April 14, 2023

Name of Submitter: Juliana Cafik

Microsoft input to the National Institute of Standards and Technology (NIST) on Special Publication (SP) 800-63-3 Digital Identity Guidelines, SP 800-63A Enrollment and Identity Proofing, SP 800-63B Authentication and Lifecycle Management, and SP 800-63C Federation and Assertions (together, "the Guidelines")

Note to reader: We have broken our submission into 3 sections:

1. Specific Feedback
2. General Considerations
3. Detailed Comments

NIST 800-63-4 Draft | Specific Feedback:

1. Clarification Request: In Figure 1: Non-federated Digital Identity Model Example (step 1) identity proofing completed successfully with one agency establishes a "subscriber". Is an individual who has become a subscriber with one Credential Service Provider (CSP) required to repeat the identity proofing process and become a new subscriber with each new CSP? If so, this does not align with the approach for Verified ID and expanded guidance to accommodate this model is recommended.
2. Clarification Request: Is it possible to use Verifiable Credentials (VCs) to enable or sustain the re-use of a previously verified identity? While VCs can be stored by an Identity Provider (IDP) at a specific Level of Assurance (LOA) in a user's account for a federation scheme, it is unclear whether they can be used across multiple IDPs. The current guidance explains how VCs can be used to verify the link between a claimed identity and the real-life existence of the subject, but it does not provide instructions for reusing a VC issued at a specific Authentication Assurance Level (AAL) to establish AAL at a new IDP without requiring the user to present additional evidence. Although there is guidance on conveying xAL between parties to allow the reuse of an existing Identity Assurance Level (IAL) from another source, it has limitations as it requires the Relying Party (RP) to maintain the federation dependency for every transaction rather than the initial transaction establishing the user's IAL
3. Consideration: While significant attention is being given to phishing-resistant authentication, there is also a pressing need for guidance on phishing-resistant accounts. We recommend defining a phishing resistant account to cover all aspects of credential lifecycle management, ensuring that the account never elevates from a phishable method to a phishing-resistant method without the appropriate security measures in place.
4. The current 7.2 guidance implies that sessions should never be extended beyond the guidelines, and that authentication factors shall be presented to extend the session. We recommend clarification on the many use cases and industry best practice where contextual, risk and other passive factors, may be a more user-friendly option, and which may be more secure in cases where user credentials have been compromised (therefore negating the value of a re-authentication).
5. Consideration: Encrypting tokens that are handled by intermediaries before presenting them to an RP/IdP can be beneficial. However, ID tokens are typically intended to be used by clients and may contain Personally Identifiable Information (PII) that is presented to the user. In such cases, the value

of encrypting an ID token may be questionable. Even if an ID token is encrypted, the client would still need to decrypt it, which could diminish the benefits of encryption.

6. Overarching Recommendation: Provide a standard NIST Level of Assurance Schema for use in cross-domain authentication context requests. Today, because these values are not set by NIST, ambiguity is created when vendors try to implement the guidance. Without an authoritative recommendation, incompatibility and complexity can result when disparate assurance level values are communicated across domains. Our specific recommendation would be to create namespaced strings for use in XML formatted protocols such as SAML and short-form strings for use in JWT formatted protocols such as OpenID Connect. We have included a set of example strings but recognize these may not exactly represent NIST preferred conventions.

Namespaced Levels of Assurance	Short-form Levels of Assurance
urn:nist:800-63a-4:ial1	ial1
urn:nist:800-63a-4:ial2	ial2
urn:nist:800-63a-4:ial3	ial3
urn:nist:800-63b-4:aal1	aal1
urn:nist:800-63b-4:aal2	
urn:nist:800-63b-4:aal3	aal3
urn:nist:800-63c-4:fal1	fal1
urn:nist:800-63c-4:fal2	fal2
urn:nist:800-63c-4:fal3	fal3

7. Overarching Recommendation: Request to review the two terms: multi-factor authentication and phishing resistance as relative to each other, and taking into consideration that these two authentication strengths are commonly attested as authentication context across domains, with the intention of describing the "authentication instant." Multi-factor authentication is a term in the glossary, and clearly does describe the authentication instant, but there is no equivalent glossary instant for phishing-resistant authentication. References exist in the guidance that refer to phishing-resistance applying to both an authenticator and account, neither of which refer to the authentication instant. This absence creates ambiguity about what exact context would be asserted in authentication method attributes of federated protocols. Attributes referring to "mfa," "phr" etc exist in multiple specifications, including RFC8176, OpenID Connect Extended Authentication Profile (EAP) ACR Values 1.0 - draft 01, and https://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf. While NIST 800-63 guidance does not prescribe the use of any of the above authentication method references, it will help the industry if NIST can have an authoritative cohort of similarly formatted definitions for both terms.

NIST 800-63-4 Draft | General Considerations

1. The use of personal characteristics data for identity verification can pose privacy concerns in the US as there are differing regulations and standards for its collection in different jurisdictions. Stronger guidance with respect to transparency on the collection, use and storage of personal data combined with explicit notice and consent from individuals prior to the collection or use of the data is recommended
2. Request to define "advance equity" with a focus on the promotion of fairness and justice in all aspects of digital identity management, including the protection of individual privacy and civil rights and ensuring that identity verification and authentication policies and practices do not discriminate

against certain groups, and that individuals have equal opportunities to participate in the digital economy without fear of discrimination or bias

3. NIST 800-63-4 acknowledges the need for federal agencies to comply with Section 508 standards. However, specific guidance for making digital identity systems accessible to persons with disabilities and interface with assistive technology is recommended.
4. 800-63-4 has been updated to include new mandates for risk management and the use of biometric-based technologies, however there are some potential gaps that additional guidance could help to resolve:
    - **Implementation challenges:** One gap that may exist in the updated guidance is that it may be difficult for organizations to implement the new requirements for risk management and biometric performance. For example, continuous evaluation of potential impacts across demographics may require significant resources and specialized expertise, which may be challenging for smaller organizations to manage
    - **Lack of specificity with respect to privacy regulations:** The guidance provides biometric performance requirements; however, it is recommended that the guidance on responsible use of biometric-based technologies be expanded to include detail on their ethical use in accordance with privacy regulations
    - **Limited guidance on community impacts**: While the updated guidance mandates that agencies account for impacts to individuals and communities, expanded guidance, or examples, on how to do so effectively would assist organizations in the development of their own frameworks for assessing community impacts
    - **Potential for discriminatory practices:** Some of the methods used for identity proofing, such as knowledge-based authentication (KBA), can be discriminatory against certain populations. For example, individuals who have not lived in the United States for a certain period may not be able to pass KBA questions, which could prevent them from accessing important services
5. Additional guidance recommended with respect to non-repudiation:
    - **Digital signature algorithms:** The guideline provides limited guidance on digital signature algorithms and key sizes, which are essential for ensuring the integrity and authenticity of electronic transactions.
    - **Limited guidance on certificate revocation:** The guideline provides limited guidance on certificate revocation, which is critical for ensuring that revoked certificates are not used to sign or encrypt transactions. The guideline does not provide specific recommendations for certificate revocation mechanisms or how to manage and distribute revocation information.
    - **Limited guidance on timestamping:** The guideline provides limited guidance on timestamping, which is essential for establishing the time of signing and ensuring that signed documents or transactions are valid for a specific period. In addition, the guideline also does not provide specific recommendations for trusted timestamping mechanisms, or how to manage and distribute timestamping information.

NIST 800-63-4 Draft | Detailed Comments

Comment Template for: NIST SP 800-63-4 Suite (Initial Public Draft)						
NIST SP 800-63-4 ipd (initial public draft), Digital Identity Guidelines						
Organization: Microsoft						
Name of Submitter/POC: Juliana Cafik						
Email Address of Submitter/POC: julianacafik@microsoft.com						
NIST Guidance	**Publication** (Base, 63A, 63B, 63C)	**Section**	**Page #**	**Line #**	**Comment** (Include rationale for comment)	**Suggested Change**
Control of a digital account: An individual is able to demonstrate control of a digital account (e.g., online bank account) or signed digital assertion (e.g.,verifiable credentials) through the use of authentication or federation protocols.This may be done in person through presentation of the credential to a device or reader, but is more likely to be done during remote identity proofing sessions.	63A	4.4.1	15	684	Can VC's be used as a way to (or sustain) re-use of a previously proofed identity. This would support the notion that an IDP can store a VC at a specific LOA in the user account for a federation scheme - but can it be re-used across multiple IDP's? Current guidance details how a VC can be used as part of the verification step for the Identity proofing to link between claimed identity and real-life existance of the subject, however, it doesn't provide guidance on the possible reuse of a VC issued at a specific AAL as a way to establish AAL at a new IdP without having the user present additional evidence. While there is guidance for converying xAL between parties that allows reusing existing IAL from another source, it is limiting since it requires the RP to maintain the federation dependency for every transaction vs simply just for an initial transaction that would be used to establish the user's IAL.	Recommend additional guidance to include a VC as a form of digital evidence that can be used in the ID proofing process
Collection of Additional Attributes: Validated evidence is the preferred source of identity attributes. If the presented identity evidence does not provide all the attributes the CSP considers core attributes, it MAY collect attributes that are self-asserted by the applicant	63A	5.3.2.2	26	1057	While it is possible to capture IAL's using a federation trust agreement, there is a need for more dynamic method allowing to convey IALs, specifically for identity attributes collected at different IALs as things evolve.	Recommend provding guidance on a consistent way to communicate an attribute in a way that the respective IAL can be captured per attribute
Authenticator and Verifier Requirements	63B	Section 5	14	657	It would be beneficial to have guidance for allowed MFA method for local authentication (sign-in/logon to machine). There are multiple regulations (IRS 1075, PCI-DSS) requiring the use of an authenticator that is separate from the access device. This leads to many question around the suitability of the platform authenticator as part of MFA to the local device.	There is clarity for accepting platform authenitcator for network/remote authentication, recommend adding guidance for local authentication as well.
Authentication using the Public Switched Telephone Network Use of the PSTN for out-of-band verification is restricted as described in this section and in Sec. 5.2.10. If out-of-band verification is to be made using the PSTN, the verifier SHALL verify that the pre-registered telephone number being used is associated with a specific physical device. Changing the pre-registered telephone number is considered to be the binding of a new authenticator and SHALL only occur as described in Sec. 6.1.2	63B	5.1.3.3	23	917	Is GSMA Rich Communication Services (RCS) considered a PSTN-based authenticator? RCS has significant improvements over the previous generation (SMS).	Guidance explicitly mentions GSMA RCS and how it compares to traditional SMS-based methods. Recommend clarification on whether additional OTA channels (such as WhatsApp) qualify. Since they don't have as strong a relationship as SMS and RCS to the subscriber's identity they might not, but would be useful to spell this out.
Use of Biometrics: Biometric comparison can be performed locally on the claimant's device or at a central verifier.	63B	5.2.3	33	1306	Current guidance for use of biometric as part of a multi-factor authentication clearly covers how biometric can be used as part of a multi-factor authenticator where the biometrics is localy checked by the authenticator. However, while NIST guidance seems to allow for the use of a biometric as part of a multi-factor authentication where the biometrics is checked in a central location, it is unclear how this is possible since also states that biometrics are not an acceptable authenticator (and there is no authenticator class capturing such authenticators). This is leading to various biometrics authentication solution providers arguing their solution is meeting NIST guidance.	Recommend clarification on whether a biometric can be part of multi-factor authentication and not be part of a multi-factor authenticator.
Connected Authenticators: Cryptographic authenticators require a direct connection between the authenticator and the endpoint being authenticated.	63B	5.2.12	39	1508	"direct connection" is not defined. The FIDO CTAP 2.2 hybrid transport protocol uses a mix of protocols to support Cross-Device Authentication in a phishing-resistant manner, without what has been traditionally defined as a direct connection (physical cable, Bluetooth pairing, and/or Wi-Fi direct assocation).	Recommend clarification of the meaning of "direct connection" and whether equivalent solutions like CTAP 2.2 hybrid transport could be considered "direct" (or potentially add a statement about "direct equivalence")
Connected Authenticators: Wireless technologies having an effective range of 1 meter or more (e.g., Bluetooth LE) SHALL use an authenticated encrypted connection between the authenticator and endpoint.	63B	5.2.12	39	1523	"use an authenticated encrypted connection". The FIDO CTAP 2.2 hybrid transport protocol uses an encrypted BLE advertisement to provide data from the client to the authenticator to then allow both parties to establish a secure websocket connection	Recommend clarification for the meaning of "connection" in this context so that solutions like CTAP 2.2 with hybrid transport qualify
Connected Authenticators : A pairing process SHALL be used to establish a key for encrypted communication between the authenticator and endpoint.	63B	5.2.12	39	1524	"a pairing process". The FIDO CTAP 2.2 hybrid transport protocol uses an encrypted BLE advertisement. There is no Bluetooth layer pairing / relationship, by design.	Recommend consideration for use cases where a traditional bluetooth "pairing" relationship is not used (such as hybrid which essentially uses an application level relationship)
Binding of an Additional Authenticator at Exisitng AAL: With the exception of memorized secrets, CSPs and verifiers SHOULD encourage subscribers to maintain at least two valid authenticators of each factor that they will be using	63B	6.1.2.1	43	1627	"at least two valid authenticators of each factor that they will be using". With a passkeys, the same credential could exist in two authenticators. Would a single passkey in multiple authenticators meet this requirement?	Recommend clarity for credential vs authenticator in this context
Single-factor cryptographic device authenticators use tamper-resistant hardware to encapsulate one or more secret keys unique to the authenticator that SHALL NOT be exportable (i.e., cannot be removed from the device). The authenticator operates using a secret key to sign a challenge nonce presented through a direct interface between the authenticator and endpoint (e.g., a USB port or secured wireless connection) as specified in Sec. 5.2.12. Alternatively, the authenticator could be a suitably secure processor integrated with the user endpoint itself	63B	5.1.7.1	28	1098	Does HTTP loopback constitute direct connection between the authenticator and the endpoint being authenticated? Assuming the authenticator secrets are stored in TPM/TEE?	Request clarification
Activation Secrets	63B	5.2.11	38-39	1480 - 1507	Authenticators making use of activation secrets SHALL require the secrets to be a least 6 characters in length. The authenticator SHALL contain a blocklist (either specified by specific values or by an algorithm) of at least 10 commonly used activation values and SHALL prevent their use as activation secrets. If the authenticator verifies the activation secret locally verification SHALL be performed within a hardware-based authenticator or in a secure element (e.g., TEE, TPM) that releases the authentication secret only upon presentation of the correct activation secret. In other circumstances (i.e., software-based multi-factor authenticators), the authenticator SHALL use the memorized secret as a key to decrypt its stored authentication secret.	Request for confirmation of intent to force both activation factor and phone unlock for every authentication?