KAISER PERMANENTE®

Kaiser Foundation Health Plan
Program Offices

April 21, 2023

RE: *Draft Guidelines on Personal Identity Verification (PIV) Credentials and Federation (SP 800-157 Rev1 and SP 800-217)*

Submitted via email to: piv_comments@nist.gov.

Kaiser Permanente (KP) appreciates the opportunity to offer comments on the above-captioned request for comment.[1] The Kaiser Permanente Medical Care Program is the largest private integrated health care delivery system in the U.S., delivering health care to over 12 million members in eight states and the District of Columbia[2] and is committed to providing the highest quality health care.

The rapid proliferation of online services over the past few years, particularly in response to social and economic changes brought about by the pandemic, has increased the need for reliable, equitable, secure, and privacy-protective digital identity solutions. As a health care organization, Kaiser Permanente has a responsibility to protect our data and systems, as well as the data of our members and patients, from security threats and breaches. We appreciate efforts by NIST to update guidelines for personal identity verification (PIV) credentials and federation, and offer the following in response to questions posed:

SP 800-157 Rev1, Guidelines for Derived Personal Identity Verification Credentials

1. *Are the new controls for issuance, use, maintenance, and termination of non-PKI-based derived PIV credentials clear and practical to implement?*

We generally find the new controls to be clear and practical to implement and offer the following recommendations and requests for clarification:

- Consider World Wide Web Consortium Decentralized Identifiers/Verifiable Credentials (W3C DID/VC) to introduce a layer of abstraction that separates key materials from claims and account for key rotation procedures that require re-issuance of credentials.
- Provide additional guidance to entities in the event a key is lost, including revocation mechanisms (e.g. centralized/distributed cloud server versus identity provider proof (IDP)/CSP).
- Clarify whether the PIV Identity Account DB is on the card or part of the maintenance environment.
- Clarify whether a public key infrastructure (PKI)-based derived PIV could be issued by a FIDO2 device using its platform authenticator in the FIDO2 registration step with the issuer.
- Clarify whether lines 425-432 refer to both PKI Auth and non-PKI derived PIV or whether they are intended to just require use of PKI-Auth.

[1] https://csrc.nist.gov/publications/detail/sp/800-157/rev-1/draft , https://csrc.nist.gov/publications/detail/sp/800-217/draft

[2] Kaiser Permanente comprises Kaiser Foundation Health Plan, Inc. and its health plan subsidiaries outside California and Hawaii; the not-for-profit Kaiser Foundation Hospitals, which operates 39 hospitals and over 720 other clinical facilities; and the Permanente Medical Groups, self-governed physician group practices that exclusively contract with Kaiser Foundation Health Plan and its health plan subsidiaries to meet the health needs of Kaiser Permanente's members.

2. *Are phishing-resistant authenticators available to meet agency use cases as well as the requirements for derived PIV authentication?*

Generally speaking, authenticators embedded into end-points (e.g. platform authenticators such as FIDO2 and ISO 18013) are phishing resistant and meet agency use cases. Other derived PIV authenticators such as USB authenticators and authenticators that are connected to wireless end-points, are likely to meet agency uses cases but may not be phishing resistant.

3. *Are the new controls sufficient to provide comparable assurance to PIV Cards and other derived PIV credentials?*

While we find that the new controls are sufficient to provide assurance to PIV Cards and other derived PIV credentials, it is also important to have assurance of Identity proof (IA L2 or IAL3) before issuance of PIV card. When a PIV card holder authenticates remotely, the possession of derived PIV credential alone is not sufficient to link to assured identity. We recommend that the controls clarify that remote authentication must perform platform biometric (AAL 3) to provide sufficient assurance. We also recommend that NIST consider including a numeric limit on the number of permitted derived-PIV as a security measure.

4. *Other Comments and Feedback?*

The proposed model for non-PKI-based credentials is based on Federated Identity. We are concerned that this model creates privacy and dependency risks in the private sector, and we recommend that NIST specify acceptable implementation conditions outside of the government sector. We also recommend that the definition of Authenticator be amended to clarify the role of the PIN associated to the integrated circuit card (ICC) because the PIV or derived PIV without the PIN is insufficient.

SP 800-217, Guidelines for Personal Identity Verification Federation

Home Agency Attributes

1. *Are additional attributes needed in the guidelines to achieve interagency or cross¬ domain interoperability?*

We recommend the guidelines include unique subject identifier information to establish cross-domain interoperability for home IdP discoverable and configurable by RPs. Email attribute is not universally defined and some home IdP use their own defined userIDs which may not be compatible with RPs. We also recommend that the guidelines list assertion presentation for home IdP (front-channel vs. back-channel). NIST may also consider including optional attributes to indicate the type of domain (e.g. healthcare, financial, government etc.) to support security profile usage and refinement.

2. *Are additional attributes required for RP provisioning and access?*

We do not recommend including additional attributes for RP provisioning and access. The RP should have minimum attributes to define access control including subject unique identifier, email, and name attributes. We recommend that the just-in-time provisioning model/SCIM APIs track the updated account timestamp without provisioning this attribute to the RP.

3. *Other Comments and Feedback*

We are concerned that the Federated Identity model creates privacy and dependency risks in the private sector, and we recommend that NIST specify acceptable implementation conditions outside of the government sector.

PIV Federation

1. *Are additional process steps or mechanisms needed for the connection and communication between home IdP to PIV identity account?*

We do not find that additional process steps are needed for the connection and communication between home IdP to PIV identify account. Home IdP is an issuer of the PIV Identity account, so no additional process steps are needed to bind the PIV card or credential other than the minimum IA L2 or IAL3 requirement to bind the accounts with the credentials.

2. *Do the required parameters for establishing trust agreements fit the use cases for PIV RPs?*

No comments

3. *Are the required identity attributes sufficient for PIV use cases?*

No comments

4. *Are the federated subject identifier requirements sufficient for PIV use cases?*

No comments

5. *Is it clear how to apply the binding ceremony for RP-managed bound authenticators at FAL3 to PIV and non-PIV authenticators?*

We do not find the guidance sufficient for binding RP-managed bound authenticators at FAL3 to PIV and non-PIV authenticators. Non-PKI based PIV credentials should be generally bound to home IdP; however, the guidelines defined in FAL3 for phishing resistance requirement for non-PKI-based PIV credentials with RP-managed bound authenticators cross-reference platform biometric (e.g. bio keys) that cannot be phishing resistant. We recommend NIST clarify the guidance for binding RP-managed bound authenticators at FAL3 to non-PKI-based PIV credentials to assure phishing resistance.

6. *Other comments and Feedback*

We are concerned that the Federated Identity model creates privacy and dependency risks in the private sector, and we recommend that NIST specify acceptable implementation conditions outside of the government sector.

***

Thank you for considering our feedback. If you have questions or concerns, please contact me at
.

Sincerely,

Vice President, Health IT Strategy and Policy
Kaiser Foundation Health Plan, Inc.