Comment Template for: NIST SP 800-157r1 (Initial Public Draft)

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

Organization:	*Defense Manpower Data Center (DMDC)*
Name of Submitter/P	
Email Address of Subr	

omment	**Section**	**Page #**	**Line #**	**Comment** (Include rationale for comment)	**Suggested Change**
1	General			The notion that a Derived PIV can only be locally trusted contradicts the definition of a Derived PIV, which by its nature is an equivalent credential meant to be accepted across the trust fabric in lieu of the PIV. There is nothing in standards or technical specification that prohibit a PIV being used to validate identity for the issuance of authenticators meant for local trust only. Therefore, non-PKI authenticators cannot be DPIV.	Recommend clarification be added.
2	1.2	2	279-281	It is our believe that, by nature, a non-Common phishing-resistant authenticator cannot be considered a PIV authentication. However, it can be an approved authenticator to extend PIV-enabled authentication services to alternative endpoints.	Recommend changing sentence to "The purpose of the derived PIV credential is to provide ~~PIV-enabled~~ strong, phishing resistent authentication services ~~to extend PIV-enabled authentication services to alternative endpoints~~ on alternative endpoints in order to authenticate the credential holder to remote systems."
3	1.2	2	298-300	It is unclear what the other types of authenticators would be here that are out of scope, if the document is also discussing non-PKI derived PIV authenticators: While the PIV Card may be used as the basis for issuing other types of derived credentials, the issuance of these other credentials is outside of the scope of this document.	Recommend clarification be added.
4	2.2 C.2	7 26	425-432 997-998	It is our understanding this section identifies an additional requirement to verify the biometric on the PIV or PIV issuanceinf rastructure to create an AAL3 derived PIV credential.	: It would be helpful to understand the rationale or risk that is being mitigated for the additional step that does not exist for AAL2 derived PIV credentials, whereas user PIV PKI authentication alone is sufficient.
5	2.2	7	436-439	It is unclear what the values is for notifying the indivduals when an indivdiual requested new PIV derived crednetail is issued. This requirement seem to be lifted from a commercial best practice related to banking and access to commerical accounts. Government credentials for employees to access government IT assets has different criteria, risks, and implementations that make such unnecessary.	Recommend moving the "shall" to "may" for notifying indivduals.

6	2.2	7	436-439	What are examples notification methods "that would not afford an attacker the opportunity to interfere with the notification"?	Add Examples
7	3.1.1	11	578-581	Agree with this statement - this concept needs to be clearly articulated in 800-63A-4.	Recommend NIST clearly articulate the concept of transferrable IAL in 800-63A and -157r1
8	3.1.4	12	618-619	Note that this requirement cannot be met today, as mobile devices are not protecting the container with the derived PIV PKI certificates with a secret/biometric. Once the user gets into the phone, they have access to the PKI certificates without any additional user veriifcation.	Suggest NIST talk with the mobile device vendors to push them to protect the containers with a secret/biometric.
9	3.2.1	13	634-637	The Federal space is a unique one which, since 2004, has utilized PKI technology to aid in federation of a single PIV/CAC credential throughout an agency and - in theory - throughout the Federal government. In draft NIST 800-63-4, NIST is suggesting to change AAL3 (previously reserved for PIV/CAC/other methods of PKI with a PIN) to include phishing-resistant authenticators that are combined with other form factors to create MFA. While the DMDC agrees that phishing-resistant MFAs should be rated high within authentication levels, it does not agree that phishing-resistant authenticators should be at the same authentication level as PIV/CAC. In fact, draft 800-157r1 proves that PKI-based MFA must be treated differently than non-PKI MFA (e.g., the lifecycle management is vastly different and non-PKI authenticators can only be utilized locally). A user does not need to perform any additional steps after binding their PKI-based credential to their CMS to utilize that credential within their agency's systems. For a non-PKI authenticator to be used within an agency's systems, it must not only be bound to the agency CMS, but also to the individual IdPs that the user needs to authenticate to; additionally, the second factor to obtain AAL3 is bound to the IdP, not the authenticator. Similarly, if a user's PIV is terminated, the CMS can simultaneously revoke all PKI certificates that have been issued to the user - including those issued on mobile devices. The user would then be prevented from authenticating to the IdPs within the agency's network. However, if one of the user's derived PIVs was a non-PKI-based derived PIV, then the agency would be required to collect that phishing-resistant authenticator to ensure the prohibition of the user's unauthorized access to the network. While implementing joiner/mover/leaver principles within the agency's IdP would enable the agency to reduce the risk of unauthorized access, the best method would be to collect the authenticator. Because the only way to reach AAL3 with a non-PKI authenticator is with a single factor crytographic device and an additional factor that is bound to the IdP, not the authenticator, and because the only way to revoke a non-PKI authenticator is to collect it from the end user, non-PKI authenticators should *not* be in the same AAL as PIV/CACs in NIST 800-63B and in this document.	Recommend removing language that make phising resistence (non-PKI) authenticators the same AAL as PKIbased authenticators like CAC/PIVs.
10	B.2.1	24	948-952	Note that this requirement cannot be met today, as mobile devices are not protecting the container with the derived PIV PKI certificates with a secret/biometric.	Suggest NIST talk with the mobile device vendors to push them to protect the containers with a secret/biometric.
11	C.2	26	1004-1005	Unsure what "agency's endpoint" means in this context. A non-PKI authenticator will need to be bound to each individual IdP for the user to utilize that credential for authentication.	Recommend clarification be added.

12	C.2	26	992	There are no "a non-PKI-based authenticators" that can authenticate at AAL3 without adding an additional factor - such as a password. However, this use case assumes that the authenticator is only bound for authentication in the derived PIV website when, in fact, the end user must bind this authenticator at every IdP that they encounter.	Recommend removing AAL3 from the use case, perhaps change to phishing-resistent MFA