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

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

Organization:	*Department of Energy (DOE)*
Name of Submitter/POC:	
Email Address of Submitter/POC:	

Comment #	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
1	3.2	13	591-594	IdPs within a federation authority SHOULD enable dynamic registration of new RPs, as discussed in [SP800-63C], subject to the rules of the federation authority, the desired federation assurance level, and the capabilities of the federation protocol in use.	
2	4.1.3	17	718-722	As defined in [SP800-63C], FAL3 requires the establishment of a bound authenticator, which the subscriber presents directly to the RP alongside the federation assertion from the IdP. Though most PIV credentials can be used as bound authenticators at FAL3, the nature of the binding depends on the type of authenticator, its use, and its phishing resistance qualities. Comment: Does this mean that subscriber present something from the PIV card to the RP directly? This seems burdensom to have OneID auth the PIV AND the RP auth the PVI - I don't see the point. There SHOULD be a mitigation the home/PIV IdP be able to assert to the RP this trust.	
3	5.1.1	20	776	However, because non-PKI-based derived PIV credentials can on be verified by the issuing	Typo change to only
4	5.1.1	20	777-778	PIV IdPs operated by third parties would need close integration with those issuing home agencies to capable of verifying those authenticators. Comment: that Close integration implies or answers to that we can as we establish the "proper" trust with other agencies for these credentials	
5	6.1	24	886-887	For a Department (for example DOE which has several agencies under it), this implies that this could be at agency level "The organization or list of organizations that the PIV identity account is affiliated with"	
6	6.3	27	978-985	Dynamic registration is attainable, however given some recent advancements in post-quantum encryption (/hashing) concerns given the current landscape this dynamisim appears to be a risk if bad actors can spoof valid dynamic registrants given current algorithms available.	
7	6.4	27	986-993	Encryption of assertions is currently bound to capability of RP (e.g., not all COTS products nor tech stacks support this)	Since it says SHALL, that means the RPs that cannot accept encrypted assertions will not be able to achieve FAL3. This especially comes into play for COTS products (these usually do not accept encrypted assertions in my experience). Suggest to tone down SHALL to perhaps MAY.

8	2.4	9	503-506	The RP's only view into the contents and status of the PIV identity account comes through its interactions with the IdP. The RP can manage its own local reference to the PIV identity account, known as the RP subscriber account, as discussed in Sec. 5.2.2.	Clarification or confirmation that RP manage the user roles and privileges
9	2.2.1	9	473-475	Note that the use of a home IdP is the only means of making non-PKI-based derived PIV credentials. **Clarification** that non-PKI based derived credentials can only be used within a Department, not outside of security boundary	Clarification
10	3.4	14	621-636	Comment - please include words which are not very Active or proactive, such as words or protocols like LDAP, SCIM interface as well. Signalling sounds very Active or proactive specially with requirement s of SHOULD for an IDP. Consider adding a passive LDAP interface made available that a RP can verify.	Consider adding a capability on IDP side that a RP can query, rather than an active signalling capability on the IDP. Clarify that SHOULD here means Recommended.