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

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

Organization:	*Department of Energy (DOE)*
Name of Submitter/POC:	
Email Address of Submitter/POC:	

Comment #	Section	Page #	Line #	(Include rationale for comment)	Suggested Change
1	1.2	2	297-298	It is often best practice not to have the Credential Management System bind and write directly to the authoritative data source, which is commonly associated to the PIV Identity Account. This allows for separation from the Derived Credential Management System, the PIV Identity Management System, and the authoritative record (such as an HR record). It is true that all three records should, or even shall, be linked, but these databases or directories are usually separated. The language should be updated to allow for the binding to occur to a record that is linked to their PIV identity account, rather than directly to the account.	
2	2.2	6	426-428	The ability to validate a biometric sample during issuance of a Derived PIV Credential for intended use of AAL3, and compare that sample against the PIV Card or against the biometric information in the enrollment record is not reflective of current capabilities of solutions today. Additionally, there does not appear to be an additional security benefit for requiring this biometric authentication, as biometric authentication with a PIV card for logical access is not commonly used by agencies. The language should be updated to make this a SHOULD or MAY versus a SHALL statement.	Biometric checks should be part of identity proofing and primary credential issuance. Derived credentials leverage the work already done to verify a user's identity, including the biometric collection and comparison. Authentication with the primary authenticator should be sufficient for enrolling a new authenticator in a separate CSP at the same level. Either remove this stringent requirement or make is SHOULD or MAY
3	2.2	7	434-435	This change more accurately reflects the relationship between agencies and USAccess and other Shared Service Providers for PIV Card issuance.	This is currently not doable. This requirement is for USAccess and other Shared Service Providers for PIV Card issuance
5	2.3.1	9	508-511	We can state that certain PIV maintenance activities SHALL mean that a new derived PIV certificate be issued and the previous one invalidated, but in cases where the PIV and the derived PIV service providers are not one and the same, how can that SHALL be reasonably achieved unless PIV service providers are somehow aware that a credential has been derived from the PIV credential and can then alert about the PIV maintenance activities to either the derived credential holder themselves or to the service provider who issued the derived credential? This feedback applies to section 2.4 Invalidation as well. What linkage will there be between the PIV and derived PIV issuance systems for one to be aware of what activities occur with the other?	We can state that certain PIV maintenance activities SHALL mean that a new derived PIV certificate be issued and the previous one invalidated, but in cases where the PIV and the derived PIV service providers are not one and the same, how can that SHALL be reasonably achieved unless PIV service providers are somehow aware that a credential has been derived from the PIV credential and can then alert about the PIV maintenance activities to either the derived credential holder themselves or to the service provider who issued the derived credential? This feedback applies to section 2.4 Invalidation as well. What linkage will there be between the PIV and derived PIV issuance systems for one to be aware of what activities occur with the other? **Either change SHALL to SHOULD or remove this requirement**
6	2.3.2	9		While it is true non-PKI-based DPCs do not contain expiration dates, there should be some standardization around token/security key expiry, and where that should reside. Ideally, the issuing Derived Credential Management System for the Non-PKI DPC *should* contain or be responsible for maintenance of this record, and expiry *should* be made available to the IDP during authentication. This would better align non-PKI-based DPCs with PKI-based DPCs, and allow agencies to address challenges of managing the maximum allowable age of deployed tokens/security keys. ATARC had vendors demonstrate this capability where they bound a configurable expiry of the token/security key to the DPC user.	
7	2.4	10		Termination of a PIV Card does not correspond with a loss of trust for the PIV Authentication Certificate. Commonly, this represents the expiry of a PIV Card, and the user may receive a new PIV card. By binding directly to the status of the PIV Card, as written in section 2.4, Derived PIV Credential lifetimes cannot remain independent from the PIV Card. This means should the user damage their PIV card, they will not have a fallback credential for use to login, as was the intent of the Derived PIV Credential in NIST SP 800-157. Additionally, it is possible for a PIV Card or Certificate to be compromised after issuance of a Derived PIV Credential. In this scenario, the integrity of the Derived PIV Credential is not compromised, as the DPC represents a cryptographically separate credential from the PIV Authentication Certificate. Should the binding occur, as is suggested in section 2.4 of this draft, this valid DPC would need to be invalidated, leaving the user without a credential for authentication, which, again, strays from the original intent of NIST SP 800-157. Invalidation of the DPC should remain against the Derived PIV Credential Eligibility, which is tied to the PIV Eligibility, of a user. The exception should be a brief calendar window after issuance in which a compromised PIV Card or Credential could have been used to issue a Derived PIV Credential. In this scenario, and in accordance with FIPS 201-3, the corresponding PIV Authentication Certificate SHALL always be revoked.	This requirement is applicable only when a user terminates his relationship with their agency.
8	missing			The current draft does not have guidance on attestation of the derived non-PKI credential/device	Guidance with regards to attestation during for example during enrollment of the derived non-PKI credential.
9	3.1.1	11		This statement is in conflict with section 2.4 of the draft, as invalidation of the Derived PIV Credential is suggested to be set directly to the PIV Card. Expired PIV Cards are supposed to be collected and zeroized, which would make any Derived PIV Credential whose lifetime exceed that of the PIV Card containing the PIV Authentication Certificate used to issue the DPC not relevant.	This requirement is applicable only when a user terminates his relationship with DOE. Hence this row can be removed
10	missing			Recommend adding a requirement for supply chain attestation to establish trust for the home agency to be able to prove the origin of all authenticators accepted for authentication.	Recommend adding a requirement for supply chain attestation
11	3.2	13		The guidance should ensure/enforce non-PKI-based credentials can only be associated/authenticated to the home agency to prevent a user from registering their non-PKI-based authenticator against multiple derived credential management systems.	Recommend adding a guidance to ensure/enforce non-PKI based credentials can only be associated to the home agency

12	3.2.2	13		Section 3.2.2 omits any reference to an attribute associated with the non-PKI Derived PIV Credential. This is in contrast to the object identifier referenced for PKI-based DPCs where either hardware or software PKI-based DPCs can be identified. This reduces the usability of non-PKI DPCs during authorization, as there is no common attribute standard for identification of the level and type of DPC being used for authentication by the user. ATARC received demonstrations by vendors showing the ability to associate an attribute within the Derived Credential Management System record, which can be linked to the PIV Identity Record, which identifies the DPC as a non-PKI DPC, and whether that non-PKI DPC is software or hardware based in accordance with AAL2 or AAL3. This attribute was then demonstrated as being possible to examine and enforce through the federation system of a non-PKI Derived Credential Solution, to provide attestation during authentication of the type and trust of the DPC associated with the authentication event. Furthermore, this allows for auditable logging of authentication. NIST should reconsider the omission of a defined attribute for the identification of a non-PKI DPC. Without a standardized attribute defined by NIST, interoperability between agencies will be reduced, as each agency is likely to implement their own attribute type. While the non-PKI DPC is not intended to be authenticated directly by an agency other than the home agency of the user, federation does, and should, allow for the passing of attributes associated with the type of credential used for authentication to be used by the interoperating agency for authorization decisions. NIST could allow for the inclusion of an identifier/attribute, similar to the object identifiers found within an x.509 certificate, within a non-PKI credential and/or require this identifier/attribute within the Derived Credential identity record.	