KAISER PERMANENTE®

Kaiser Foundation Health Plan
Program Offices

April 14, 2023

RE: *Draft revisions to NIST Digital Identity Guidelines (SP 800-63-4)*

Submitted via email to: dig-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 applaud efforts by NIST to update the suite of Digital Identity Guidelines in response to changes in the digital landscape over the past 5 years, and offer the following in response to questions posed:

IDENTITY PROOFING AND ENROLLMENT

1. *NIST sees a need for inclusion of an unattended, fully remote Identity Assurance Level (IAL) 2 identity proofing workflow that provides security and convenience, but does not require face recognition. Accordingly, NIST seeks input on the following questions:*
    a. *What technologies or methods can be applied to develop a remote, unattended IAL2 identity proofing process that demonstrably mitigates the same risks as the current IAL2 process?*

We agree that there is a need for an unattended, fully remote IAL identity proofing workflow. Image Hashing (discrete cosine transform, wavelet transform) is probably best suited meet this need, however, it still depends on a photo presentation and liveness test. We also note that a Stanford University Research team[3] is investigating approaches to authenticate image provenance to recognize differently rendered photos using zero-knowledge proof technology based on cameras with built-in cryptographic signature technology. This could present a pathway to make in-person identity

[1] https://csrc.nist.gov/publications/detail/sp/800-63/4/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.

[3] https://crypto.stanford.edu/

assurance widely available as it can be brought to trusted, physical interaction points such as a postal office, pharmacy, bank, medical office visit etc.

We recommend that NIST fully embrace the World Wide Web Consortium (W3C) decentralized identity (DID)/ verifiable credentials (VC) data models and Linux Foundation Trust over IP protocols in the NIST Digital Identity Model to guide industry to the re-use of Identity Assurance outcomes. This would allow public/private sector collaboration in specific digital trust context much that like demonstrated in the industry approach for the U.S. Drug Supply Chain Security Act[4].

b. *Are these technologies supported by existing or emerging technical standards?*

Yes. Image hashing is being explored by the European Commission[5] (EC).

c. *Do these technologies have established metrics and testing methodologies to allow for assessment of performance and understanding of impacts across user populations (e.g., bias in artificial intelligence)?*

Yes. We recommend reviewing resources made available by the Swiss Center for Biometrics Research and Testing[6].

2. *What methods exist for integrating digital evidence (e.g., Mobile Driver's Licenses, Verifiable Credentials) into identity proofing at various identity assurance levels?*

We recommend that identity proofing output be standardized, ideally as a VC, using evidence elements, with every identity proofing credential service provider (CSP) required to participate in a Trust Registry that indicates conformance to a set of rules associated with IAL they create outputs for.

3. *What are the impacts, benefits, and risks of specifying a set of requirements for CSPs to establish and maintain fraud detection, response, and notification capabilities?*
    a. *Are there existing fraud checks (e.g., date of death) or fraud prevention techniques (e.g., device fingerprinting) that should be incorporated as baseline normative requirements? If so, at what assurance levels could these be applied?*

We recommend additional research to determine and clearly delineate between additive fraud checks (as described above) and verification rule requirements and establish how these checks can be done in a privacy-preserving way. We are concerned that it may be overly burdensome for organizations to apply additive fraud checks and audit requirements to IALs generally. Instead, we recommend NIST consider utilizing the concept of Trust Ecosystems to prescribe fraud prevention techniques in a defined manner as part of its governance within a bounded ecosystem.

[4] See https://www.oc-i.org.
[5] https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf
[6] https://www.biometrics-center.ch

b. *How might emerging methods such as fraud analytics and risk scoring be further researched, standardized, measured, and integrated into the guidance in the future?*

We recommend that emerging methods be investigated in collaboration with Trust Ecosystems and auditors, such as Kantara.[7]

c. *What accompanying privacy and equity considerations should be addressed alongside these methods?*

Transfers of personally identifiable information (PII) outside of the CSP require an explicit consent or authorization from the individual. To maintain privacy controls, self-sovereign identity (SSI) (DID/VC) offers the ability to track a cryptographically verifiable consent by the individual, which could be utilized as a condition for 3rd party background checks.

4. *Are current testing programs for liveness detection and presentation attack detection sufficient for evaluating the performance of implementations and technologies?*

In our assessment, there is not yet sufficient conclusive evidence of soundness and completeness to evaluate the performance of implementations and technologies. Additionally, we are concerned that a lack of transparency regarding hardware and algorithms used by a CSP can create a "black box" that leaves the relying party (RP) with no way to assess exposure.

5. *What impacts would the proposed biometric performance requirements for identity proofing have on real-world implementations of biometric technologies?*

We are very concerned that the proposed biometric performance requirements may be overly burdensome for organizations to implement and audit. As mentioned above in our response to question (3)(a), it may be more attainable to redefine the identity model and guidance such that it drives for secure re-use of in-person identity assurance that has been augmented with certified biometric tools by a certified professional.

RISK MANAGEMENT

6. *What additional guidance or direction can be provided to integrate digital identity risk with enterprise risk management?*

As digitalization pushes the consumer expectations from accounts with individual services to broader transferability, the operational and liability complexity of the Federated model at scale may be an impediment and require a fresh look to consider a more decentralized model that fosters actors' autonomy and reduces the risk exposures. We recommend NIST consider providing additional guidance on the Federated model regarding structure for contractual agreements between RP, IDP and auditors that is typically defined in Trust Frameworks.

[7] See What We Do - Kantara Initiative: Trust through ID Assurance

Additionally, proposals where a federal department or agency (such as HHS) expands its ID-broker service to the public sector would greatly benefit from specific risk guidance, particularly regarding privacy and availability, that impacts private sector to consumer transactions.

7. *How might equity, privacy, and usability impacts be integrated into the assurance level selection process and digital identity risk management model?*

The selected Assurance Level (whether for Identity – IAL, Authentication – AAL, or Federation – FAL) must meet or exceed minimum regulatory or contractual obligations. Digital identity risk management must balance the efforts (cost, time, resources) to maintain the digital identity program against the benefits of such program.

Impacts on equity, privacy, and usability must be considered as elements of the business requirements for the proposed solution so that these factors are "baked into" the system as it is designed, developed, tested, implemented, and operated.

8. *How might risk analytics and fraud mitigation techniques be integrated into the selection of different identity assurance levels? How can we qualify or quantify their ability to mitigate overall identity risk?*

Risk analytics provide possible scenarios and risk factors where fraud or negative/unintended results may occur in the use of digital identity. Risk level is a product of the "likelihood" of an event occurring and the "potential impact" of that event should it occur. Fraud mitigation techniques can be integrated into the IAL selection process based on the various risk levels of the identified risk factors and how they can be controlled or offset, accounting for the organization's risk appetite or risk threshold.

The risk factors and their risk levels can be quantified through data modeling and analysis into specific expected costs to the organization (again, based on its risk thresholds) to quantify their ability to mitigate overall identity risks.

AUTHENTICATION AND LIFECYCLE MANAGEMENT

9. *Are emerging authentication models and techniques – such as FIDO passkey, Verifiable Credentials, and mobile driver's licenses – sufficiently addressed and accommodated, as appropriate, by the guidelines? What are the potential associated security, privacy, and usability benefits and risks?*

Emerging authentication models and techniques are not sufficiently addressed or accommodated by the guidelines. Risks associated with the 3rd digital identity model stem from lack of maturity and complexity for user agents. The benefits associated with this model include more consumer control and privacy (including metadata about interactions) and less complexity in protocol flows and

interconnections. Additionally, the new model allows for new use cases, such as transferability of a digital trust that can dictate terms and conditions.

10. *Are the controls for phishing resistance as defined in the guidelines for AAL2 and AAL3 authentication clear and sufficient?*

We recommend that the definition of phishing resistance in section 5.2.5 be expanded to address scenarios of multiple devices usage, understanding the extent to which associated mechanisms are impacted. For example, Channel Binding may not work well across multiple devices. We also recommend that NIST clarify whether OS-level (platform) authenticators as in FIDO2 satisfy AAL3.

11. *How are session management thresholds and reauthentication requirements implemented by agencies and organizations? Should NIST provide thresholds or leave session lengths to agencies based on applications, users, and mission needs?*

We recommend that NIST provide thresholds and include refresh tokens as this is useful guidance for organizations.

12. *What impacts would the proposed biometric performance requirements for this volume have on real-world implementations of biometric technologies?*

No comment.

FEDERATION AND ASSERTIONS

13. *What additional privacy considerations (e.g., revocation of consent, limitations of use) may be required to account for the use of identity and provisioning APIs that had not previously been discussed in the guidelines?*

Privacy and RP-dependency on the IDP are the main concerns with the Federated Identity model because the IDP will maintain all authentications undertaken by a user and RP will be unable to function without the IDP. We find that the Decentralized Identity model addresses both these concerns.

14. *Is the updated text and introduction of "bound authenticators" sufficiently clear to allow for practical implementations of federation assurance level (FAL) 3 transactions? What complications or challenges are anticipated based on the updated guidance?*

The updated text and introduction of "bound authenticators" are not sufficient to allow for practical implementations of FAL 3 transactions. We recommend NIST define the process and type of authenticator the subscriber presents to the RP in section 6.1.2.

Additionally, it is unclear whether the updated text assumes cryptographic authenticator as in FIDO2. If a cryptographic authenticator is assumed, we recommend that the RP use this to authenticate the subscriber rather than relying on the IDP to eliminate additional, unnecessary complexity. We also recommend providing a reference if this is already defined in common protocols like OAuth or OIDC.

GENERAL STATE OF GUIDELINES

15. Is there an element of this guidance that you think is missing or could be expanded?

As mentioned earlier in our responses, we recommend including a 3rd model for Decentralized Identity in revision 4. We also recommend including another RP to address the emerging pattern of consumer apps request data from a data holder who uses IDP.

16. Is any language in the guidance confusing or hard to understand? Should we add definitions or additional context to any language?

We recommend ensuring alignment between terminology for CSP and IDP across the Volume A, B and C documents.

17. Does the guidance sufficiently address privacy?

The guidance does not sufficiently address privacy concerns implicated by the interaction of metadata in the Federation model where the IDP maintains knowledge about every authentication. This is problematic for healthcare entities required to adhere to specific, strict privacy and security guidelines. We recommend NIST take a "privacy by design" in conjunction with a "security by design" approach and offer improved guidance across all documents and actors to assist implementers. For example, the storing of evidence material such as biometric scans after ID proofing has occurred is of particular concern because it leads to storing private data for a longer periods of time than needed to perform the function.

18. Does the guidance sufficiently address equity?

a. What equity assessment methods, impact evaluation models, or metrics could we reference to better support organizations in preventing or detecting disparate impacts that could arise as a result of identity verification technologies or processes?

We are concerned that the guidance inaccurately assumes that all people who are entitled to digital services possess a driver license or passport (see A 4.1.1) and potentially impedes handling of scenarios where it is required to verify control over an authenticator in combination with an entitlement credential, such as a valid Medicaid card.

19. *What specific implementation guidance, reference architectures, metrics, or other supporting resources may enable more rapid adoption and implementation of this and future iterations of the Digital Identity Guidelines?*

This draft enhances fraud prevention measures by updating risk and threat models to account for new attacks, providing new options for phishing resistant authentication, and introducing requirements to prevent automated attacks against enrollment processes. It also opens the door to new technology such as mobile driver's licenses and verifiable credentials. We recommend NIST consider including relevant open-source protocol libraries to support software development for ID proofing, authentication, and federation.

20. *What applied research and measurement efforts would provide the greatest impact on the identity market and advancement of these guidelines?*

The following applied research and measurement efforts would promote the identity market and advancement of these guidelines:

- Binding of the Identities for RP-bound authenticators using minimum IAL2/IAL3.
- The guidelines around platform biometric authenticators versus cross platform biometric authenticators to meet phishing resistant use case.
- Linking of digital wallet Identities as non-KPI based authenticators that meets IAL2/ IAL3 ID proofing criteria, as an issuer in decentralized Identity / SSI space.
- Similar efforts or collaboration as put forward by the EU and ISO/IEC for Digital Identity Wallets.
- Province of British Columbia funding Open-Source Software projects in the area of Self-Sovereign Identity, e.g., Verified Organization Network (VON).
- Zero-knowledge cryptography to improve privacy and image provenance.
- The creation of a 3rd Identity Model for "Decentralized Identity" as it would significantly simplify Digital Identity and Trust ecosystems with enhanced protection against identity theft, and an economic competitiveness perspective.

OTHER THOUGHTS

We offer the following additional recommendations:

Add "Decentralized Identity" as a 3rd model

In accordance with W3C DID/VC data models and Linux Foundation Trust-over-IP (TOIP), the model is adjusted showing the RP as a Resource Server (RS) with a Verifier function. Each actor (subject, RP, CSP) controls one or more Decentralized Identifiers (DID) which enables symmetrical mutual authentication. This model conceals the knowledge about with whom a subject authenticates while still allowing for trusted and governed 3rd parties in the role of CSP/ID proofers. It removes the role of an IDP as an authentication function and allows for authoritative first-source actors to directly issue Verifiable Credentials (VC) to subjects attesting specific identity attributes (claims). As digital service

consumers, subjects then present these VCs to register their DID with the RP which inherently registers a cryptographic authenticator.

Decentralized Identity as a 3rd model could take on several governance functions already specified by TOIP. Subjects themselves can also issue self-signed Verifiable Credentials which could be used as directives or data-sharing and usage authorizations. This would significantly simplify proposed approaches to sector-wide challenges for Open Banking and Health Information Exchange by providing the subject with the ability to grant one RP (e.g., a health app) access to data in a resource server of another RP (e.g., the hospital). The subject simply issues an authorization-VC to the health app which presents it in the data request to the hospital. This highly composable pattern can also apply to education diplomas and in credentialling of professionals. Similarly, health plans could issue standardized digital insurance cards as VCs which would simplify real-time eligibility verification for providers, particularly when there is no prior business relationship between provider and payer (e.g., urgent care, emergency).

Add a new volume D to the SP 800-63 series for Decentralization and Verifiable Credentials with DAL1-3 covering assurance levels for "digital trust"

The definition for these levels should be vetted in a broader outreach to W3C Credential Community Group, Linux Foundation TOIP, Open Identity Foundation, and Decentralized Identity Foundation. We recommend the following suggested Decentralization Assurance criteria be used in a similar combinational form as provided by FAL: criteria for cryptographic qualities assuring privacy, confidentiality, and non-repudiation; criteria for qualities associated with the trust ecosystem's governance model assuring transparency and operational excellence; criteria for decentralization qualities assuring sustained funding sources, fair power distribution and participatory rights of all stakeholders.

Align with standards evolution for OAuth2.1 and OIDC

We are concerned that OAuth 2.1 and OIDC appear to be misaligned, for example, in document 800-63C, line 486, OAuth2.1 appears to depreciate "Implicit Flow" in the "Implicit Client profile" while the reference provided may divert. We recommend clarifying this and ensuring alignment throughout the document.

***

Thank you for considering our feedback. If you have questions or concerns, please contact me at jamie.ferguson@kp.org or megan.a.lane@kp.org.

Sincerely,

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