Comment Template for: NIST SP 800-63-4 Suite (Initial Public Draft)

Please submit responses to dig-comments@nist.gov by April 14, 2023

Organization:	*Google*
Name of Submitter/POC:	*Catherine Nelson*
Email Address of Submitter/POC:	[REMOVED]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
1	63-Base	Appendix A	56	2041	This definition applies to symmetric key pairs as well. Grammar correction.	Modify: "Private Key The secret part of an asymmetric key pair that is used to digitally sign or decrypt data." To: "Private Key The secret part of a symmetric or asymmetric key pair that is used to digitally sign or decrypt data."
2	63A	4	6	442	When verifying identity the user should be provided reasonable assurances that the environment is trusted.	Modify: "At a minimum, this SHOULD include accepting multiple types and combinations of identity evidence, supporting multiple data validation sources, enabling multiple methods for verifying identity (e.g., use of trusted referees), multiple channels for engagement (e.g., in-person, remote), and offering assistance mechanisms for applicants (e.g., applicant references)." To: "At a minimum, this SHOULD include accepting multiple types and combinations of identity evidence, supporting multiple data validation sources, enabling multiple methods for verifying identity to give assurances that the environment is trusted (e.g., use of trusted referees), multiple channels for engagement (e.g., in-person, remote), and offering assistance mechanisms for applicants (e.g., applicant references)."
3	63A	4.3.3.2	11	576	Overall, the proposed 5.1 and 5.1a suggest requiring digital information for STRONG identity evidence. Recognizing that such a requirement would disqualify legacy evidence as STRONG. This assumes the owners of the spec will reject this change if their intent is not to disqualify legacy evidence as STRONG. Justification for 5.1a: Specifying relevant digital information, information which presumably is also presented as analog information (e.g. text) in the identity evidence, is easier for the user to understand (as digital information can mean many things). Requiring "that can be verified" seems incomplete without clarity on what is to be verified, so the modification also tries to disambiguate.	Add the following new sub-sections: "5.1 The evidence includes digital information that can be verified." "5.1a The evidence includes a digital version of the analog information contained in the identity evidence, that can be verified for authenticity of source."
4	63A	4.3.3.3	12	586	This addition clarifies that a person's existence must be physical (as opposed to only digital).	Modify: "The issuing source visually identified the applicant and performed further checks to confirm the existence of that person." To: "The issuing source visually identified the applicant and performed further checks to confirm the physical existence of that person."
5	63A	4.3.4.1	12	605	Grammar correction.	Modify: "Confirming the evidence is not counterfeit and that it as not been tampered with." To: "Confirming the evidence is not counterfeit and that it has not been tampered with."
6	63A	4.3.4.3	13	622	Need to articulate levels of trust based on the situation to properly verify the authenticity of identity.	Modify: "Visual inspection by trained personnel for remote identity proofing," To: "Visual inspection by trained personnel for remote identity proofing meeting the bar of the physical inspection,"
7	63A	4.3.4.3	13	623	Specifies minimum acceptable validation.	Modify: "Automated document validation processes using appropriate technologies," To: "Automated document validation processes using appropriate technologies and achieving at least a comparable standard to manual inspection,"
8	63A	4.4.1	14	673	As written, the party responsible for the capture of evidence is left open to interpretation. It is the responsibility of the CSP to capture video or photograph evidence.	Modify: "The CSP operator may interact directly with the applicant during some or all of the identity proofing event (attended) or may conduct the comparison at a later time (unattended) using a captured video or photograph and the uploaded copy of the evidence." To: "The CSP operator may interact directly with the applicant during some or all of the identity proofing event attended) or may conduct the comparison at a later time (unattended) using a video or photograph captured by the CSP and the uploaded copy of the evidence."
9	63A	4.4.1	14	686	Individuals should be able to validate their authentication independently without having to hand over username/password credentials to a CSP.	Modify: "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." To: "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 validated authentication or federation protocols."
10	63A	5.4.4.1	29	1128	The CSP should not have an indefinite period of time to conduct identity proofing after evidence collection. This process should occur with expediency in a reasonable time frame. Additionally, re-verification to maintain IAL 2 level of trust should be stipulated to ensure the CSP has not fallen out of compliance.	Add the following numbered list items: 3. The CSP shall conduct the identity proofing in a timely manner after evidence collection." 4. The CSP will require re-verification on a predefined frequency in order to maintain the IAL 2 level of trust".
11	63A	5.5.8	31	1209	Many different mechanisms can be used in place of physical tamper detection, broadening a CSP's choice of mechanisms provides a wider range of choices that may be more suitable in a given scenario.	Modify: "6. The CSP SHALL employ physical tamper detection and resistance features appropriate for the environment in which it is located." To: "6. The CSP SHALL require assurances that the environment is trusted and employ resistance features appropriate for the environment in which it is located."

12	63A	5.5.8	31	1232	Re-verification to maintain IAL 3 level of trust should be stipulated to ensure the CSP has not fallen out of compliance.	Add new numbered item to list: "8. The CSP will require re-verification on a predefined frequency in order to maintain the IAL 3 level of trust."
13	63B	4.1.3	7	473	Clarifies that action occurs when reauthentication is not available.	Modify: "The session SHOULD be terminated (i.e., logged out) when this time limit is reached." To: "In the absence of reauthentication, the session SHOULD be terminated (i.e., logged out) when this time limit is reached."
14	63B	4.2.3	9	548	Clarifies that action occurs when reauthentication is not available. Not all instances will require system termination and reauthentication e.g. in the event a screensaver is used with non-exfiltration credentials	Modify: "The session SHALL be terminated (i.e., logged out) when either of these time limits is reached." To: "In the absence of reauthentication, the session SHALL be terminated (i.e., logged out) when either of these time limits is reached. The session termination is not required if there are screensaver and non-exfiltration credentials"
15	63B	4.3.3	11	613	Clarifies that action occurs when reauthentication is not available.	Modify: "The session SHALL be terminated (i.e., logged out) when either of these time limits is reached." To: "In the absence of reauthentication, the session SHALL be terminated (i.e., logged out) when either of these time limits is reached ."
16	63B	7.2	50	1897	Managed devices can play a role in security. Add additional detail around the use of managed devices to achieve the re-authorization. Link "managed device" in suggested change paragraph to NIST glossary here: https://csrc.nist.gov/glossary/term/managed_devices.	Add the following paragraph: "Presentation of reauthentication factors can be performed locally on a managed device that meets the security requirements of the associated authentication level. For instance, a device-lock password enforced periodically at the appropriate intervals can satisfy the memorized secret factor, and similarly a device fingerprint reader can provide the biometric factor."
17	63C	4	6	442	Grammar correction.	Modify: "This can be traced back to a static agreement between the parties or occur implicitly from the connection itself." To:"This can be traced back to a static agreement between the parties or may occur implicitly from the connection itself."
18	63C	4.2	8	501	"May" is more appropriate than "can" in this context.	Modify: "Regardless of the presentation method used, injection attacks can be further mitigated by always requiring that the federation transaction start at the RP instead of being initiated by the IdP, thereby allowing the RP to associate an incoming assertion with a specific request that the subscriber initiated within a continuous session." To: "Regardless of the presentation method used, injection attacks may be further mitigated by always requiring that the federation transaction start at the RP instead of being initiated by the IdP, thereby allowing the RP to associate an incoming assertion with a specific request that the subscriber initiated within a continuous session."
19	63C	4.3	9	532	Remove the language around key material as key material distributed through the well-known path from the OpenID Connect Discovery 1.0 standard is secure and authoritative for a given OpenID Connect issuer and should satisfy FAL3. Similarly, key material retrieved from a SAML IdP via a previously-agreed-upon metadata URL should satisfy FAL3.	Modify: "All identifying key material and federation parameters for all parties (including the list of attributes sent to the RP) SHALL be fixed ahead of time, before the federated authentication process can take place." To: "Federation parameters for all parties (including the list of attributes sent to the RP) SHALL be fixed ahead of time, before the federated authentication process can take place."
20	63C	5.3	21	828	The SHALL statements in this section are business data management practices or overall system management practices, which may be different for every business, or there may be a legitimate business or legal requirement which might require the need to deviate from the requirements. These statements should be guidance, rather than requirements. As such, "SHOULD" is a more-appropriate verb for this constraint.	Replace "SHALL" and "SHALL NOT" with "SHOULD" and "SHOULD NOT" respectively in this section and where applicable throughout the entirety of the document.
21	63C	5.3	21	828	The SHALL statements in this section are business data management practices or overall system management practices, which may be different for every business, or there may be a legitimate business or legal requirement which might require the need to deviate from the requirements. These statements should be guidance, rather than requirements. As such, "SHOULD" is a more-appropriate verb for this constraint.	Modify: "A subscriber's attributes SHALL be transmitted between IdP and RP only for identity federation transactions or support functions such as identification of compromised subscriber accounts as discussed in Sec. 5.5." To: "A subscriber's attributes SHOULD be transmitted between IdP and RP only for identity federation transactions or support functions such as identification of compromised subscriber accounts as discussed in Sec. 5.5."
22	63C	5.3	21	832	The SHALL statements in this section are business data management practices or overall system management practices, which may be different for every business, or there may be a legitimate business or legal requirement which might require the need to deviate from the requirements. These statements should be guidance, rather than requirements. As such, "SHOULD" is a more-appropriate verb for this constraint.	Modify: "A subscriber's attributes SHALL NOT be used by the RP for purposes other than those stipulated in the trust agreement." To: "A subscriber's attributes SHOULD NOT be used by the RP for purposes other than those stipulated in the trust agreement."
23	63C	5.3	21	834	The SHALL statements in this section are business data management practices or overall system management practices, which may be different for every business, or there may be a legitimate business or legal requirement which might require the need to deviate from the requirements. These statements should be guidance, rather than requirements. As such, "SHOULD" is a more-appropriate verb for this constraint.	Modify: "The subscriber SHALL be informed of the transmission of attributes to an RP." To: "The subscriber SHOULD be informed of the transmission of attributes to an RP."
24	63C	5.3	21	840	The SHALL statements in this section are business data management practices or overall system management practices, which may be different for every business, or there may be a legitimate business or legal requirement which might require the need to deviate from the requirements. These statements should be guidance, rather than requirements. As such, "SHOULD" is a more-appropriate verb for this constraint.	Modify: "The IdP SHALL provide effective mechanisms for redress of subscriber complaints or problems (e.g., subscriber identifies an inaccurate attribute value)." To: "The IdP SHOULD provide effective mechanisms for redress of subscriber complaints or problems (e.g., subscriber identifies an inaccurate attribute value)."
25	63C	6.1.2	37	1323	IdP-managed authenticators are vulnerable to IdP compromise scenario. HoK, for example, does not achieve independent authentication.	Modify: "Furthermore, use of a bound authenticator protects the RP against malicious or compromised IdPs through the use of independent authentication." To: "Furthermore, use of a RP-managed bound authenticator protects the RP against malicious or compromised IdPs through the use of independent authentication."

26	63C	6.1.2	37	1326	This could be problematic for enterprise use cases, e.g. using a machine client certificate as a bound authenticator devices will not always be assigned to a single user and thus will not be unique per subscriber We have concerns that a user with multiple subscriber roles should be able to share the account. It would be impractical for individual users to have multiple authenticators per account (e.g. if they have multiple accounts on the same machine).	Modify: "A bound authenticator SHALL be unique per subscriber at the RP such that two subscribers cannot present the same authenticator for their separate RP subscriber accounts." To: "A bound authenticator SHOULD be unique per subscriber at the RP for the lifetime of an assertion such that two subscribers cannot present the same authenticator for their separate RP subscriber accounts."
27	63C	6.1.2	27	1327	Suggest moving this sentence "All bound authenticators..." to 6.2.2 - as this is only applicable for SP bound not IDP-managed bound authenticators Example - TLS certificate is used for the federated login which does not meet IAL3. A relying party should be able to meet FAL3 requirements using holder-of-key with an MTLS certificate, even if that is non-interactive.	Move the following sentence to section 6.2.2 and add reference to section 5.2.5 in 800-63B: "All bound authenticators SHALL be phishing resistant (as defined in section 5.2.5 in 800-63B)."
28	63C	6.1.2.1	37	1342	This clause should be removed, as it precludes mTLS, which should satisfy the goals of IdP-managed bound authenticators at FAL3.	Remove: "Bound authenticators managed at the IdP SHALL be phishing resistant..."
29	63C	6.1.2.1	37	1343	Remove this clause or clarify what 'dereferenceable' means. Perhaps something like 'validatable', 'verifiable', or 'confirmable', if the meaning is that the RP should be able to determine on its own whether the bearer possesses the authenticator."	Remove or clarify: "... and SHALL be independently dereferenceable by the RP based on a mutually-trusted security framework, such as a public-key infrastructure."
30	63C	6.1.2.1	37	1345	Most authenticators have no attributes to validate against. In the HoK example below, the RP should simply verify that the subscriber is in possession of the corresponding private key. Additionally, the mention of 'for the first time' implies that state is maintained on the RP's side for IdP-managed bound authenticators, which is not otherwise implied in this standard. When the bound authenticator is managed by IdP, the RP neither manages the state for the bound authenticator, nor stores any association of authenticator to the user" And therefore (i) an RP cannot verify whether an authenticator is appropriate for the subscriber account. (ii) authenticators do not provide attributes that identifies the subscriber account.	Remove: "When processing an IdP-managed bound authenticator for the first time, the RP SHOULD verify whether the authenticator being presented is appropriate to be associated with the subscriber account, such as through account resolution from the attributes in the authenticator's presented information."
31	63C	6.2.3	43	1467	NIST 800-63C-3 requires encrypted assertions at FAL2 and above. Requiring encrypted assertions starting at FAL2 benefits integrators targeting FAL1 only by simplifying RP and IDP assertion handling while ensuring integrators subject to more stringent compliance regimes realize the privacy benefits of encrypted assertions.	Consider enforcing the following requirement at FAL2 and higher: "When personally-identifiable information is included in the assertion and the assertion is handled by intermediaries such as a browser, the federation protocol SHALL encrypt assertions to protect the sensitive information in the assertion from leaking to unintended parties."