard to understand why the RP is being so closely controlled here. If the RP wants to tie the assertion lifetime to the IDP session, shouldn't it have that volition? "In common practice" in the next sentence seems to suggest that is the case.	Consider revising this "SHALL" to a "SHOULD" so it becomes a best practice not an imperative.
39	5.2.4	23	867-868	This is confusing. Not sure why the RP is being regulated in this way.	Consider removing this moratorium on the RP.
40	6.1	24	878-890	Not sure what this is saying - These attributes must be available or these attributes must be shared regardless of RP need?	Consider revising this section for accuracy and to avoid confusion
41	6.1	24	886-887	Organizational Affiliation - How does this differ from Issuing Organization? Not in glossary. Needs more explanation. Why does the RP need this information	Review/revise this reference to "Organizational Affiliation".
42	6.5	28	1008-1009	Why does the RP have to justify itself to the Attribute API? if the attributes requested are available, then an RP should be permitted to request them based on their own processes and SORs.	Consider revising this "SHALL" to a "SHOULD" so it becomes a best practice not an imperative.
43	6.6	28	1011	Do all of the requirements associated with the IDP also apply to the proxy? If so, it should say that.	Consider providing more detail concerning proxies.