

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

*Please submit responses to piv\_comments@nist.gov by March 24, 2023*

<b>Organization:</b>	Defense Manpower Data Center (DMDC)
<b>Name of Submitter/POC:</b>	
<b>Email Address of Submitter/POC:</b>	

Comment #	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
1	Gen	Gen	General	<p>For this specific draft standard, its creation in parallel with updates to Draft SPs 800-63 and 800-157 creates disconnects as those drafts evolve. Some of those disconnects are as follows:</p> <ul style="list-style-type: none"> <li>* Draft 800-157r1 states non-PKI-based authenticators can only be utilized locally, but they are discussed as a federated authenticator in 800-217.</li> <li>* Draft 800-63C-4 contains conflicting statements and requires more clarity for practitioners to understand clear delineations between FAL levels; once those are addressed, DMDC believes facets of 800-217 would need to be changed.</li> <li>* Draft 800-63-4/63C-4 lacks an uniform processes and identieirs for federal agencies to know an individual in federation trasactions resolve to the same John Smith that may already be known to a federal agency.</li> <li>* If a practitioner strictly reads 800-217, DMDC believes neither max.gov or login.gov could authenticate PIV cards – as they should be accepting assertions from the home agency.</li> </ul>	Recommend NIST rewrite this SP to reflect the final verisons of 800-63C-4 and 800-157r1.