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

Please submit responses to piv_comments@nist.gov by ~~March 24~~ April 21, 2023

Organization:	*MAX.gov (OMB)*
Name of Submitter/POC:	
Email Address of Submitter/POC:	

Comment #	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
1	3	11	519	There are already several shared services within the government that accept valid PIV credentials from any agency. RPs utilizing these services can be thought of as using them as the PIV IdP for the population of PIV Identity Accounts that emcompasses the entire federal government, albeit with an implied trust agreement. Should this scenario be mentioned here?	
2	4.1.3	17	713	This section seems to preclude third-party (non-"home") PIV IdPs from operating at FAL3. There may be cases where an IdP/RP needs to operate at FAL3 as defined by SP800-63C using a PIV authentication cert as a bound authenticator, but only has access to the identity data stored in the PIV card and does not have access to any data from the issuing agency's internal identity attributes. This document should support such scenarios.	
3	4.1.3	17	724	Subject Distinguished Name is NOT sufficient to bind a PIV authentication cert between an IdP and RP. Multiple issuers could produce certificates for different users with the same Subject Distinguished Name in some corner cases, and a malicious actor with the ability to issue certs under any trusted issuer could produce certificates with the same Subject DN, Serial #, and other fields as existing certificates for users under another issuer, facilitating cross-issuer attacks. A more appropriate way to bind the athenticator is to include a full copy of the PIV certificate used for authentication. (Section 6.2.1 also needs to be updated accordingly.)	
4	6.1	24	878	This section seems to assume that every PIV IdP will have access to identity data that may only be available to the issuing agency. Thus, a third-party PIV IdP that only has access to the identity data stored in the PIV card and does not have access to any data from the issuing agency's internal identity attributes cannot meet these requirements. For example, PIV authentication certs are not required to include an email address, so a third-party PIV IdP that only has access to a user's PIV auth cert cannot provide an "Email address" attribute to RPs. Similarly, PIV card are not required to contain organizational affiliations other than the agency name and FASCN agency code, so a third-party PIV IdP may not be able to provide a meaningful "Organizational Affiliation" attribute that isn't simply a copy of the "Issuing Agency" attribute. Also "Physical Address" and "Phone Number" are generally not included in PIV certificates. There is arguably insufficient standardization of even the "Full Name" in PIV cards, so it isn't clear that a third-party PIV IdP could even provide a consistently-formatted "Full Name" attribute that doesn't include other non-name data (such as affiliate/contractor flags, ID numbers, etc). NIST should coordinate with the FPKI to develop a minimum set of "required" identity attributes, and to specify standardized formatting for each attribute, so that these attributes can be incorporated into the PIV standards and encoded into PIV certificates for use by PIV IdPs and RPs that do not have access to the issuing agency's identity data. Alternatively (if that isn't possible/practical), this document should make optional all attributes that cannot be directly extracted from all existing PIV certificates.	

5	6.1	24	888	It isn't clear what the purpose of the "Last Updated" attribute is. There may be cases where a third-party IdP collects attributes from multiple data sources. Should this attribute indicate the last time any attribute value from any data source changed? The last time the IdP retrieved any attribute from any data source, regardless of whether that attribute's value changed? The time when the least-recently retrieved attribute was last successfully retrieved? Is there a reason this attribute is required and not just optional?	
6	6.1	24	890	There are a number of cases where an RP may need a full copy of the PIV cert that was used to authenticate (for example, this may be necessary for FAL3). Should that be considered a "core identity attribute", and use some standardized formatting (eg. PEM formatting without line breaks or with encoded line breaks)?	