The Third Revision of FIPS 201

High Level Change Requests

1 PKI-based PIV Credentials in other Form Factors

Until recently, the smart card has been the form factor for PIV Credentials which are being used both for physical and logical access. With the advance of mobile devices, however, these PKI credentials are now present in mobile devices in the form of Derived PIV Credentials (DPC) as specified in SP 800-157. Department and agencies have a need to further expand the PIV PKI credentials to computing platform that do not easily integrate with smart cards. Apple Laptops, for example, have no integrated readers and Windows based laptops have virtual smart cards.

Considerations:

1) The new form factors may not be able to accommodate AAL-3 credentials as is the case with Derived PIV Credentials for mobile devices where two factor software based AAL-2 is the norm today.
2) The derivation process of SP 800-157 can be applied to other form factors. NIST suggests generalizing the process to accommodate other form factors. Interagency interoperability at the service level could be achieved through GSA's certificate conformance testing.

Decisions:

Questions 1-3 address logical access use-cases only. For physical access uses cases, see item 3.

1) Shall PKI-based Derived PIV Credentials be expanded to other form factors?
2) Shall there be restrictions on what platform PKI Derived PIV Credentials applies to (i.e., edge cases only)?
    a. Would restrictions be specified in the FIPS or OMB policy?
3) Shall AAL-2 in addition to AAL-3 PKI solution be considered in light of HSPD-12's goal to provide graduated levels of security?

2 Non-PKI PIV Credentials

Some departments and agencies are considering deploying non-PKI credentials. This movement towards non-PKI alternate credentials for PIV has intensified especially since the cybersecurity sprint effort of 2015 that ask department and agencies to implement alternative two factor authentication solution, when PIV smart card based 2-factor authentication is not possible. These alternatives could become part of HSPD-12 and the FIPS 201 suite of standards if aligned with the objectives of HSPD-12. It is assumed that the derivation process as specified for the Derived PIV Credentials for mobile devices will be generalized to derive and issue non-PKI PIV Credentials.

Consideration:

1) Federation profiles will be necessary to achieve governmentwide interoperability goals of HSPD-12.
2) The focus of federation models and underpinning trust framework has been on C2G use cases, but parts of these use-cases could be leveraged for a PIV Federation.
3) Federation models today exist in decentralized fully-meshed or centralized hub-and-spoke architecture with fully-meshed being the predominant model. Benefits and considerations for both models should be considered for large departments/agencies as well as for micro federal enterprises.

Decisions:

1) Federations:
    a. Should the PIV standard be complemented with specific federation models (SAML, OpenID Connect) and include assertion token profiles?
    b. What type of federation models should be chosen (hub-and-spokes, fully-meshed, or a combination of both)? Who would be the broker in the hub-and-spokes architecture?
2) Authenticators:
    a. Shall two factor AAL-2 in addition to two factor AAL-3 solutions be considered in light of HSPD-12's goal to provide graduated levels of security?
    b. In the federation, shall the PIV authenticator profile be generic to allow any type of AAL-2 or AAL-3 token as long as it conforms to SP 800-63 B or are specific token profile required?
    c. Is there a need for interagency-interoperable revocations for non-PKI PIV credentials?

3 Facility Access

Federal Government facility access described in FIPS 201 is further detailed SP 800-*116 Revision 1, Guidelines for the Use of PIV Credentials in Facility Access.* This publication specifies up to three authentication factors for access to secure facilities and inner areas using the PIV Card. Adoption of the PIV Card for facility access has been slow partially because of legacy PACS infrastructure and partially because of the slow technology refresh cycles attributed to PACS. For example: The transition away from weak CHUID authentication to strong PKI-CAK authentication was expected by now. However, only a few departments and agencies are implementing PKI-CAK.

Considerations:

1) Federal facility access with mobile devices:
    a. Mobile devices with NFC chip operate over the same transport protocol as facility access readers; namely the ISO/IEC 14443 transport protocol. This will substantially reduce integration task and cost of adopting federal building access with mobile devices.
    b. NFC has several modes of operation one of which is the "Card Emulator." – This is the mode used by mobile devices to emulate the PIV Card application to the PACS reader. Support of card emulation varies however, as the Android mobile platform supports it, but iOS does not.

c. Single Factor CAK authentication can be implemented without the need of secure messaging (SM) channel. Two or three factor authentication, will require a secure channel. SM capability in commercial PACS offerings are minimal; thus, vendor support as well as PACS infrastructure upgrade for SM needs to be fostered.

Decisions:

1) Should FIPS 201 be amended to allow facility access with mobile devices using NFC or other communications protocols?
2) Some Departments and Agencies store the PIV biometric credentials on PACS servers. Cardholder authentication is done by matching cardholders' life scan biometrics against the server's stored biometric. The PIV Card is only minimally involved to provides the identifier lookup to the cardholder's biometric on server. Traditionally, server-based authentication has been outside of scope for PIV. Should server-based authentication be considered a PIV Authentication mechanism in FIPS 201?

4 Remote Identity Proofing

The new SP 800-63 *Digital Identity Guidelines* adds the possibility to supervised remote identity proofing for IAL-3. The process of supervised remote identity proofing is not necessarily a low-cost option for departments and agencies. It is comparable to a kiosk scenario or an USAccess/MSO setup at a client's site where dedicated hardware/software are deployed to include biometric reader to collect and verify biometrics, camera to supervise identity proofing. Additionally, the transaction is staffed at the CSP side by an operator who interact with the applicant and observe the entire identity proofing process. This setup is required to be secured with SP 800-53 high baseline security controls as per SP 800-63. Supervised remote identity proofing should not be confused with unsupervised remote IAL-2 identity proofing that can be done inexpensively on the subject's laptop/device.

Considerations:

Related: The derivation process specified in SP 800-157 does not repeat identity proofing as it has already been done to receive a PIV Card. Instead, identity proofing is inherited by the cardholder showing proof of possession and control of the PIV Card. This process, however, is required to be performed in-person for derived credentials issued at IAL-3. Should remote proof of possession and control be allowed and modeled according to a supervised remote issuance?

Decisions:

1) Should FIPS 201 be amended to allow supervised remote identity proofing?
2) Related: Should derivation, (i.e., the proof of possession and control of the PIV Card to issue a Derived PIV Credential), be allowed to be performed in supervised remote fashion (see considerations)?
3) Should chain-of-trust provide for a Derived PIV Credential Issuance, this infers the same due-diligence as original PIV Card Issuance for the Derived PIV Credential issuance.

5 Quantum Computing Resistant Algorithms

NIST recognizes that large-scale quantum computers, when available, will threaten the security of NIST-approved public key algorithms. NIST is undergoing a process to identify quantum-resistant cryptographic algorithms for standardization. This process is a multi-year effort, with draft standards anticipated in 2022. In the meantime, NIST encourages implementers to plan for cryptographic agility to facilitate transitions to quantum-resistant algorithms where needed in the future.

Considerations:

1) PIV relies on public key cryptography for multiple purposes: authentication for logical access, digital signatures, support for encryption technologies, and card authentication for physical access.
2) Standards for quantum-resistant public key algorithms are years away, with many potential candidates possessing different performance characteristics from current algorithms (e.g., larger public keys, signatures or ciphertexts, greater computational complexity, etc.).
3) Standards and specifications supporting PIV may need to be updated- perhaps significantly- based on the results of the algorithm standardization process. These changes will likely lead to significant updates to PIV readers and other supporting systems.
4) Most applications of PIV do not require forward security, meaning that it will only be necessary to complete a transition before quantum computers are a threat.

Decisions:

1) What long-term planning activities can be taken to align the refresh cycle of PIV systems with the anticipated need to adopt quantum-resistant cryptography?
2) Are there near or moderate term steps that could be considered to mitigate the impact of early development of quantum computers, either as part of this revision cycle or the next?