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

Security Industry Association
POC:

Comment #	Section	Page #	Line #	**Comment** (Include rationale for comment)	Suggested Change
1	1.1 Background	N/A	N/A	The language in this section does NOT inform the user of the difference between "derived" and "emulated."	As a derived PIV has no Signed CHUID data object, it remains inappropriate for certain envionments where a real PIV card or emulated PIV card would in fact work. This distinction is critical to
2	2.1	5	N/A	Figure 1, block "DPC Usage" is shown but this section (2.x) does not address as a sub block.	Add in a new Section 2 a paragaph or more on appropriate "DPC Usage." We suggest placeing "DPC Usage" prior to maintenace
3	General	N/A	N/A	Regarding the choice of authentication method by agency, consider how agencies set up their authentication systems. They basically have three choices: 1) Enable both PIV and "non-PKI based derived PIV credentials." 2) Enable just PIV methods: smartcard login, HTTPS with client cert authentication, etc. 3) Enable just non-PKI based derived PIV credentials. When considering whether all three possibilities would be allowed, or whether #3 should be discouraged, an implementing agency would need to ask what is the system, what data will it need, what risks exist (inherent and perceived), what level of inter-agency interoperability is needed and then determine how	

4	General	N/A	N/A	Regarding PIV use in mobile devices: In 2015, NIST stated- “The next generation PIV Card can be used with mobile devices, enabling federal employees to connect securely to government computer networks from such devices.” And, “A new specification protects wireless communications between the PIV Card and mobile device when the cardholder uses authentication, signature or encryption services with a mobile device.” However, in 2023, NIST writes in NIST.SP.800-157r1 - “While the use of the PIV Card for electronic authentication works well with many traditional desktop and laptop computers, it is not well-suited to other devices, such as mobile devices.” What prevents mobile devices from using a PIV card over NFC, with SP-800-73-4’s Secure Messaging & VCI? There is a lack of built in support for PIV SM in mobile phones that would allow the use of PIV card private keys in keychain operations. Cards that implement the SP-800-73-4 PIV secure messaging have	
5		ii	128-129	Cloning a PIV card with on-card generated keys is difficult, and thus the cardholder knows when they control it. But the possibility of temporarily gaining control of a PIV card (perhaps by "shoulder surfing" the PIN, and then using the card for a PIV-AUTH while the cardholder is distracted) and creating a bogus derived PIV AAL2 credential creates a new scenario. Even though the cardholder has the PIV card back in full control, they can’t be sure that a derived PIV credential was not created for a malevolent party. The PIV cardholder notification requirement attempts to mitigate this problem, but messages can be intercepted and deleted. Thus [for AAL3], "the applicant SHALL	
6	2.1		386-388	"Certificate modification is used ..." It should be emphasized that any/all certificate practices should follow the same practices that apply to PIV. Affecting the same lifecycle activities / actions.	
7	2.2		411-412	"Derived PIV Credentials SHALL be issued ..." Issuance of a derived credentials should be based on agency policy and risk	We suggest changing the word "SHALL" to "MAY" in this instance.

9	2.2		436-438	Notification to PIV holder. This statement is not well defined. Use of "independent means" is not clear. Examples of how that communication may occur would/should offer clarity, e.g. email to personal / work email, text to personal / work mobile	
10	2.3		488-493	"Derived PIV credentials are unaffected ....." This should be a home agency risk decision/policy statement to depict necessary	This paragraph should be identified as informative - home agency discretion needs to apply to this area and policy document for
11	2.3.1		508-514	"Some maintenance activities ....." appears/reads as an opinion. If this is a requirement, the issuing card management system workflow would need to enforce such situations. Additionally, policy should be written to support/enforce the	Determine if this paragraph is a requirement.
12	3.1.1		584-588	"The expiration date of a derive PIV authentication certificate ...." This paragraph reads as an "informative" statement not a	Move the statement/para to Section 2.
	3.3	14	663-668	This section merits to be placed at the beginning of Section 2 and not at the very end. The binding to PIV account is a prerequisite to all Drived PIV Credentials and/or MFA	
13	Appendix A	17	728-730	"…It will be necessary to store a copy of the PIV Card's key management private key and certificate in the keystore that hosts the derived PIV credential." Placing email encryption / decryption private key(s) in a third location creates an	Adjust language to address this concern.
14	2.2		417-420	Some have described a so-called "Pre-PIV" authenticator as providing quick issuance to new potential PIV cardholders. It is clear that a "Pre-PIV" authenticator issued before the PIV card can never be a derived PIV credential, and thus has no support in SP800-157 for access to any data/service that properly requires a PIV card.	Suggested addition to 2.2 – "Issuance of Pre-PIV authenticators may be deemed a useful alternative while an applicant awaits issuance of their PIV credential. A Pre-PIV (PKI or Non-PKI) authenticator would be an authenticator issued by the home agency based on PIV issuance practices, as no PIV PKI-Auth authenticator exists to issue/create a Derived PIV authenticator. Agencies MAY leverage the use of alternative PKI and non-PKI
	2.2.2	8	470-482	It should clarify and emphasize that agency cannot issue a MFA authenticator as a derived PIV without a prior PIV credential issuance. Also, given the emerging adoption of syncheable MFA authenticator (passkey), NIST should be clear on whether this authenticator as non PKI based derived PIV can be syncheable or	Change "physical authenticator" to single device bound security key.

15	All		102	When referring to home agency's responsibility to vertify or to authenticate an individual certificate based and non-certificate based credential, NIST should also reference home agency's	
16	All			Given NIST' current effort on on Migration to Post-Quantum Cryptography, will NIST review how to implement changes in PIV applet certification to accomodate the need of crypto agility, encryption algorithm patching, etc? Addressing how the FIPS 140-3 certification specification and process can be adopted to	