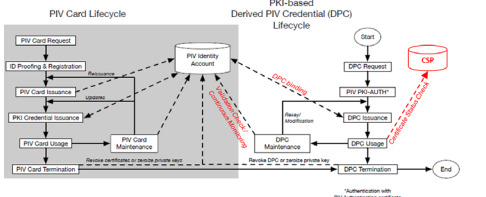
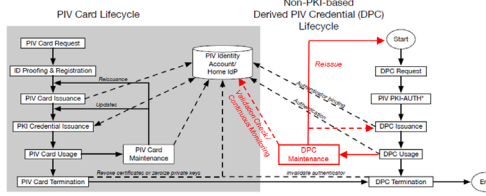


**Comment Template for: NIST SP 800-157r1 (Initial Public Draft)**

Please submit responses to [piv\\_comments@nist.gov](mailto:piv_comments@nist.gov) by ~~March 24, 2023~~ April 21

<b>Organization:</b>					<b>Secure Technology Alliance - Identity &amp; Access Forum</b>	
<b>Name of Submitter/POC:</b>					April 18, Team Meeting	
<b>Name of Participants</b>						
Comment #	Commenter	Section	Page #	Line #	Comment <i>(Include rationale for comment)</i>	Suggested Change
					<p>Comment: It's not clear what non-PKI credentials are being addressed in the draft (and this comment extends to SP-800-63). Lack of definition undermines the intent of the document.</p> <p>There is a growing interest in the concept of alternative non-PIV (for example mDLs, mIDs)/Non-PKI (FIDO) derivative/extended credentials. As these concepts and capabilities mature, these may be worthy of and should be addressed within a separate document.</p>	<p>Recommendation: Since it's not clear what non-PKI credentials are being addressed in the draft, the concept of non-PIV/Non-PKI derivative/extended credentials should be addressed within a separate document that accounts for other capabilities when non-PKI credentials are better defined. SP 800-63 and SP 800-157 need to be more explicit on what non-PKI credentials are being envisioned (for example FIDO, Mobile Credential not FIDO). If clarity cannot be provided regarding references to non-PKI credentials, then they should be removed from the 800-157 draft, and thus, NIST SP-800-157 r1 Guidelines for Derived PIV Credentials should focus exclusively on PKI based credentials and their enablement</p>
	Andrew Webb	General Comment			Choice of authentication method by agency: Consider how agencies setup their authentication systems they basically have three choices.	
					<p>1) Enable both PIV and "non-PKI based derived PIV credentials "</p> <p>2) Enable just PIV methods: smartcard login, HTTPS with client cert authentication, etc</p> <p>3) Enable just non-PKI based derived PIV credentials</p> <p><b>Will all three possibilities be allowed, or should #3 be discouraged.</b></p> <p>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.</p>	
	Andrew Webb	General Comment			PIV Use in Mobile Devices	
					<p>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."</p> <p>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 What prevents mobile devices from using a PIV card over NFC, with SP-800-73-4's Secure Messaging &amp; VCI? There are two reasons:</p> <p>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.</p> <p>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.</p>	

	Mark Dale	Note to Reviewers	i		Regarding initial section "Note to Reviewers": "The draft details the expanded set of derived PIV credentials in a variety of form factors and authenticator types as envisioned in OMB Memoranda M-19-22, M-22-09, and subsequently outlined in FIPS 201-3." Is M-19-22 (i.e., "Evaluating and Improving the Utility of Federal Advisory Committees") the correct relevant reference? M-19-22 has no mention of "derived".	It's understood that this section is Note to Reviewers, and won't be in the final publication, but does NIST mean "OMB M-19-17" instead of M-19-22? Also, 800-157 r0 provides OMB guidance/authority by referencing OMB M-06-16 and M-07-16. Recommend r1 make similar references to M-19-17 and M-22-09's influences on the r1 draft.
						The PIV cardholder notification requirement attempts to mitigate this problem, but messages can be intercepted and deleted.
						[For AAL3] The applicant SHALL identify themselves using a biometric sample that can be verified against their PIV Card or against the biometric information in their enrollment record.
	SIA - Multiple Providers (Idemia, Thales... Card Manufactures)	Note to Reviewers	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. [For AAL3] The applicant SHALL identify themselves using a biometric sample that can be verified against their PIV Card or against the biometric information in their enrollment record.	
	Andrew Webb	General	N/A	N/A	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	Also an SIA comment as well
	SIA - Jake Parker	General	N/A	N/A	What prevents mobile devices from using a PIV card over NFC, with SP-800-73-4's Secure Messaging & VCI?	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 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.
	Mark Dale	General/Other	N/A	N/A	<b>Physical Access:</b> OMB M-19-17 states: "The Department of Commerce (DOC) is responsible for the following actions: ... Develop guidance to facilitate deployment and use of derived credentials for logical and physical access using authenticators that satisfy the security and privacy requirements of NIST SP 800-63 while leveraging the PIV identity proofing process;" SP 800-157 is focused on accessing remote IT systems using derived credentials and has no references	Suggest including considerations for using derived credentials for physical access per OMB M-19-17 and what various agencies (GSA, DHS, FEMA, DOD/DMDC) are independently exploring for using mobile devices for physical access; e.g., conducting demos/pilots, RFI's and RFPs. Thus suggesting, providing guidance to these independent agencies re. derived credentials for physical access.
	Gerald Smith	1.1 Background	5	N/A	The language in this section does NOT inform the user of "derived" versus "emulated". Etc.	As a derived PIV has no Signed CHUID data object, it remains inappropriate for certain environments where a real PIV card or emulated PIV card would in fact work. This distinction is critical to implementers understanding this point.
	Mark Dale	1.1 Background	1	253	Section 1.1 - (Background) " <b>Non-PKI-based derived PIV credentials ..</b> " SP800-63/A/B/C-4 docs do not contain, nor define, the term "non-PKI". However, SP800-63B-4 does mention FIDO and Verifiable Credentials in the "Notes to Reviewers" section, and is assumed to be referencing non-PKI-based derived credentials.	Suggest providing a better understanding of the scope of what a non-PKI derived credential is, and reconciling the definition and use of the term "non-PKI" between the 800-157 and 800-63/A/B/C draft standards. (see major comment above)
	Mark Dale	1.1 Background	1	253	Section 1.1 - (Background) i " <b>Non-PKI-based derived PIV credentials are authenticators (as defined in [SP800-63B]) ...</b> ". This is the first mention of the term "authenticators" in the draft. SP800-63B-4 defines "authenticator types" that can be anything from a "Memorized Secret" to a "Multi-factor cryptographic device". For non-PKI derived credentials, it is not clear what authenticator types are relevant until one gets to sections 3.1.3 and 3.2.1 in the 157 draft; i.e., multi-factor or single-factor cryptographic authenticators (software or device), or implicitly in Section 1.2, line 274.	Suggest moving sentence at line 274 (Section 1.2 Purpose and Scope) up into Section 1.1, before mentioning non-PKI derived credentials, and include references to section 3.2.1 and 3.2.1. e.g., "Authenticators used as derived PIV credentials must meet the requirements for either hardware or software cryptographic authenticators, as specified in Sections 3.1.3 and 3.2.1."
	Mark Dale	1.1 Background		253	Section 1.1 - (Background) " <b>Non-PKI-based derived PIV credentials are authenticators (as defined in [SP800-63B]) that may be separate from the endpoint being authenticated and, if so, are connected to the endpoint for that purpose.</b> " Had to reread this sentence several times to get the gist of "are connected to the endpoint for that purpose". It's not clear what the word "purpose" is referring to --authentication of an authenticator?	Remove "and, if so, are connected to the endpoint for that purpose", or better state the meaning of it. For example: " <b>Non-PKI-based derived PIV credentials are authenticators (as defined in Section 3.2.1) that may be separate from the endpoint being authenticated, and, if so, the endpoint provides identifying linkage to the separate authenticator, which relying parties/home agencies can validate out-of-band/online from the endpoint (such as a non-PKI derived credential record in a database, directory, online ledger or other trusted authenticator repository).</b> "
	Mark Dale Randy Bowman	General/Glossary	N/A	N/A	<b>Endpoint Definition:</b> "Endpoint" should be defined and used consistently between drafts SP 800-157 and SP 800-63.	Add "Endpoint" to the "Glossary" in 800-157 and "Definitions and Abbreviations" in 800-63-4. Also, in the "Definitions and Abbreviations" in 800-63-4, modify the definition of "Session" where it implies that an "endpoint" is a relying party or CMS, not a user device hosting an authenticator. For example, would virtual smartcard Windows Hello for business be considered as an authenticator (TPM)

Mark Dale					<p><b>Regarding initial section "Note to Reviewers":</b> "The draft details the expanded set of derived PIV credentials in a variety of form factors and authenticator types as envisioned in OMB Memoranda M-19-22, M-22-09, and subsequently outlined in FIPS 201-3." Is M-19-22 (i.e., "Evaluating and Improving the Utility of Federal Advisory Committees") the correct relevant reference? M-19-22 has no mention of "derived".</p>	<p>It's understood that this section is Note to Reviewers, and won't be in the final publication, but did you mean "OMB M-19-17" instead of M-19-22? Also, 800-157 r0 provides OMB guidance/authority by referencing OMB M-06-16 and M-07-16. Should r1 make similar references to M-19-17 and M-22-09's influences on the r1 draft?</p>
Mark Dale	Section 2	N/A	N/A	N/A	<p>OMB M-19-17 states: "The Department of Commerce (DOC) is responsible for the following actions: ... Develop guidance to facilitate deployment and use of derived credentials for logical and physical access using authenticators that satisfy the security and privacy requirements of NIST SP 800-63 while leveraging the PIV identity proofing process;" The 800-157 r1 draft has no references to using derived credentials for physical access. Derived credentials are viable as credentials for using mobile devices for physical access control.</p>	<p>Suggest including considerations for using derived credentials for physical access per OMB M-19-17 to the extent that DOC developed any related guidance, or anything related to what various agencies (GSA, DHS, FEMA, DOD/DMDC) are independently doing for using mobile devices for physical access; e.g., conducting demos/pilots, RFI's and RFPs. THUS suggesting, providing guidance to these independent agencies re. derived credentials for physical access.</p>
Gerald Smith	2.1	5	5	N/A	<p>Figure 1, block "DPC Usage" shown but this section (2.x) does not address as a sub block.</p>	<p>Add in new Section 2 a paragraph or more on appropriate "DPC Usage". Suggest place "DPC Usage" prior to maintenance and after issuance.</p>
Mark Dale	2.1. Derived PIV Credential Lifecycle Activities	5	5	379	<p><b>Figure 1:</b> 1. The line between "DPC Usage" and "PIV Identity Account" should be labeled with something like "DPC Binding", which reflex the requirement for binding the authenticator and/or DPC to the PIV Identity Account, per 800-63 and FIPS 201-3. 2. Add another dashed line for "Authentication", as exists in Figure 2. During DPC Usage/Authentication, the relying party may check the status of the certificate with the CSP associated with the PIV Identity Account. See notional suggested changes.</p>	 <p>Figure 1. PKI-based derived PIV credential lifecycle activities</p>
Mark Dale	2.1. Derived PIV Cre 6	6	6	386	<p><b>Figure 2:</b> As stated at the beginning of Section 2, line 366 - "The lifecycle activities for a derived PIV credential are initial issuance, maintenance, and termination." Thus, "Maintenance" applies to both PKI and non-PKI derived credentials. Add "DPC Maintenance" to Figure 2, as is done in Figure 1. <b>Also,</b> Line 391 states - " Instead of re-keying, the current non-PKI-based derived PIV credential SHALL be invalidated and the initial issuance process (except for the device or authenticator approval process) repeated to bind a new derived PIV credential. " See notional suggested changes.</p>	 <p>Figure 2. Non-PKI-based derived PIV credential lifecycle activities</p>
Bill Windsor	2.1			386-388	<p>"Certificate modification is used .....". Any / all certificate practices should follow the same practices that apply to PIV. Affecting the same lifecycle activities / actions.</p>	<p>It looks like this section is not following normal PKI maintenance - reference FPKIPA policies and practices.</p>
Mark Dale	2.1 Derived PIV Credential Lifecycle Activities 2.2.2. Non-PKI-based Derived PIV Credential Issuance	5	8	389 471	<p>Non-PKI Derived Credential Physical Authenticators: Line 389 - "While non-PKI-based derived PIV credentials are not typically re-keyed and do not contain PII about the subscriber, they may require maintenance, such as replacing the activation secret or biometric factor used to activate the physical authenticator." Line 471 - "The applicant SHALL be provided with or supply an approved physical authenticator for the highest AAL that the [non-PKI] derived PIV credential will be used to authenticate."</p>	<p>Line 389 - Since, there is no defined contextual understanding of what "non-PKI" credentials that are being addressed, whether or not they are typically re-keyed, whether or not they may contain PII about the subscriber. or whether or not their authenticators are "physical" -- suggest changing Line 389 to: "Non-PKI-based derived PIV credentials may require maintenance, such as replacing the activation secret or biometric factor used to activate the [delete "physical"] authenticator."  Line 471 - "The applicant SHALL be provided with or supply an approved [delete "physical"] authenticator</p>
Bill Windsor Andrew Webb Tom Lockwood Tim Baldrige Mark Dale	2.2			411-412	<p>"Derived PIV Credentials SHALL be issued .....". Issuance of a derived credentials should be based on agency policy and risk decision making. If the expanded use of derived PIV credentials is envision, relying parties/other agencies need to make an informed decision based-on-risk. If so, it should be inclusive not exclusive of relying parties (should be within the theming/perview of SP-800-217 core principles).</p>	<p>Derived PIV credentials MAY be issued by any government sponsoring agency. If so, the issuing agency should assess risk with issuance and only issue against validated PIV (PIVI) credentials. Issuing agencies will 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.</p>

Bill Windsor Teresa Wu	2.2		234 Parallel discussion on: 417-420	Some have described a so-called "Pre-PIV" authenticator as providing quick issuance 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. A Derived PIV card may only be issued bound to a valid PIV subscriber account.	Because it's a pre-requirement, the discussion needs to added to the introduction section - a Derived PIV card may only be issued bound to a valid PIV subscriber account. This needs to be clear within the introduction, section 1 at line 234.
Bill Windsor	2.2		436-438	Notification to PIV holder. This statement is not well defined. Use of "independent means" is not clear. Strategic intent needs to be clarified to provide through 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 of the issuance act.
Mark Dale	2.2.1. PKI-based Derived PIV Credential Issuance	8	455	"CSP" is used for the first time - it should be defined (certificate service provider; credential service provider - clear differentiation is required). Note spelled wrong on line 1061. FYI, there is a conflict of the definition of the acronym "CSP" between this 800-157 draft's Appendix E, i.e., "Certificate Service Provider"; and 800-63B-4 draft's Section 1, i.e., "Credential Service Provider".	For contextual readability and understandability, suggest spelling it out for this first time use; i.e., "Certificate Service Provider".
Bill Windsor	2.3		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 - while it may be unaffected - it should be emphasised the home agency discretion needs to apply to this area and policy document for maintenance / lifecycle activities.
Bill Windsor	2.3.1		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. If a requirement, examples should be provided.
Mark Dale	2.3.2. Non-PKI- based Derived PIV Credential Maintenance	9	516	"The maintenance activities for non-PKI-based derived PIV credentials are somewhat simpler than for PKI-based derived PIV credentials since the former do not contain information about the cardholder and do not carry a specific expiration date."  With this statement, it's unclear what types of non-PKI DPCs NIST has in mind and/or envisions. In the draft SP800-63-4, the "Notes to Reviewers" section lists "FIDO passkey, Verifiable Credentials" as "emerging authentication models and techniques", which may be considered as non-PKI DPC candidates. Some candidate non-PKI credentials (e.g., FIDO authenticator with "extensions") can contain attributes within the authenticator, which might contain cardholder information necessary for authentication and/or authorization for specific use cases for accessing home agency resources.	Suggest that SP800-157 not limit the potential characteristics/features of some non-PKI DPCs that may contain more descriptive attributes, other than identifiers and authenticators, that can be used to derive privileges during access requests to relying party resources.  If the intent of this version of SP 800-157 is to set a requirement that non-PKI derived credential authenticators are only to contain identifiers and/or asymmetric keys, and any other credential-holder attributes (e.g., expiration date) (that might be needed to establish access to relying-party resources) are to be maintained in a home-agency derived credential account (external to the non-PKI authenticator), then it should be stated.
Bill Windsor	3.1.1		584-588	"The expiration date of a derive PIV authentication certificate ....." This para reads as an "informative" statement not a technical requirement.	If a requirement, move the statement / para to Section 2. If not a requirement - recommend deleting.
Tim Baldrige	3.2	13	630-31	Should include home agency authorized credential validators for the associated PIV account.	When used, non-PKI-based credentials SHALL be used to authenticate only to the home agency and/or its authorized credential validators of the associated derived PIV credential.
Andrew Webb	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. This should be restated as optional.	Proposed change - Subscribers may store copies of the PIV Card's key management private key.... at the start  731 change "should" to "may" be stored in the derived...