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

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

| | |
|---|---|
| ***Organization:*** | *Electrosoft Inc* |
| ***Name of Submitter/POC:*** | |
| ***Email Address of Submitter/POC:*** | |

| Comment # | Section | Page # | Line # | Comment<br>(Include rationale for comment) | Suggested Change |
|---|---|---|---|---|---|
| 1 | 1.2 | 2 | 270 | Purpose and scope does not currently address using PIV credentials installed on alternate tokens and mobile devices for contactless authentication for Physical Access Control System (PACS). | We would like this section to add information about using the mobile devices and hardware tokens (e.g., FIDO tokens) that support a contactless interface to be leveraged for PACS authentication. As you do in line 292, please add how AAL 2 and AAL 3 may impact SP 800-116r1 for moving between security areas.<br>Further, since Derived is for both logical and physical, please consider reworking the format of the document to highlight both -- either by (1) clearly differentiating LACS requirements vs PACS requirements section by section, (2) creating a 157A for LACS purposes and a 157B for PACS purposes (like 800-63 is a suite of documents), or adding a PACS appendix. We believe this will greatly help readers in the future. |
| 2 | Appendix A | 17 | 721 | Unclear why Digital Signature certificate and key management certificated are not specified as Derived whereas the other certificates discussed in the document are specified as Derived. These certificates are derived in that, like the other certificates, come from authenticating with the PIV Auth Certificate -- just like the other Derived certificate. | Please clarify and if necessary, update the document to specify the aforementioned certificates as Derived. |
| 3 | 2.2 | 7 | 411 | Unclear whether "Derived PIV credentials SHALL be issued only by the home agency of the associated PIV identity account." impacts Shared Services, if at all. | Please elaborate in the document how this statement, if at all, impacts Shared Service Providers. |
| 4 | 2.2 | 7 | 412 | Unclear whether "Derived PIV credentials SHALL be issued only to devices (such as mobile devices) or authenticators that are approved by the home agency." still needs to meet cryptographic requirements for the certificates issued to the devices -- needs to meet FIPS and be approved by home agency. | Please elaborate in the document whether meeting cryptographic requirements for the certificates issued to the devices is indeed still required. |
| 5 | 2.2 | 7 | 441 | Regarding "Derived PIV credentials SHALL meet the requirements for authentication assurance level (AAL) 2 or 3 specified in [SP800-63B]." -- It is our belief that most Derived credentials will be AAL2, which begs the question of how will AAL2 Derived credentials move between physical locations as discussed in NIST SP 800-116. FYI: cannot get to AAL3 unless biometric. | Please address this issue in this document and in NIST SP 800-116 whenever it opens for comment. |
| 6 | 2.2.1 | 8 | 465 | Regarding "The private key SHALL be stored on the device in a manner that makes it accessible only upon entry of the correct activation secret or presentation of a biometric factor that matches a stored biometric image or template." -- this would not be the case for PKI-CAK (regular or derived) and SM-AUTH, which will involve a contactless free-read (i.e., no activation) approach. | Please update this text to account for all contactless free-read data objects available for PIV in SP 800-73-4. PACS use cases often include Registration and Time of Access. We believe that activation of the PIV Card is required at time of registration. During registration, the fingerprint templates are stored on the PACS server. Time of Access should be allowed to authenticate using PKI-CAK and BIO from CTE without requiring an activation secret. |
| 7 | 3.1.1 | 11 | 576-578 | Since we propose supporting a PKI-CAK (PIV or Derived PIV) and SM-AUTH for non PIV Cards (alternate tokens), we need to investigate what certificate policies are applicable. | Please coordinate with the FPKI Policy Authority to determine whether any new/different certificate policies are needed for PKI-CAK and SM-AUTH for contactless use on alternate tokens, and if so then please update this section accordingly. Are all PIV authenticators issued via the Derived PIV process AAL 2 or 3? |
| 8 | 3.1.1 | 11 | 578-581 | Regarding "All derived PIV credentials SHALL be deemed to satisfy [SP800-63A] IAL3 since that is the identity proofing and issuance level associated with the PIV Card and bound to the PIV identity account. How do we address this with PKI-CAK alternate tokens when Common policy says no identity assurance is allowed to be associated with the PKI-CAK certificate? Our concern is how this might impact PACS use cases.<br>See also NIST SP 800-116 Section A.3 which states, "the PKI-CAK authentication mechanism is to authenticate the card and therefore its possessor."<br>See also NIST SP 800-116 Section A.3 which states, ""The PKI-CAK authentication mechanism is unique among the PIV authentication mechanisms since it is the only PIV authentication mechanism that provides at least SOME confidence in the identity of the cardholder that can be performed over the contactless interface using only card features that are mandatory under [FIPS201]."" | Please see Common policy 1.4.2 and reconcile against what it says; as well as what FIPS 201-3 and 800-116 say about SOME confidence in identity of presenter -- and update this document accordingly. |
| 9 | 3.1.1 | 11 | 582-583 | Regarding "Derived PIV authentication certificates SHALL comply with the Derived PIV Authentication Certificate profile in [PROF]." -- Currently, this section does not include proposed certificates such as PKI-CAK and all PIV objects associated with the PIV contactless and VCI interfaces allowed by SP 800-73-4. | Also, please add PKI-CAK and all PIV objects associated with the PIV contactless and VCI interfaces allowed by SP 800-73-4.<br>Please also coordinate with the FPKI Policy Authority to determine whether a new Profile is required for Derived PKI-CAK or other certificate profiles, and if so please update this text accordingly. |

| | | | | | |
|---|---|---|---|---|---|
| 10 | 3.1.1 | 11 | 584-588 | Current text is limited to Derived PIV Authentication certificate. | Update discussion to have similar language for PKI-CAK (PIV or Derived). Determine how all the expiration dates of certificates, data objects and renewal/re-issuance would work. |
| 11 | 3.1.2 | 11 & 12 | 590-605 | Section is limited to Derived PIV Authentication certificates. | Update discussion to also address PKI-CAK, SM-AUTH and other contactless PIV data objects. |
| 12 | 3.1.3 | 12 | 607-612 | This section is limited to Multi-factor crypto authenticators for Derived PIV Authentication. | Please update this section to also address single-factor PKI-CAK approach. Also address use case where PKI-CAK is the only certificate (i.e., no PIV Authentication certificate). Coordinate with NIST SP 800-116r1 list of authenticators. |
| 13 | 3.2.1 | 13 | 641-642 | Regarding "All single-factor authenticators SHALL be used in conjunction with a memorized secret that meets the requirements of [SP800-63B] Sec. 5.1.1.1." -- this text requires memorized secret. | Please update discussion to account for Single Factor, contactless free-read PKI-CAK and other single factor authenticator approaches, which would not require the memorized secret. |
| 14 | References | 15 | 690 | Add reference for SP800-116r1 | |
| 15 | References | 15 | 690 | Add reference for E-PACS 3.0 | |
| 16 | References | 15 | 690 | Add reference for SP800-166 | |
| 17 | B.1.1 | 18 | 763 | Unclear why Derived AID is necessary and whether it is mandatory. We believe we should be able to use just the PIV AID. | Please update to allow Derived credentials to be issued on tokens that support PIV AID. |
| 18 | B.1.2 | 18 | 774-778 | This section focuses solely on Derived PIV Authentication certificate. For PACS, we only want/need Derived CAK certificate. | Please update this section (and anywhere else in the document where appropriate) to allow the option of (single-factor) Derived CAK as the only mandatory certificate. If that option is not acceptable, next best option is to have (single-factor)Derived CAK certificate mandatory in addition to mandatory Derived PIV Authentication certificate. |
| 19 | B.1.2.1 | 21 | 843 | Table 1 does not include an entry for mapping Derived CAK. | Please update Table 1 to add entries for all data objects that may be used during PACS contactless authentication (e.g., Derived CAK, CHUID). |
| 20 | B1.4.1 | 22 | 865 | Table 2 does not include an entry for mapping Derived CAK. | Please update Table 2 to include an entry that maps Derived CAK |
| 21 | B.1.5 | 23 | 889 | FIPS 201-3 and 800-116 indicate SOME confidence in identity of presenter (HolderV). You can get SOME HolderV confidence without an activation secret. | Please see Common policy 1.4.2 and reconcile against what it says; as well as what FIPS 201-3 and 800-116 say about SOME confidence in identity of presenter -- and update this document accordingly. |
| 22 | B.1.5 | 23 | 898 | This second bullet addresses translation of "PIV auth certificate" to "derived PIV authentication certificate." | Please add additional bullet similar to this but for a translation of PIV CAK certificate to Derived CAK certificate. |
| 23 | B.2 | 24 | 922 | This bullet addresses PIV Authentication Key being replaced with Derived PIV Authentication Key. | Please add additional bullet similar to this but for a replacing PIV CAK with Derived CAK. |
| 24 | B.2 | 24 | 929 | Regarding "References to "card management key" are replaced with "derived PIV token management key." -- shouldn't this be 'PIV Card application administration key' ? | Please update this bullet to use 'PIV Card application administration key'. |
| 25 | B.2.1 | 24 | 935-936 | This text speaks to Derived PIV activation secret. For the proposed contactless, free-read Derived CAK approach, activation is not required. | Please update text to also address contactless, free-read Derived CAK authentication approach where activation is not required. |
| 26 | C.1 | 25 | 983 | Regarding "The provisioning application loads the derived PIV authentication certificate on the mobile device." -- this cites only Derived PIV Authentication certificate. | Please update text to included Derived CAK certificate as well. |
| 27 | C.2 | 26 | 989-990 | Title of this section is a bit misleading/confusing as section speaks specifically to non-PKI credentials | Suggest opening this section with "The following is an example of a non-PKI-based derived PIV credential." similar to how you open section C.1. |
| 28 | Appendix D | 27 | 1031 | The PKI-based derived PIV credential definition only cites Derived PIV Authentication certificate. | Please update definition to also address Derived CAK. Perhaps just use "X.509 certificate" instead. |
| 29 | | | | FIPS 201-3 states, "The PIV relying subsystem becomes relevant when the PIV Card or derived PIV credential is used to authenticate a cardholder who is seeking access to a physical or logical resource. … mechanisms for authentication are defined in … [SP 800-157] for derived PIV credentials to provide consistent and secure means for performing the authentication function preceding an access control decision." --so seems that PACS authentication using derived PKI-CAK should be defined in 800-157. | Please update document to define PACS authentication using derived PKI-CAK. |
| 30 | | | | FIPS 201-3 Section 4.1 states, "The PIV Card SHALL comply with the physical characteristics described in [ISO 7810], [ISO 10373], and [ISO 7816] for contact cards in addition to [ISO 14443] for contactless cards." -- accordingly, SP 800-157 should define the contactless characteristics for Derived PIV. | Please update document to define the contactless characteristics for Derived PIV. |
| 31 | | | | FIPS 201-3 Section 4.1.3 states, "The card body structure SHALL consist of card materials that satisfy the card characteristics in [ISO 7810] and test methods in [ANSI 322]." -- should there be a Derived PIV Mobile or Token Durability requirement? | Please determine whether there should there be a Derived PIV Mobile or Token Durability requirement, and if so update this document accordingly. |
| 32 | | | | FIPS 201-3 Section 4.2.1 states, "The CHUID SHALL also include an expiration date data element in machine-readable format that specifies when the card expires " -- for a Derived credential, should it match the expiration date of the certificates? | Please determine whether for a Derived credential CHUID expiration date should match the expiration date of the certificates, and if so update this document accordingly. |
| 33 | | | | FIPS 201-3 Section 4.2.1 states, "The FASC-N, card UUID, expiration date, and, if present, cardholder UUID SHALL NOT be modified post-issuance." -- Should this apply to Derived Credentials? If issued for 3 years, to match certificates, would the re-issuance process write a new CHUID? | Please determine whether this should apply to Derived Credentials, and if so update this document accordingly. |
| 34 | | | | FIPS 201-3 Section 4.2.1 states, "The content signing certificate SHALL NOT expire before the expiration of the card authentication certificate." -- Do we need to line up all the expiration dates for Derived PIV? | Please determine whether we need to line up all the expiration dates for Derived PIV, and if so update this document accordingly. |
| 35 | | | | FIPS 201-3 Section 4.2.2.2 states, "The asymmetric card authentication key MAY be generated on the PIV Card or imported to the card." -- this should also be allowed for Derived PIV. | Please update document to also allow this for Derived PIV. |

| | | | | | |
|---|---|---|---|---|---|
| 36 | | | | FIPS 201-3 Section 4.2.2.2 states, "The X.509 certificate SHALL include the FASC-N in the SAN extension using the pivFASC-N attribute to support physical access procedures. The X.509 certificate SHALL also include the card UUID value from the GUID data element of the CHUID in the SAN extension. The card UUID SHALL be encoded as a URN, as specified in Section 3 of [RFC 4122]." -- the requirements should be the same for Derived PKI-CAK. | Please update this document to specify the same for Derived PKI-CAK as PKI-CAK. |
| 37 | | | | FIPS 201-3 Section 4.2.3.2 states, "The content signing certificate SHALL NOT expire before the expiration of the card authentication certificate" -- need to know when the content signing certificate should expire. | Please update document to define when the content signing certificate should expire. |
| 38 | | | | FIPS 201-3 Section 4.3.1 states, "PIV Cards SHALL implement user-based cardholder activation to allow privileged operations using PIV credentials held by the card." -- A PIN is only required for privileged operations, so BIO from reader to system (CTE) should not be considered a PIV Card privileged operation. | Please update document to explicitly state that A PIN is only required for privileged operations and that BIO from reader to system should not be considered a PIV Card privileged operation. Also need to take this into account for authenticators required to move between PACS Security Areas. |
| 39 | | | | FIPS 201-3 Section 5.2.1 states, "The expiration date of the PIV authentication and card authentication certificates SHALL NOT be after the expiration date of the PIV Card." -- additional requirements about lining up expiration dates is needed. In other words, address expiration dates of all objects issued as part of a Derived credential. | Please update document to ensure all expiration dates for all objects issued as part of a Derived credential are lined up as necessary. |
| 40 | | | | FIPS 201-3 Section 6 states, "Graduated authenticator assurance levels are also applicable to derived PIV credentials used in accordance with [SP 800-157 ]." -- SP 800-157 should specify AAL for Derived PKI-CAK vis a vis PACS. | Please consider updating the document to specify AAL for Derived PKI-CAK vis a vis PACS. |
| 41 | | | | FIPS 201-3 Section 6.3 states, "Authentication mechanisms for physical and logical access using derived PIV credentials is described in [SP 800-157]. " -- need to add requirements around derived authentication mechanisms specifically for PACS. | Please update document to add requirements around derived authentication mechanisms specifically for PACS. |
| 42 | | | | FIPS 201-3 Glossary states, "Card Verifiable Certificate - A certificate stored on the PIV Card that includes a public key, the signature of a certification authority, and further information needed to verify the certificate." -- CVC for Derived credentials should be addressed in this document. | Please update document to add CVC for Derived Credentials |
| 43 | | | | FIPS 201-3 Glossary states, "Identity Assurance Level (IAL) - A category that conveys the degree of confidence that a person's claimed identity is their real identity, as defined in [SP 800-63] in terms of three levels…" -- IAL should be defined for Derived credentials vis a vis PACS. | Please consider updating the document to specify IAL for Derived credentials (e.g., Derived PKI-CAK) vis a vis PACS. |
| 44 | | | | FIPS 201-3 states, "The PIV Card SHALL store private keys and corresponding public key certificates and SHALL perform cryptographic operations using the asymmetric private keys. At a minimum, the PIV Card SHALL store the PIV authentication key, the asymmetric card authentication key, and the corresponding public key certificates." -- therefore, both PIV authentication key, the asymmetric card authentication key, and the corresponding public key certificates should be mandatory for Derived. | Please update document to make both PIV authentication key, the asymmetric card authentication key, and the corresponding public key certificates mandatory for Derived. |
| 45 | | | | NIST SP 800-116, Section 6.5 bullets: "The interoperability of temporary badges with PIV readers and authentication mechanisms (especially PKI-CAK for physical access)." AND "The assignment of unique identifiers (FASC-N or UUID) to temporary badges, to foster interoperability with PIV reader." AND "contactless-only temporary badges for physical access" -- is there a solution for temporary credentials similar to the way we issue derived cred leveraging certificate profiles for logical and physical access? | Please consider whether there is a solution for temporary credentials similar to the way we issue derived cred leveraging certificate profiles for logical and physical access, and update this document accordingly. |
| 46 | | | | Do you see PIV applets used on Derived Credentials being tested by NIST? | |