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

Please submit responses to piv_comments@nist.gov by March 24, 2023 ***- Revised comment deadline - April 21, 2023***

Organization:	***Idemia***
Name of Submitter/POC:	
Email Address of Submitter/POC:	

Comment #	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
	General Comment			Choice of authentication method by agency: Consider how agencies setup 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	
				Will all three possibilities be allowed, or should #3 be discouraged.	
				In general, an implementing agency would ask what is the system, what data it will need, what risks exists (inherent and perceived), what level of inter-agency interoperability is needed and then determine how auth would apply to the system.	
	General Comment		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 authorized service provider.	Throughout the document, we suggest to further clarify the term of home agency with "Home Agency or Home agency's autorized service provider".
	General Comment			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? How FIPS 140-3 certification specification and process be adopted to facilitate the deployment of derived PIV in post quantum era.	
	General Comment			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." "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."	
				In 2023, NIST writes in NIST.SP.800-157r1.ipd.pdf: "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 are two reasons:	
				1. Lack of built in support for PIV SM in mobile phones that would allow the use of PIV card private keys in keychain operations.	
				2. Issuer deployment of the PIV SM chain of trust. Cards that implement the SP-800-73-4 PIV Secure messaging have been available for years, but they are typically issued without the chain of trust and possibly with VCI disabled. The agencies need to push the CMSs to enable the feature.	
				As derived PIV is provisioned on mobile device, we encourage NIST CCOE to consider including derived PIV provisioning implementers to adopt ISO 18013-5 mDoc standard. By centering such standard, it will enable standardized solution development and adoption for device engagement (QR Code, BLE, NFC) and data engagement.	
		ii	128-129	Response to Question 3	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

					The PIV cardholder notification requirement attempts to mitigate this problem, but messages can be intercepted and deleted. [For AAL3] The applicant SHALL identify themself using a biometric sample that can be verified against their PIV Card or against the biometric information in their enrollment record.
	2.1	6	386-388	"Certificate modification is used ....." Any / all certificate practices should follow the same practices that apply to PIV. Affecting the same lifecycle activities / actions.	
	2.2	7	411-412	"Derived PIV Credentials SHALL be issued ....." Issuance of a derived credentials should be based on agency policy and risk decision making.	Derived PIV credentials MAY be issued by the any government sponsoring agency. Issuing agency should assess risk with issuance and only issue against validated PIV (PIVi) credentials. Issuing agencies will to accept / take the risk could manage the issued PIV-D by maintaining status of the PIV through periodic validation of the PIVAuth certificate. Such a capability could offer an alternative to Federation use cases.
	2.2	7	417-420	At the time of issuance, the applicant SHALL authenticate to the derived PIV credential issuer using their PIV Card. ***This authentication SHALL be performed using the PKI-AUTH authentication mechanism described in Sec. 6.2.3.1 of [FIPS201]*** .". Some have described a "Pre-PIV" authenticator as providing quick issuance for 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 authenticators to gain physical and/or logical within the home agency based on Agency policy and suitability.
	2.2	7	426-428	"The applicant SHALL identify themself using a biometric sample that can be verified against their PIV Card or against the biometric information in their enrollment record". This statement does not consider the issuance of a PIV Card w/o biometric information stored int he card or in the enrollment record. Additionally, this could be an issue for meeting / maintaining ADA compliance.	"The applicant MAY identify the themself .....". Add language to address issuance / validation for applicants without biometric information. Agency policy really should dictate these conditions.
	2.2	7	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 number, written correspondence, etc.	This is likely a discretionary area of an issuing agency, home agency policy should be defined for usage, application and added data (if needed) for communication the issuance act.
	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 not. Phyiscal Authenticator does not provide enough clarity.	Change "physical authenticator" to single device bound security key.
	2.3	9	488-493	"Derived PIV credentials are unaffected ....." This should be a home agency risk decision / policy statement to depict necessary actions.	This paragraph should be identified as informative - home agency discretion needs to apply to this area and policy document for maintenance / lifecycle activities.
	2.3.1	9	508-514	"Some maintenance activities ....." appears / reads as an opinion. If this is a requirement, the issuing card mgmt. system workflow would need to enforce such situations. Additionally, policy should be written to support / enforce the "requirement / actions".	Determine if this para. is a requirement. No suggested edit.
	3.1.1	11	584-588	"The expiration date of a derive PIV authentication certificate ....." This para reads as an "informative" statement not a technical requirement.	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 authenticators lifecycle acitivities	
	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 opportunity for an attacker to hunt and harvest the private keys.	