

Comment Template for: NIST SP 800-217 PIV

mmr	Publication	Section	Page #	Line #	Comment	Suggested Change
1	800-217 Initial Public Draft	1.3	2	294-296	Disagree: Most IdP capability providers are not PIV CSPs. Do PIV CSPs offer APIs for IdPs to do more than just certificate validation?	Address cases where IdP is not tightly coupled to PIV issuance and drive a common data set or APIs for 3rd parties to leverage PIV issuance data
2	800-217 Initial Public Draft	2	7	403	Perhaps could expand further, because with the move to zero trust, other factors may be leveraged not tied to PIV that could meet requirements for federation (such as hardware backed and/or phishing resistant factors).	Consider broader scope of strong authenticators in addition to PIV
3	800-217 Initial Public Draft	2	7	404	No capture of IdP initiated flows	Add IdP initiated flows
4	800-217 Initial Public Draft	2.1	7	427-428	While out of scope, non-PIV standards include authentication method references to communicate to other relying parties how an identity was authenticated. Why not include/require where applicable/reference for a holistic view?	Consider more context of non-PIV AMRs within SAML/OIDC standards as also important in the broader federation conversation.
5	800-217 Initial Public Draft	2.2	8	446-447	Need a stronger call out or formal tasking for organizations to recognize they need to establish or designate a home IdP	Highlight key tasks for organizations to consider under this SP
6	800-217 Initial Public Draft	2.2.1	8	468-470	What functionality is needed to satisfy home IdP requirements?	Better define home IdP requirements/functionality
7	800-217 Initial Public Draft	3	11	537	For the purpose of use of each attribute, should common uses be defined and be allowed to be expanded upon for unique scenarios?	Define a common set of purpose/definitions for attribute use

8	800-217 Initial Public Draft	-	-	-	No federation threat section, to include risks of insider threats, user impersonation, account mapping to name a few	Suggest a section on threat consideration and mitigations with federation