NIST January 12, 2023 Workshop on draft SP 800-63-4 Additional Questions and Responses.

This set of questions and responses addresses questions that were raised in the chat during the NIST January 12 workshop that did not have a specific response during the workshop. Any comments or additional questions can be sent to dig-comments@nist.gov.

SP 800-63-4 (base volume)

1. Since 800-63 currently excepts physical access from the publication, risk assessment for granting assess to a fed building does not get addressed. Recommend this get readdressed - physical access is fundamentally the same as logical and should be covered as part of this effort. Conversations with the Interagency Security Committee should be had to put this on the plate

The scope of SP 800-63 is digital identity management. The SP 800-63 process and technology requirements for digital authentication over networks may be used for physical access control processes, as determined appropriate.

2. IoT, AI systems and virtual personas are evolving and new implementations coming out every day Will 63-A ever have a poV on Identity proofing and assurance for such systems and recommendations on handling such unique use cases?

The scope of SP 800-63 is digital identity management of persons over networks. Please see NIST preliminary guidance for IOT and device security NIST SP 1800-36A *Trusted Internet of Things (IoT) Device Network-Layer Onboarding and Lifecycle Management* at: https://www.nccoe.nist.gov/sites/default/files/2022-12/iot-onboarding-nist-sp1800-36a-preliminary-draft.pdf.

3. In SP 800-63-4 (Base doc), Section 4.1 states: "In all cases, the RP should request the attributes it requires from a CSP or IdP before authenticating the claimant." (line 689) This is confusing, what is the intent of this statement?

Note that section 4.1 is informative and presents summary information on the digital identity model and the processes and technologies described in the following volumes. The cited text presents the normative requirement from SP 800-63C-4 regarding federation trust agreements and federation transactions between the CSP/FDP and the RP. See SP 800-63C-4 section 5 for the detailed requirements for federated authentication and assertions and RP/IDP trust agreements and responsibilities.

To clarify the cited text, the RP should make an up-front request for access to the attributes it needs for the RP's functioning before processing the direct or federated authentication. In other words, the RP should not authenticate the claimant, then return to the claimant to submit additional information in order to gain access. This would lead to a confusing and potentially negative experience for the claimant where they are possibly prompted multiple times for the same transaction.

SP 800-63A-4

4. Is there reference to the accuracy rate of the biometrics and the ability of applications, for example, to deal with PAD and how does it affect the IAL or the AAL and are there any guidelines on the subject

Performance metrics for biometric comparison for identity verification in SP 800-63A-4 are specified at false match rate: 1:10,000 or better, false non-match rate: 1:100 or better. Performance metrics for biometric comparison for authentication in SP 800-63B-4 is specified at false match rate: 1:10,000 or better,

5. What I don't see in the CSP processes is consideration of a method for subjects to block access to identity verification in a manner similar to a subject could block credit verification.

Access control processes and decisions are outside the scope of SP 800-63-4.

6. Is Biometrics a requirement for IAL2 and above? Or is it only a recommendation?

Biometrics comparison for remote identity proofing is a requirement for remote identity proofing at !AL2 and for identity proofing at IAL3. Alternative identity verification processes are also presented for IAL2 and IAL3. Biometrics collection and retention is a requirement for IAL3.

7. A few questions re Identity Attributes. 1: Can you give an example of Identity Attribute? 2: Will the Identity Attributes be added to the PIV card data model and written to the card during Personalization/?

1. Address, phone number, date of birth, place of birth are common examples of identity attributes.

2. See FIPS 201-3 *Personal Identity Verification of Federal Employees and Contractors* for identity attributes required for the PIV program.

8. Is there separate general biometrics collection statutory or regulatory authority specifically tied to the collection of biometrics solely for enrollment or initial access to systems as part of the identity-proofing process as opposed to the general statutory authorities the agencies rely on for their specific mission, in terms of provision of service, executing transaction, or benefit being offered by the agency?

There is no specific statutory or regulatory authority for the collection and use of biometric information for the identity proofing and enrollment or authentication processes and requirements beyond the authority for NIST to provide guidance for the implementation of the Federal Information Security Modernization Act (FISMA).

9. Have practices been added which address information collection limitation/minimization for information flows from the CSP to the RP? If I recall correctly, 800-63 addresses the CSP itself but not necessarily the flows from CSP to RP. I have the Australian Optus breach in mind - where Optus kept images of identity evidence documents, and those were stolen.

Please see the draft SP 800-63C-4 for specific guidance on the privacy controls for PII/attribute information disclosure, transport, and protections from the CSP/IDP to the RP for federated authentication processes.

10. Raising the barrier on IAL1 makes sense, but I am concerned that this would lead to further decrease in adoption and may lead to more people being denied basic identity. What are your thoughts on the same?

IAL1 is one of the changes in the draft SP 800-63 that are intended to increase the capabilities and options for agencies and individuals to meet identity proofing processing and technical requirements to enable broad participation in the digital ecosystem.

11. Will you consider liveness detection of identity evidence to ensure the applicant is in possession of the document?

Please see draft SP 800-63A-4 section 5.1.8 which states in part: “When collecting and comparing biometrics remotely, the CSP SHALL implement liveness detection capabilities to confirm the genuine presence of a live human.” This requirement applies to the applicant involved in the identity proofing process. The draft does not specify requirements for the liveness detection of identity evidence, but comments on this are welcomed.

12. If we have to look at an external trusted source to validate all core attributes, how is that different from the verification requirement in IAL2 to verify by looking at external sources. Academically, I understand these are different steps; but practically I don't understand how IAL1 is different from IAL2 in this regard.

Validation of core identity attributes presented for identity proofing at all three IALs require validation through an authoritative or credible source.

13. It appears the evidence required at IAL1 and IAL2 are the same - since this is a lower assurance IAL, why not allow just one piece of STRONG?

SP 800-63A-4 rev. 4 recognizes that there is additive assurance for the collection of 2 pieces of identity evidence (STRONG + FAIR) if one piece of SUPERIOR evidence is not presented. However, SP 800-63A-4 also recognizes that multiple pieces of FAIR evidence at either IAL1 or IAL2 do not significantly raise the level of assurance. Therefore, both IAL 1 and IA:2 require a single piece of FAIR evidence with a single piece of STRONG evidence. NIST requests comments on this requirement.

14. How are you thinking about equity attributes with respect to how they are collected at enrollment, and how are for what purposes are they used or shared?

SP 800-63A-4 does not specify the collection of equity attributes. However, see SP 800-63A-4 section 5.1.8.11 which states:
CSPs SHALL assess the performance and demographic impacts of employed biometric technologies in conditions substantially similar to the operational environment and user base of the system. When such assessments include real world users, participation by users SHALL be voluntary.

Any collection of equity attributes by the CSP would be voluntary for users and subject to the privacy risk assessment requirements of section 5.1.2.

15. How do Subscriber accounts work in cases where regular renewal of subscription is needed?

Maintenance of the subscriber account is required for the duration of the subscribers’ eligibility for active participation in the CSP identity service. It is not intended, but also not precluded, that the CSP may establish renewal requirements to maintain subscriber eligibility for the Identity Service. Any renewal requirements for the subscriber account, information maintained in the account, or authenticators registered to the account are not specified in SP 800-63A-4 and, if imposed, should be clearly conveyed to subscribers.

16. It was mentioned that data privacy risk aspects have been added. I wonder if the collection of biometrics during the ID proofing is therefore becoming optional (depending on the DP risk assessment)

on IAL 3 level? On IAL 2 this collection is optional but on IAL 3 I hear complaints/get blockers(end-up in NIST compliance deficiencies due to that mandatory biometric collection requirement on IAL 3 level

SP 800-63A-4 continues the requirement from the current guidelines that the collection and retention of biometric characteristic information is required for IAL3. NIST requests comments on the effectiveness and use of this requirement.

17. Why do you see a need for an IAL2 process that does not require face recognition?

NIST seeks alternative methods for facial recognition capabilities for identity verification in order to allow a broad range of capabilities and alternatives for identity verification and to account for potential equity bias or applicant reluctance or inability to provide biometric characteristic collection for identity proofing.

18. How can reviewers comment on ways to 'demonstrably mitigate the SAME risks' if the currently considered risks and mitigations are not made available. On what risk assessment has NIST based its normative requirements and when will that assessment be made available?

See SP 800-63A-4 section 7 Threats and Security Considerations. This section presents the threats, attacks, and vulnerabilities to the processes and technologies for identity proofing and presents mitigation strategies and associated controls to address such risks that are presented as normative requirements in SP 800-63A-4.

19. NIST SP 800-63A-4 removed the requirement for IAL1, 2 and 3 to be tied to the low moderate and high SP 800-53 baselines respectively. What was the rationale for this removal?

SP 800-63-4 sec. 2.3.1 presents the overall information system security requirements for agencies under the Federal Information Security Modernization Act (FISMA) and assumes that the information categorization and information system baseline controls have been determined for the online information systems and applications protected by the digital identity guidelines. The baseline controls determined for the organization's online information system and applications should be applied to the controls for the digital identity management protections for those resources. As described, the digital identity management risk management processes in SP 80--63-4 are used for the determination of assurance levels for the associated digital identity functions and supplement but do not replace or alter the controls determined under FISMA.

20. Could you provide a definition of "direct linkage" that @DavidT used in your definition of Authoritative Source during proofing? It seems slightly different than lines 645. If not, what are the accuracy, freshness, provenance requirements that establish a direct linkage?

SP 800-63A-4 states that one of the characteristics of an authoritative validation source is that the entity "*Has access to evidence and attribute information that can be traced to the issuing source of a piece of identity evidence*." This means that the entity can trace the linkage of evidence/attribute information to the issuing source.

SP 800-63B-4

21. It would be useful to have an authoritative list of commonly used or breached passwords.

There are multiple sites that provide breached password lists, such as: https://haveibeenpwned.com/Passwords. These lists may be used to check selected passwords as well other smaller lists presenting the most common breached passwords.

22. Many authenticators should expire so that the cryptographic material can by cycled. What resources can CSPs use to help determine expiry best practices or guidelines for each type of 63B-defined authenticator?

See NIST SP 800-57 *Recommendation for Key Management Part 1, R5*, issued May 2020: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf. Section 5.3.6 Cryptoperiod Recommendations for Specific Key Types provides narrative guidance for cryptoperiods for various types of keys and summarizes the guidance for cryptoperiods in Table 1. Appropriate key lifetimes/usage periods will depend heavily on the specific use case and architecture. SP 800-57 provides a description of some of the considerations that may drive a decision to select cryptographic key usage periods either much shorter or much longer than the examples listed in the summary table. In some cases, the usage period may be limited only by the continued acceptability of the cryptographic algorithm and key length.

23. There is a distinction between single-device vs multi-device passkeys. Are you asking for both use cases?

NIST is interested in use cases for both single and multi-device passkeys and request comments on this, especially for multi-device passkeys and considerations for authentication assurance levels and models.

24. Our privacy office indicates that even usernames are PII. So therefore, AAL1 isn't possible? (if the logic is: presence of PII = AAL2).

AAL1 represents authentication processes for lower risk access to online services, information, and applications. If the online service requires establishment of a subscriber account containing associated PII/identity attributes, then AAL2 or AAL3 multi-factor authentication processes are required to protect the account. AAL1 may be selected for accounts that contain no PII (e.g., anonymous accounts).

25. When it comes to inactivity timeout, the IdP has limited visibility to the user's activity (which could span different RPs connected to the same IdP). This leads to implementation of short-lived tokens which are taxing to the IdP and can affect the user when there is an IdP outage. Can you cover acceptable compensating controls such as device lock timeout?

The session requirements are separate between the IdP and RP. The assertions should be short-lived because they are only the starting point for session management at the RP. The session at the IdP should not affect the session at the RP.

SP 800-63C-4

26. Any notable standards/effort that can be used to consistently convey xAL and to support interoperability?

OpenID Connect assertion class reference (ACR) and IETF RFC 8485 Vectors of Trust can be used to convey the xAL. The specific implementation details of data like this are outside the scope of the Digital Identity Guidelines and can be addressed by a protocol-specific profile.

27. Will the bound authentication be verified against the bound authenticator source (e.g., a FIDO key).

Bound authenticators are verified at the RP in a manner consistent with the authenticator itself. A FIDO key would be verified using the FIDO protocols standards against the origin to which the keys are bound. In most cases, a FIDO token would be an RP-managed bound authenticator.

28. The draft indicates that federated logins need to include in their assertion signals statements about which xALs the user is/authenticates as. It wasn't clear on the read-through as to how to implement that. Is there guidance on how the data tags in the assertion are to be tagged, so each RP knows what to look for in code? (also see question 27.)

The specific implementation details of data tags like this are outside the scope of these guidelines and would be addressed by a protocol-specific profile.