ATARC Identity Management Working Group Comment for NIST SP 800-217

Overall, the ATARC Identity Management Working Group did not find anything within the draft release of NIST SP 800-217 that we wished to comment on directly. With that said, the working group wishes for NIST to consider expanding this current draft, or suggest NIST to create a follow-up special publication for the purpose of creating technical guidelines for federation implementation.

The current draft of NIST SP 800-217 does not currently contain any naming schemas for those attributes required to be included within an OIDC or SAML federation. This could be detrimental to interoperability within and between agencies.

Within an agency, application developers currently do not have a standard to develop against. This has led to different interpretations of standard attributes. For example, some applications accept userprincipalname for the subject identifier, while others want samaccountname or email. This requires IDPs to be flexible in their attribute schema. This also has slowed the adoption of federation, as each application must be examined to understand which attributes can be accepted, and in which format those attributes need to be presented. As the government looks to adopt a federated identifier, as identified within NIST SP 800-217, application owners, especially those that service multiple agencies and departments, are likely to continue to implement different naming structures without a common standard.

Between agencies, the lack of a formal standard for attributes, especially with the beforementioned federated identifier, will require each agency to examine the attribute naming structure of the other agency, and modify their federation agreement(s) accordingly. This attribute mapping will be required for each agency, and, potentially, for each shared application between agencies.

What is needed is a more formal set of guidelines for attribute naming. This should be similar to how NIST defined the PIV Applet standard within the NIST SP 800-73 series. The release of NIST SP 800-73 gave application owners and industry vendors a defined structure to develop against and has resulted in a more interoperable smart card solution than would likely have occurred without this direct guidance from NIST. While it would not be practical for NIST to define the naming structure of every possible attribute, the common attributes for use by the federal government ought to be defined.

Section	Context	Comment
2.3.2	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. Identity information SHALL be maintained in the PIV identity account and SHALL be updated when needed.	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.
1.2	Instead, the user proves possession and control of a valid PIV Card to bind a derived PIV credential to their PIV identity account.	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	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.	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.

2.2	The newly issued derived PIV credential SHALL be represented in the cardholder's PIV identity account.	Comments for this are the same as previous comments for 1.2. Furthermore, this would likely require the PIV Identity Management System to be the issuer of the Derived PIV Credential, as that is likely the only system with write access to the PIV identity account record. Instead, having a link between the home agency's authoritative record used for identification of PIV eligibility, the PIV Identity record in the PIV Identity Management System, and the Derived Credential Management System allows for greater flexibility in the systems able to issue a Derived PIV Credential, and still allows for centralized management of all credentials should the user no longer be PIV Eligible, or Derived PIV Eligible. This change more accurately reflects the relationship between agencies and USAccess and other Shared Service Providers for PIV Card issuance.
2.2	N/a- missing	The issuance criteria for Derived PIV Credentials in NIST SP 800-157r1 omits the previous requirement to perform reauthentication of the presented PIV Authentication Certificate after successful issuance of a Derived PIV Credential. This omission should be revised, and the revocation check (previously identified to be performed 7 days after issuance in section 2.2 in NIST SP 800-157) should be included. This is necessary as it allows for a grace period for the user to identify their PIV Card and/or PIV Authentication Certificate has been compromised, and a mechanism for the agency to identify any Derived PIV Credentials issued against this compromised credential. ATARC has received demonstrations from Vendors showing the ability to perform these re authentication revocation checks, and the ability to revoke the corresponding Derived PIV Credential (including Non-PKI DPCs) using commercial off the shelf technology.

2.4	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.	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 for 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.
3.1.1	There is no requirement to align the expiration date of a derived PIV authentication certificate with the expiration date of the PIV authentication certificate or the expiration of the PIV Card.	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. As written, this draft would make any Derived PIV Credential whose lifetime exceeds that of the PIV Card containing the PIV Authentication Certificate used to issue the DPC not relevant.
3.2	When used, non-PKI-based credentials SHALL be used to authenticate only to the home agency of the associated PIV Card.	This statement does not contain guidance to ensure/enforce non-PKI-based credentials can only be associated/authenticated to the home agency. There is no guidance in this document to prevent a user from registering their non-PKI-based authenticator against multiple derived credential management systems. What is needed is the requirement for supply chain attestation, where the home agency must enforce only non-PKI-based authenticators belonging to that agency can be bound to the user account. This establishes trust for the home agency to be able to prove the origin of all authenticators accepted for authentication. ATARC had vendors to demonstrate this capability. NIST should update the language to provide guidance on how to enforce this SHALL statement.

3.2.2	N/a- missing	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 from NIST SP 800-63b. This attribute was then demonstrated as being possible to examine and enforce through the federation system of a non-PKI Derived Credential solution. This provides attestation during authentication of the DPC type and AAL of the DPC associated with the authentication event. Furthermore, this allows for auditable logging of the authentication event(s). 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 should, and does, 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,