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

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

Organization: CertiPath, Inc.
Name of Submitter/POC:
Email Address of Submitter/POC:

Comment #	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
2	2.2	7	425-432	This paragraph makes a distinction between AAL3 and the other AALs in that it requires the use of a biometric as part of its identity proofing process for issuance of the DPIV. This doesn't make any sense. A DPIV, by its nature, is linked to the PIV. Identity Proofing for the DPIV holder should be the same across the board. In other words, there should be a consistent confidence in the DPIV holder's relationship to the PIV holder.	If a biometric sample is to be required to prove possession/ownership of the PIV card, make it a consistent requirement across all DPIV AALs.
	2.2	7	428-431	Appears self-contradictory. Needs to be clear that it applies to subsequent transactions.	If the issuance process consists of two or more transactions, the applicant SHALL identify themself during subsequent transactions using a biometric sample that can be verified against either their PIV Card or against a biometric that was recorded in a previous transaction.
	2.3.2	9	516-518	The use of "non-PKI-based Derived PIV Credential" would appear to be a misnomer. At best, they are tokens or authenticators. It is only their association with the PIV credential itself that gives them any credibility.	Recommend here and throughout the document, refrain from using the term 'credential' to describe the non-PKI Derived PIV authenticators.
	2.4	10	538-545	This paragraph is confusing. It is conflating termination with revocation and the given example is indicative of a situation in which it is not necessary to know the card was terminated regardless of revocation status to establish the viability of the associated DPIV.	The issuer of the derived PIV credential SHALL NOT solely rely on tracking the revocation status of the PIV authentication certificate as a means of tracking the termination status of the PIV Card. This is because there are situations in which the PIV authentication certificate is not revoked even though the PIV Card has been terminated ~~and subsequently replaced with a new card~~. This may happen, for example, when a terminated PIV Card is collected and either zeroized or destroyed by an agency. In this case and in accordance with [FIPS201], the corresponding PIV authentication certificate does not need to be revoked.
	3.1.1	11	575	This section title should be revised for accuracy. Certificate Policies only apply to PKI based credentials.	Proposed Section Title: Certificate Policies for PKI-based Derived PIV Credentials
	3.1.1	11	584-585	There is only one Certificate Policy associated with PIV and Derived PIV. It is the Federal Common Policy administered by the Federal PKI Policy Authority. Each implementing organization does maintain its own Certification Practice Statement, however.	The expiration date of a derived PIV authentication certificate must conform to the requirements for subscriber authentication certificates as specified in the *X.509 Certificate Policy for the Federal Common Policy Framework* ~~is based on the certificate policy of the issuer~~. Alternatively, remove the sentence altogether.
	3.1.3	12	606-612	This is PKI-based, either on a hardware token or a software token. It complies with the Federal COMMON Policy. Why is it being obfuscated with this language from SP 800-63? Why not just state that human activation is required - either a min. 6 digit alpha-numeric or biometric? And that it must be a hardware module for AAL3 and a software module for AAL2	Replace this section with some plain language, that the DPIV PKI credential requires activation using a 6 to 8 digit PIN or a biometric and that a hardware module that does not allow export of key is required at AAL3.
	3.1.4	12	614	For clarity's sake, it should clearly indicate that this section refers to PKI-based PIV credentials	Activation of the PKI-based derived PIV authenticator using a memorized secret SHALL meet. . .
	3.1.4	12	625-628	The sentence beginning "If the PUK is not implemented by the authenticator. . ." is confusing. The term "authenticator" seems misplaced here. Once again, if we're talking PKI-based DPIV, why not just say "private key"	If the PUK is not implemented by the private key ~~authenticator~~or cannot be provided, either the associated public key ~~authenticator~~ certificates SHALL be revoked or the ~~associated~~ private keys SHALL be destroyed or zeroized.
	3.2	13	630	"When used, non-PKI-based credentials SHALL be used to authenticate only to the home agency of the associated PIV Card." In actuality, these are not DPIV credentials, but Locally-Trusted Only authenticators. If they were DPIV they could be presented in lieu of a PIV card for interagency authentication.	Strike all reference to non-PKI authenticators as DPIV.
	Appendix C	25-26	953-1012	I find it interesting that the choice was made to give a PKI example at AAL2 and a non-PKI example at AAL3. PKI technology is sufficiently distinct from any other type of authenticator that an example of the issuance process of some unspecified non-PKI authenticator would have no relationship for the issuance process for a PKI credential. It is also more efficient to use PKI at AAL3 than to shoe-horn some other technology at this level.	Instead of establishing an AAL for these two examples, recommend being AAL agnostic and simply describe the on-boarding process for each type of credential. Determination of the AAL is external to the actual credential or authenticator type.
	C.2	26	989	This section title should indicate that this is a non-PKI authenticator. Unlike Section C.1. this section does not begin with a declaration of the type of authenticator.	Example Binding of a non-PKI-based Derived PIV credential at AAL3