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: MITRE

Name of Submitter/POC: ***Russ Reopell***

[REMOVED]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
1	63	Notes to Reviewers	ii-iv	170-243	Lines 170-243 do not follow the flow of the Digital Identity Guidelines volumes	Suggest rearranging the content of lines 170-243 to align with the 4 volumes of the Digital Identity Guidelines to improve flow. Lines 201-208, then 170-200, then 209--243 (Risk Management, Ideneity Proofing and Enrillment, Authentication and Lifecycle Management, Federation and Assertions, and General.
2	63		iv	225-228	"Is the updated text and introduction of "bound authenticators" sufficiently clear ..." No. The reviewers felt that the discussions related to bound authenticators with 800-63C are not sufficiently clear. The glossary lacks a definition. The glossary should be the authoritative source for all terms.	
3	63	Notes to Reviewers	iv	230-238	"Does the guidance sufficiently address equity?" Although Section 2.3.3, page 8 does a good job of defining equity and identifies groups or individuals that may be affected by inequtites. Lines 574-586, pages 9 leave it up to each organization to consider inequities and remedy on their own, no clear guidance is provided. These are difficult issues to address, however, the reader feels that without providing some clearer guidance organization may wind up with IAL proofing results that are not equivalent, making federation agreements more difficult to negotiate.	Suggest adding example of how certain inequities can be mitigated.
4	63	Notes to Reviewers	iv	231-232	Many of the terms used in the 63-4 update ae are not included in Appendix A Definitions and Abbreviations. See Comments for Appendix A.	Add Definitions
5	63-Base	2	3	355-356	Digital Identity define here limits it to people online. Many devices ,services and applications have identities. Seems to restrict identities to people controlling or monitoring active computing. Many processes operate autonomously without any ongoing, direct human involvement. Their identity relates more to the service they provide rather than a human operator. The definition of Digital Identity needs to be added to Appendix A.	
6	63	2	3	355	Seems to restrict identities to people controlling or monitoring active computing. Many processes operate autonomously without any ongoing, direct human involvement. Their identity relates more to the service they provide rather than a human operator.	
7	63	2	3	361	The person distinction is not clear.	Clarify
8	63	2.2	6	457-488	These lines provide descriptions of the 4 Volumes of 800-63-4 and althought each volume has a set of requirements, only the citing of 800-63A and 800-63C says "Provides requirements..." The requirement sections are normative in each volume and should be mentioned here.	
9	63	4	11	605	Since this entire section is informative, suggest Inserting before line 694 to be consistent with 4.3 and 4.4 "Normative requirements can be found in [SP800-63A], Enrollment and Identity Proofing.	
10	63	4.1	11	611-612	"The entities and their associated functions found in digital identity models include:" does not include the Non-Person Entities (Objects, Service Provider, Resources).	include and provide provide definitions
11	63	4.1	11	613-617	Definition of "Subject" does not match definition in Appendix A, p.60, lines 2161-2162	
12	63	4.1	11	618-622	Definition of "Credential Service Provider (CSP)" does not match definition in Appendix A, p.49, lines 21797-1800. Also in many communities the CSP and IdP are used interchangeably.	
13	63	4.1	11	623-625	Definition of "Relying Party (RP)" does not match definition in Appendix A, p.58, lines 2091-2093	

14	63	4.1	11	630-632	Definition of "Identity Provider" does not match definition in Appendix A, p.52, lines 1919-1921. Also in many communities the IdP and CSP are used interchangeably.	
15	63-Base	4.1	12	Figure 1	IN the non-federated model the Subject (Applicant, Subscriber, and Claimant) all interact with the Service Provider. The CSP, Verifier, and RP are function sof the Service Provider.	
16	63	4.1	12	640-641	Step 2: Upon successful proofing, the applicant is enrolled in the identity service as a subscriber with a digital identity.	add "with a digital identity"
17	63	4.1	12	642-645	Shouldn't this be considered Step 3 or Step 3a?	
18	63	4.1	12	648-657	Since Authentication is separate process from Identity Prooving and Enrollment, should the steps start from 1 again. Perhaps having two diagrams one from enrollment and one for authentication would be clearer.	
19	63	4.1	12	649-650	In situations where the Service Provide Functions are provided by different entities, there are two sub steps that could be shown on the right of the diagram: - Step 4a The verifier interacts with the CSP to verify the binding of the claimant's identity to their authenticators in the subscriber account and to optionally obtain additional subscriber attributes. - Step 4b The CSP or verifier functions of the service provider provide information about the subscriber. The RP requests the attributes it requires from the CSP. The RP, optionally, uses this information to make authorization decisions.	
20	63	4.1	12	633	Service Provider Functions comprise the RP, Verifier, and CSP. The term Service Providers is not defined. Please Add to Appendix and put reference here.	Add definition of "Service Provider" to Appendix
21	63	4.1	13	658	In Figure 2 the Subject (Applicant, Subscriber, Claimant) interacts with an IdP which provideds the functions of a CSP and Verifier AND the subject (Subscriber, Clamant) interat with a Relying Party (RP)	
22	63	4.1	13	659-681	The exisiting text is confusing and in some instances not accurate. Suggest changes provided.	•Step 1: An applicant applies to an IdP through an enrollment process and is identity proofed. •Step 2: Upon successful proofing, the CSP functions of the IdP enrolled the applicant into the IdP service as a subscriber. - The CSP functions of the IdP create a subscriber account and corresponding authenticators that are bound to the subscriber. The CSP functions of the IdP maintain the subscriber account, its status, and the enrollment data collected for the lifetime of the subscriber account (at a minimum). The subscriber maintains their authenticators. The usual sequence of interactions involved in using one or more authenticators in the federated model to perform digital authentication is as follows: •Step 3: The RP requests authentication from the claimant. •Step 4: The claimant proves possession and control of the authenticators to the verifier function of the IdP through an authentication protocol. - Within the IdP, the verifier authenticates the binding of the claimant's authenticators with those bound to the claimed subscriber account and optionally to obtain additional subscriber attributes from the CSP function of the IdP. •Step 5: The IdP provides an assertion and optionally additional attributes to the RP through a federation protocols over secured channels (e.g., TLS or mTLS). •Step 6: An authenticated session is established between the subscriber and the RP.
23	63	4.1	13	651-653	"The verifier interacts with the CSP to verify the binding of the claimant's identity to their authenticators in the subscriber account and to optionally obtain additional subscriber attributes." This fundamental change is commendable, but could be nmade clearer. That this model, called "non-federated" yet with a nominal verifierwhich may be separate from the RP shows this interaction as no more than a HTTPS redirect [most commonly]. This allows for a distinction when descrbing these interactions in a federated model.	"The verifier interacts with the CSP within the service provider boundary, which may or may not involve network protocols to verify the binding of the claimant's identity to their authenticators in the subscriber account and to optionally obtain additional subscriber attributes."
24	63	4.1	13	663-666	"A subscriber account and corresponding authenticators are established between the IdP and the subscriber. The IdP maintains the subscriber account, its status, and the enrollment data collected for the lifetime of the subscriber." This definition differs from that in 642-645.	It's critical that definitions be as close as possible, if not identical in the glossary and the text. In this case, there should be no difference between the federated and non-federated CSP functions.

25	63-Base	4.1	14	689-690	Text says "In all cases, the RP should request the attributes it requires from a CSP or IdP before authenticating the claimant." How can an RP request attribute for an identity that has not been authenticated? The claimant must be authenticated by the CSP/IdP before requesting attributes. The authentication assertion and optional attributes can then be relayed to the RP.	
26	63-Base	4.2	15	706-707	Is "subscriber account" the equivalent of what was a digital identity or credential (63-3) and if so change to: "subscriber account (formerly known as a digital identity or credential)"	
27	63-Base	4.2	15	709-710	The bullets "• bind authenticators provided by the subscriber, and/or • bind authenticators to the subscriber account at a later time as needed. are confusing. Understand binding an authenticator to a subscriber account. What are the authenticators in the first cited bullet bound to, if not the subscriber account? Should first cited bullet read "bind authenticators provided by the subscriber" or "bind authenticators provided to the subscriber" since the previous bullet says issue one or more authenticators to the subscriber. Can authenticatorsissued by another entitiy be presented to a subscribers CSP to be bound to that subscriber?	
28	63-Base	4.2	15	716	"they may be renewed and/or reissued." or "they must be renewed and/or reissued." if renewal requirements are met	
29	63	4.2	15	717	"… authenticators may be invalidated and destroyed …" Overkill, as written. It should be sufficient to either invalidate or destroy the authenticator.	
30	63-Base	4.2	15	723	Why wouldn't a subject who's authenticator has expired or been revoked not be required to repeat the ideneity proofing process? The expired or revoked subject are unknown or their circumstances for ieneity proofing would have changed	
31	63-Base	4.2	15	Figure 3	Based on the definition of Enrollment and Identity Proofing, it would seem that ID proofing and CSP subscriber account creation are the components that make up the Enrollment Process	
32	63-Base	4.2	17	Entirety	Think section 4.3.1 need to be clearer and more concise. The first sentence should define what an authenticator is (Appendix A) and then describe that an authenticator is mde up of one or more authentication factors. It could explain that physical ideeity evidence, KBA, and biometrics by themselves cannot be authenticators.	
33	63	4.3.1	17	733-735	"Something you …" in the three bullets s written in the 2nd person.	Suggest cahnges bullets to: - Something one knows (e.g., a password) - Something one has (e.g., a Smart Card/cryptographic key) - Something one is (e.g., a fingerprint or other biometric characteristic data
34	63	4.3.1	17	745	"The authenticators will have been bound with the subscriber account." should use "to".	Change "with" to "to".
35	63	4.3.1	18	777	"record any authenticators registered (bound) to that subscriber account." shouldn't this read "assign and/or record any authenticators registered (bound) to that subscriber account."	
36	63	4.3.1	18	767-769	"There is another type of memorized secret used as an activation factor for a multi-factor authenticator. These are referred to as activation secrets. An activation secret is used to decrypt a stored key used for authentication or is compared against a locally held stored…" should define "activation factor" before using it.. The document introduces two new terms, activation secret and activation factor. Activation factor should be explained first before defining actiavtion secret.	

37	63	4.3.1	18	773-774	"As used in these guidelines, authenticators always contain or comprise a secret; however, some authentication methods used for in-person interactions ..." subtly switches terminology. The paragraph uses terms "authenticators" and "authentication methods", and begs whether a license is an authenticator that can't be used for online services or whether it's not an authenticator at all. And behind that, it begs whether the biometric itself (in this the claimant's face is an authenticator. And if biometrics are not / can not be used as authenticators, why not drop the entire "something you are"?	
38	63	4.3.1	18	789	"For example, item 1 can be satisfied ...". Change "item" to "option".	
39	63	4.3.1	18	789-790	"... pairing a memorized secret (something you know) with an out-of-band device (something you have)." Please explain "out-of-band". "out-of-band" usually is used to describe a complete, distinct and separate communications channel between a claimaant and a verifier. Here it seems to be used to describe a physical device that the verifier does not actually touch ("out-of-band"), which applies to every "something one has".	
40	63	4.3.2	19	806	Seems too strong. Why can't the subscriber account be updated with information after the proofing process? Wouldn't the subscriber accout be updated every time and Authenticator is bound to that subscriber?	
41	63	4.3.2	19	803-807	Subscriber Accounts As described in the preceding sections, "a subscriber account binds one or more authenticators to the subscriber via an identifier as part of the registration process. A subscriber account is created, stored, and maintained by the CSP. The subscriber account records all identity attributes validated during the identity proofing process." Are Subcriber account the term used to replace credentials in 800-63-3?	
42	63	4.3.3	19	809-810	"... a claimant is who they say they are ...". Change to "claim" [to be].	
43	63	4.3.3	19	Figure 4	The sample Authentication Sequence should start with the Subject/Claimant requeusting access to a resource owned by the relying party. Current Picture show exchange starts with Relying Party requesting Authentication.	
44	63	4.3.3	19	816-818	Shouldn't this sentence end with "over a secure or protected channel (e.g., TLS or mTLS).	
45	63	4.3.3	19	819-822	Shouldn't there e a mention of TLS or mTLS as part of the authentication protocol.	
46	63	4.4	20	830-847	Shouldn't these paragrpahs be used to define federation as the agreement between two or more organizations to share information and that what is described in 800-63 referes to Federated Identity as described in Appendix A, p51, lines 1879-1881?	
47	63	4.4	20	835-839	Appendix defines the acronym PKI but does not define OpenID Connect, SAML, SCIM, or XACML.	
48	63	4.4	20	832-833	Change to: Some common example of "information sharing" or "Federated Infromation sharing"	
49	63	4.4	20	832-839	NIST is to be commended for decomposing federation with the following: "Some common examples include: • sharing identifiers (e.g., using a driver's license number or an email address), • sharing authenticators (e.g., using a PKI authenticator for multiple applications), • sharing identity assertions (e.g., a federation protocol like OpenID Connect or SAML), • sharing account attributes (e.g., a provisioning protocol like SCIM), and • sharing authorization decisions (e.g., a policy protocol like XACML)"	
50	63-Base	4.4	20	842	Should "deploy a digital identity scheme according..." be "deploy a digital identity model according..."	

51	63-Base	4.4	20	848	Should "An organization should consider accepting federated identity assertions if..." be "An organization should consider usinga federation model assertions if..." IF you keep "federated identity assertions" please provide a definition in Appendix A.	
52	63-Base	4.4	20-21	852-853 and 861-862	Item #3 and Item #7 seem to conflict with each other. One says "does not have the necessary infrastructure to support management of subscriber accounts (e.g., account recovery, authenticator issuance, help desk).: while the other says"The ability to centrally manage account lifecycles, including account revocation and binding of new authenticators is important", Managing subscriber accounts would include all that is listed in Item #7.	
53	63	4.4	21	863	Define "federated identity attributes" in Appendix A and refer to it here. Spme attributes may be contextual or environmental.	
54	63	4.4	21	867	It's unclear what partial means here, and whether it means a subset of the subscriber's attributes, the RP's list of acceptable attributes, or something else.	
55	63-Base	4.4	21	868	Derived attribute value" should reference definition in Appendix A.	
56	63-Base	4.4	21	877	"Cost reduction to both the user (reduction in authenticators) and the organization (reduction in information technology infrastructure)." Think cost reduction to users is a stretch . In many instances the cost of the authenticator is not passed on to the user.	
57	63	4.4.2	22	890	"In a federation scenario, as shown in Figure 2, the CSP provides a service known as an identity provider, or IdP." This is not what Figure 2 shows. In Figure 2, the IdP provides the CSP function, not the other way around.	Change "In a federation scenario, as shown in Figure 2, the CSP provides a service known as an identity provider, or IdP." to "In a federation scenario, as shown in Figure 2, the IdP provides a service known as an credential Service Provider, or CSP."
58	63	4.4.2	22	894	" ... provided by the IdP, but the RP does ...". Is not proper english	Change "but" to "as"
59	63	4.4.3	22	919	"... such as personal attributes or expiration times ...". "Personal" is vague about just what it might cover.	Change "personal" to "subscriber" or "claimant"
60	63	5	23	Entirety	The absense of the DecisionsTrees that were in 800-63-3 leaves to much leeway for organizations to arrive at a common assurance level, especially instances where federation between organizations is used. Think reinstated the decision trees to arrive at an initial assurance level is important to continuity across organizations doing risk assessments and in support of federated models.	
61	63	5	23	922	NIST is to be commended in the development of the 4 Step Digital Identity Risk Management process. That said, conducting an initial impact assessment for each assurance level (IAL, AAL, FAL) for 3 or more entities, with 6 or more impact categories, 1 or more harms associated with each category would minimally result in 36-54 impact assessments being made. Once Impact Levels are determined , each impact assessment would require an inital assurance level for Identity, Authenticators, and Federation. ONce an inital assurance level is determined Tailoring and Documenting Assurance Levels is then performed which included assessing privacy, equity, usability, and threats, identifying compensating controls (requirements?), identifying and supplemental controls and documenting the results in the Digital Identity Acceptance Statement. Having to perform this sequence of assessment for each Digital service being offered by and organizations seems to be require a significant effort on the organization provide that service. Does NIST envision this process be performed once for a services offered or once for each service offered? Past experience would lead one to believe that only the minimal amount of effort would be expended during this process using the smallest set of entities and Impact categories required to docment the process.	
62	63	5	23	929-933	The terms "Impact categories" and "impact levels" are not defined in Appendix A	
63	63	5	23	934	The term "Initial Assurance Level" is not defined in Appendix A.	
64	63	5	23	943	The term "Digital Identity Acceptance Statement" is not defind in the glossary	
65	63	5	23	928	Either there are 5 Steps if you include Cyber, Fraud, and Identity Program Integrity OR at a minimum Cyber, Fraud, and Identity Program Integrity should be included as part of Step 4. Continuously Evaluate and Improve.	

66	63	5	23	942	Is "supplemental controls" really additional requirements? This document uses controls and requirements interchangeably, which could confuse implementers of this guidance. Would additioanl security cootrls be part of the RMF process?	
67	63	5	23	953-959	The paragraph seems to be a different way of saying what is already Step 4 and seems redundant. Step 4 should mention that changes uncovered during Continuous Evaluation and Improvement may require revisiting a previous step.	
68	63	5.1.2	25	999-1007	The document lists a minimum of 6 Impact Categories with each have one or more potential harms the could be experienced by an entity. This would require a minmum of 18 impact assessments ot be performed for identity, authenticators, and optionally federation. The addition of more impact categories as described in lines 1005-1007 seem to add undue burden on the organization attempting to complete this process. Can NIST provide any examples of additional impact categories and organization may encounter?	
69	63-Base	5.1.3	26	1055	In is unclear how potential harms to individuals and organizations for each impact category are assessed based on Potential Impact Categories. One has to assess the harm to individuals and organizations and the impact a failure would have for each with impact levels of low, moderate and high resulting in a table similar to the one on page 30. It seems to be up to the organizations to harms for each entity as it relates tot eh Impact of a potential failure, rsulting in an impact level. is this correct?	
70	63	5.1.4	29	1164-1166	"This kind of analysis would be done for each type of potential failure for identity proofing, authentication, and federation to determine the overall risks to entities interacting with the digital identity system."	
71	63	5.1.4	30	Table 1	It is unclear how the Combined Impact Level column is determined because "Combined Impact Level" is never defined. Is it the high water mark impact level of the entities harmed ?	Define Combined Impact Level and show the steps in determining its value
72	63	5.2.2.1	31	1196-1197	Section 4.2 line 701 refers to an IAL0 equivalent to "no identity proofing" and Section 2.2, page 4, lines 408-411 of 800-63A describes a No Identity Proofing (IAL0) level. Recommend the text fro 800-63A lines 403-411 be included in Section 5.2.2.1 of 800-63.	
73	63	5.3	36	In it's Entirety	NIST is to be commended in providing a Tailoring process to allow for modification of an initially assessed assurance level with compensating and supplemental controls, taking into account Privacy, Equity, Usability, and Threats based on an organization's operational environment. The concern however is the introduction of varing forms of xALs to where it becomes difficult to determine if organization A's xAL1,2,or 3 is really equivalent to organization B's xAL1,2, or 3. Please provide guidance onhow organizations can be assured that zALs are indeed eqivalent when tailoring has been performed. Is this only determiend by comapring Digital Identity Acceptance Statements?	
74	63	5.3.4	39	1474-1475	"Federal agencies SHOULD include this information in the system authorization package described in [SP800-37]" Add and make the Digital Identity Acceptance Statement available to other organizations, especially those in which federation is used.	
75	63	5.5	39	1484	Cyber, Fraud, and Identity Program Integrity are critical to the successful operations of an organization's digital sServices as well as the Functions provided by CSP/IdPs. This section should provife much more details on Cyber, fraud and ideniety program integrity and point to the security control baselines available in [SP800-53R5].	
76	63	5.3.1	37	1406	The term "Privacy" is not defined in Appendix A.	
77	63	5.3.1	37	1414	The term "Threat" is not defined in Appendix A.	

78	63	Appendix A	43	1587	If not already mentioned, please add the following definitions to Appendix A: - Activation Secret - Bound Authenticator - Digital Identity Acceptance Statement (DIAS) - Digital Transaction - Digital Services - Identification - Supplemental Control(s) - Control(s) (Security) - Compensating Control - Credible Source(s) - Digital Identity - Verifiable Credential - Verified Credential	
79	63	Appendix A	46		Add "Authentication factor: The three types of authentication factors are something one knows, something one has, and something one is. Every authenticator has one or more authentication factors." to appendix A. Section 4.3.1, line 773 in particular ("authenticators always contain or comprise a secret"), says biometrics (something you are) cannot be authenticators.	"Authentication factor: The three types of digital authentication factors are something one knows, something one has, and something one is. Every authenticator has one or more authentication factors, however, authenticators always contain or comprise a secret. A biometric (somethng one is) by itself cannot be an authenticator."
80	63	Appendix A	47		"An association between a subscriber identity and an authenticator or given subscriber session." There are many more definitions of binding. Other definitions of binding include: --Identity attribute (Vol A, line 408) --Applicant digital information (Vol A, line 533) --Applicant identity (Vol A, line 1079) --Enrollment record (Vol A, line 866) --Channel (Vol B, line 1370) --Verifier name (Vol B, line 1384) --Token (Vol B, line 1383) --Unauthorized (Vol B, line 1940) --Assertion (Vol C, line 1301) --Identifier (Vol C, line 2118)	
81	63	Appendix A	48		"Binding: An association between a subscriber identity and an authenticator or given subscriber session." is ambiguous. Is a binding between a subscriber identity and an authenticator OR between a subscriber identity and a given subscriber session? Or is a binding between a subscriber identity and an authenticator OR between an authenticator and a given subscriber?	
82	63	Appendix A	49		Credential Service Provider (CSP): A trusted entity whose functions include identity proofing applicants to the identity service and the registration of authenticators to subscriber accounts. A CSP may be an independent third party. The identity proofing function should be separated from the CSP. Identity proofing and issuing credentials / establishing accounts are two distinct functions.	
83	63	Appendix A	52		"Identity Provider (IdP): When using federation, this is the party that ... issues assertions derived from the subscriber account." Does not comport with CSP and Verifier definitions. In the glossary, neither the Verifier or the CSP issues assertions; Figure 2 does not include other functions beyond these two.	Identity proofing, account registration / authenticator binding, verification, assertion issuing. Who does what?
84	63	Appendix A	62	2228	"Selected" abbreviations in these guidelines are defined below.	Remove the word "selected" and change to "All" abbreviations used in these guidelines are defied below.

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: MITRE

Name of Submitter/POC: ***Russ Reopell***

[REMOVED]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
1	63A	Advance Equity	ii	148	Bias should also be included as part of the use of biometric-based technologies with respect to demographics. Reference NISTIR 8280 for demographic effects.	
2	63A	Emphasize Optionality and Choice for Consumers	iii	153	Please do not remove requirement to capture a selfie for IAL2. I cannot be absolutely confident that the applicant is who they claim to be other than doing that biometric comparison of the selfie to the strongest form of identity evidence (Passport, driver's license). If one removes that biometric check, then all I have confidence is of (1) the device is registered to the applicant and (2) the device is in the geo-location of the applicant. If I remove that requirement of a selfie from the identity flow, how do I know who is in control of that device? Is it the true applicant or is itthe applicant's child, a (former) spouse, or someone else?	Please keep biometric check in the IAL2 and IAL3 flows.
3	63A	Identity Proofing and Enrollment	iii	178	Nothing can replace capture of face to who possession of device and possession of identity evidence. I suggest use of behavioral biometrics to supplement this flow. Behavioral biometrics can help weed out the bots and fraudsters through hidden challenges as well as familiarity with the application and/or the information asked on the application.	
4	63A	Identity Proofing and Enrollment	iii	181	To my knowledge, behavioral biometrics aren't supported by existing or emerging techncial standards. Having said that, I truly believe these technologies help detect and prevent fraud. It is why agencies have taken a serious look at it. IRS and HHS are two examples of considering use of this technology. Pindrop is a good example of a vendor who offers it (and risk scroing) for call centers. MassMutual has deployed this type of technology for their fraud unit. Reference: https://identiverse.com/video/streamlining-identity-proofing-in-the-contact-center-massmutuals-trusted-identity-program/	
5	63A	Identity Proofing and Enrollment	iii	185	Integration of an mDL will require the CSP to trust the issuer of that mDL. It will also require performing a query (most likely to AAMVA) of the status of the mDL to determine if it's been revoked, suspended, etc.	
6	63A	Identity Proofing and Enrollment	iii	190	Given the rise in synthetic identities, a check on the Master Death Record should be an optional requirement for IAL1 but mandatory for IAL2. Device fingerprinting should be mandatory for IAL1.	
7	63A	Identity Proofing and Enrollment	iii	197	Fraud consortium network should be used at IAL2 to help share known fraudulent events, sources, or IP addresses. The issue I have with these consortiums in practice is that they are closed and only shared amongst that vendor's customer base. I believe there is an opportunity to have Government and Industry work together to create a wider fraud collaboration network. This will capture and share known fraudulent identities and devices on a much broader scale. This fraud consortium network is optional for IAL1 and possibly IAL2. Mandatory for IAL3.	
8	63A	Identity Proofing and Enrollment	iii	199	Partner with DHS S&T for results of their RIVTD testing. In my opinion, liveness detection of a document MUST be part of IAL2 flow. Scanning a document to a computer for upload invites the risk of document replay as well as no proof of possession of that document. Liveness detection of the document will help ensure that the applicant is in possession of that document. Furthermore, I recommend that anyone who submits a scanned STRONG or SUPERIOR evidence be automatically routed to a TR for review.	

9	63	Notes to Reviewers	iv	209-213	"Does the guidance sufficiently address equity?" Although Section 2.3.3, page 8 does a good job of defining equity and identifies groups or individuals that may be affected by inequtites. Lines 574-586, pages 9 leave it up to each organization to consider inequities and remedy on their own, no clear guidance is provided. These are difficult issues to address, however, the reader feels that without providing some clearer guidance organization may wind up with IAL proofing results that are not equivalent, making federation agreements more difficult to negotiate.	Suggest adding example of how certain inequities can be mitigated.
10	63A	2.1	4	394	I would think that another expected outcome of identity proofing is binding the validated identity evidence to the applicant.	Add another step titled Identity Binding Verification and describe this process of binding the validated identity evidence to the applicant.
11	63A	2.2	4	414	What exactly is a "credible source" in this context? Please add a definition of credible source to 63 Base. There could be confusion between credible and authoritative sources. AAMVA is a good example where some will view it as credible and others will view as authoritative. I personally view AAMVA as credible ad not authoritative.	
12	63A	2.2	4	417	I do not see any difference in the collected identity evidence for IAL1 and IAL2. Both require one piece of superior evidence OR one piece of strong plus one piece of fair evidence.	
13	63A	2.2	4	421	I would add language here that SRIP must be in controlled spaces.	
14	63A	4.1	6	450	"A CSP can then bind these attributes to an authenticator ...". This type of binding should be qualified. Binding types include, at least: channel, verifier name, authenticator, session, token, and unauthorized. If identity attribute binding is an additional type, it should be defined more explicitly.	
15	63A	4.1	6	450	It is unclear what attributes are bound to the authenticator in this sentence "A CSP can then bind these attributes to an authenticator" Is it the identity proofed IAL? I assume that one is supposed to go to section 6.1 to read more regarding the binding of these attributes to an authenticator. However, I do not see any language regarding binding of attributes in volume B, section 6.1 or 6.1.1	
16	63A	4.1	6	454	The end of the sentence "to accomplish identity proofing" seems vague. Shouldn't this read that collection of minimum set of core attributes necessary to ensure that the applicant is who they claim to be?	
17	63A	4.1	6	455	shouldn't the agency/customer in concert with the CSP choose the set of core attributes? This reads that just the CSP chooses them.	
18	63A	4.1	7	462	This sentence is confusing. Does it belong somewhere else in the document?	
19	63A	4.1.1	8	466	It would be nice to show the binding in the figure.	
20	63A	4.1.1	8	472	Suggest phrasing this step to be consistent with steps 3 a and 3 b. In other words "The CSP asks the applicant to take a photo of one or more pieces of identity evidence, such as the front and back of their driver's license". Please take in consideration the threat of document replay or document altering with the scan and upload identity evidence from computer flow that is currently permitted. Take a look at document liveness to avoid these threats.	
21	63A	4.1.1	8	473	Do you want to add another step where the CSP sends an email to the applicant to confirm they have control of the email account in the identity resolution phase? I believe this is common practice	
22	63A	4.1.1	8	481-482	That should be an"or" instead of an "and" for. Additionally the language in this step should be consistent with that in 1b above and use the term identity evidence "The CSP compares the picture on the identity evidence (license OR the passport) to the photo..."	
23	63A	4.1.1	9	487	This is the perfect step to add the binding language.	
24	63A	4.2	9	490	Suggest adding the word "core" in front of attributes to read "use the smallest set of core attributes"	

25	63A	4.2	9	490	KBV has been removed from the identity resolution step. Hurray! However, it is still listed in the appendix in 63 Main (line 1934). Suggest stating in Resolution step that KBV SHALL NOT be used for Identity resolution for anything other than IAL0.	
26	63A	4.2	9	491	suggest tweaking this sentence to state that this is within the given population or context of the CSP.	
27	63A	4.3	9	495	This section would benefit from a figure to show the process.	
28	63A	4.3	9	500	key data? What does that mean? Can simplify by removing the text "key data contained on" from that sentence	
29	63A	4.3	9	505	Strongly suggest rethinking allowance of scan of identity evidence for anything above FAIR. This will help prevent replay of digital identity evidience such as a driver's license and passport. Until we have a cryptographically backed digital mdoc such as an mDL, there's nothing to prevent this from occuring. Suggest searching for why do document liveness to learn more about this threat or go to antispoofing.org (https://antispoofing.org/Identification_Document_Liveness_Detection). It seems a few vendors are now starting to implement document liveness including IDR&D, Mitech, and accurascan. Document liveness detection is done similar to PAD for face; a live video of the identity document is taken during capture.	
30	63A	4.3.1	10	520	This requirement of a printed reference number eliminates birth certificate as not all birth certificates issued by the US have a birth certificate number. See https://www.usbirthcertificates.com/glossary/birth-certificate-number	
31	63A	4.3.1	10	523	This is a very awkward and confusing sentence. "The issuer of the document....issuing the document" Suggest a synonym of issuing. Perhaps use "disseminating" or "distributing" instead?	
32	63A	4.3.2	10	526	Please provide a definition of what is meant by digital evidence. See Line 509 which references a digitla record. Is this an mDL type use case (I think yes)? Or does this also apply to an mDL OR a scanned copy of a physical document (which I still have issues with for replay) OR an mDL plus a live capture of a physical document via camera on a smartphone?	509
33	63A	4.3.2	10	533	"... sufficient attributes to bind the digital information to the applicant". This type of binding should be qualified. Binding types include, at least: identity attribute, channel, verifier name, authenticator, session, token, and unauthorized. If applicant digital information binding is an additional type, it should be defined more explicitly.	
34	63A	4.3.3.1	11	548	From a readability perspective, suggest using a similar format for FAIR evidence that was used in 63A.	The evidence: - contains at least one reference number that uniquely identifies the person to whom it relates. OR - contains a facial portrait of the person to whom it relates. OR - sufficient attributes to uniquely identify the person to whom it relates.
35	63A	4.3.3.2	11	560	Add "The full name on the evidence must be the name that the person was officially known by at the time of issuance." Suggest pointing to section 10.1 for equity if the current name doesn't match identity evidence to allow for piecing together the current name (or gender) to a document showing the change in name (or gender). This should be permissible (and a pathway to achieve) for Strong and Superior.	
36	63A	4.3.4.1	12	606	Typo. Change "as not been tampered" to "has not been tampered"	
37	63A	4.3.4.1	12-13	611-615	Conflicting CAN and SHALL statements in this paragraph. Isn't part of verification of a digitally signed object (SHALL) to ensure the document hasn't been tampered with (CAN)? I suggest both of these are a SHALL for an integrity check of the PKI certificate/digitally signed object. This will also work for disconnected use cases for verifying the issuer of an mDL though the RP will need a local cache of the CA trust chain and, opitonally, the CRL. This statement is reinforced in lines 627-628 in 63A section 4.3.4.3.	

38	63A	4.3.4.3	13	620	Incorrect Section Number. Believe this sections should be 4.3.4.2.1 instead of section 4.3.4.3	
39	63A	4.3.4.3	13	623	Be specific regarding who these personnel were trained by. I assume by the CSP but should be explicitly stated here as well as in the practice statement. For the practice statement, there should be lanaguage regarding frequency of training intervals (refresher training) for these personnel.	
40	63A	4.3.4.4	13	629	Incorrect Section Number. Believe this sections should be 4.3.4.2.2 instead of section 4.3.4.4	
41	63A	4.3.4.3	13	625-626	Suggest someway to point the reader to Section 4.3.4.4 for definition of authoritative and credible sources. Also, please add the definition for credible source in Appendix A (main).	
42	63A	4.4.1	14	678-682	"The facial portrait, or other biometric characteristic, contained on identity evidence is compared by an automated biometric comparison system to the facial image photograph of the live applicant or other biometric live sample submitted by the applicant during the identity proofing event." Looking for an eample of automated biometric comparison other than face. The only other biometric characteristic that could be compared is the fingerprint. Yet I'm unaware of a use case where the fingerprint is taken of the applicant and compared to what is contained on the identity evidence for a Use Case though for CAC and PIV a fingerprint is captured and stored in the chip during enrollment after the applicant has been identity proofed. Given that 63A is digital only, I don't think voice applies (nor do I know of any evidence that stores a voice print on a chip). I would appreciate an example of that alternative biometric is.	
43	63A	5	16	692-694	"This section also includes additional requirements for Federal Agencies regardless of whether they operate their own identity service or use an external CSP." Wouldn't these requirements apply/benefit to other organizations such as banks? Should a sentnece be added that states although these reuuirements are targeted at Federal Agencies, organizations and institutions looking to provide higer assurance identites would benefit for this guidance.	
44	63A	5.1.1	16	700-701	"The practice statement SHALL include, at a minimum" Suggest adding 10. The frequency for performing audits and (refresher) training of CSP personnel.	
45	63A	5.1.1	16	708-712	Need to document whether the use of credible or authoritative source is used to collect the core attributes as well as the method of collection.	
46	63A	5.1.1.2	17	732	Please specify where these mitigations are documented. I assume they will be documented in the practice statement.	
47	63A	5.1.2.1	18	769-771	Suggest adding another sentence at the end of this bullet for Federal Agencies to publish a SORN per PIA if core attributes are retrieved by the subscriber (I'm thinking stored in subscriber's account could be the same as retrieved by the subscriber). A PIA helps define if a SORN is required. "The Privacy Act requires Agencies to publish a SORN describing the personally identifiable information collected, maintained, and used in an automated system. If personal information is collected but never retrieved by the unique identifier, it is not a system of records and a SORN is not required." Also direct the reader to section 5.1.5 for SORN/PIA and additional requirements for federal agencies.	
48	63A	5.1.9	19	977	Applicant references is not defined in the appendix of 63 Main (just lift the definition in lines 977-978 in 63A). Also suggest mentioning to the reader that furtehr discussion of what an applicant reference is will be in section 5.1.9.	
49	63A	5.1.5	20	848-857	I suggest this is a strong SHOULD or a weak SHALL. I think outreach is absolutely critical to gain acceptance in IAL2 identity proofing for any citizen facing platform (and could help avoid some unwelcome media attention). You may want to consider moving this paragraph up on the list.	

50	63A	5.1.6	21	683	Enrollment codes can also be mailed to the address of record to start an identity proofing process for mDL. Here, the DMV will mail a one-time enrollment code to the address of record. The driver launches the mDL app on their phone and enters the one-time enrollment code in the app prior to starting the resolution step in identity proofing....See DHS S&T mDL Handbook for reference.	
51	63A	5.1.6	21	866	"... re-establish an applicant's binding to their enrollment record ..."This type of binding should be defined. Binding types include, at least: identity attribute, channel, verifier name, authenticator, session, token, and unauthorized. If enrollment record binding is an additional type, it should be defined more explicitly.	
52	63A	5.1.5	21	861-862	Shouldn't this be documented in the practice statement?	
53	63A	5.1.8	22	911	I am unsure how a fingerprint can be used to help identity proof someone. It certainly can be used to authenticate a person for PIN reset or at a door lock. I'm drawing a blank for identity proofing use case and would appreciate an example.	
54	63A	5.1.8	22	922	add "how it is protected"	
55	63A	5.1.8	22	923	What about retention of biometric data for fraud detection and prevention? I would think this is a separate issue. The question is: does this need to be documented publicly somewhere?	
56	63A	5.1.8	22	924	Should also include bias. Suggest referening NISTiR 8280	
57	63A	5.1.8	22	915-916	".... verify that an individual is the rightful subject of identity evidence, and/or bind that individual to a new piece of identity evidence or credential. ...". If this is the same as applicant digital information binding, it should be made clear. There are many types of binding defined in Volume A, or so it seems, and each type should be defined	
58	63A	5.1.8	23	948	Remove line 948 as this is a duplicate of line 943.	
59	63A	5.1.8	23	957	How does one remotely view fingers as part of the proofing process without some sort of fingerprint reader (in controlled spaces)?	
60	63A	5.1.9	24	969	the TR must be identity proofed at the highest level they are identity proofing others for the CSP.	
61	63A	5.1.9	24	969	Please include who trained the TR. I assume the CSP trains them.	
62	63A	5.1.9	24	970	The term Risk-based decision is not defined in 63-A or in Appendix A of Main. I think it would be helpful to provide an example of a Trusted Referee making a risk-based decision	
63	63A	5.1.9	24	963-968	also if name/gender/address of applicant doesn't match on presented strong/superior identity evidence.	
64	63A	5.1.9	24	979-980	Who trains the applicant reference? Where are they physically located? With the applicant? With the TR? How does the TR determine whether the AR has already been identity proofed at the appropriate level? How does the TR know that the AR is being truthful in their vouching of the applicant? This seems like a leap of faith if this is a neighbor of the applicant or an acquaintance. Sorry, but I have fraud on my mind and I can see without a background check or some sort of liability tied to this individual that this role can be misused.	
65	63A	5.1.9.2	25	1003	How are the applicant references affiliated with the CSP? How does the TR determine whether the AR has already been identity proofed at the appropriate level?	
66	63A	5.1.10	25	1021-1022	Suggest requiring a parent or guardian to be in the room as a minor under the age of 13 during an identity proofing event with a TR.	
67	63A	5.3.4	27	1079	"... verify the binding of the applicant to the claimed identity ...". The type of binding referred to is unclear.	
68	63A	5.3.4	27	1084-1085	I assume that this is for IAL0 accounts if the applicant can log into a digital account with an AAL1 authentictor. I also assume that this IAL0 account is in control or the CSP? Else how would the CSP confirm that the applicant is in control of that account (from a purely NON federated perspective)? Also, will there be some attribute associated with the version (revision 3 or revision 4) of what level this person was identity proofed at given IAL0 (revision 4) is pretty much the same as IAL1 (revision 3)	

69	63A	5.4.4.1	29	1133-1134	I assume that this is for IAL0 or IAL1 accounts if the applicant can log into a digital account with an AAL2 authentictor. I also assume that this IAL0 or IAL1 account is in control or the CSP? Else how would the CSP confirm that the applicant is in control of that account (from a purely NON federated perspective)? Also, will there be some attribute associated with the version (revision 3 or revision 4) of what level this person was identity proofed at from a federation perspective?	
70	63A	5.5.2.1	30	1157	Two pieces of SUPERIOR will be problemmatic for many though mDL I believe is deemed SUPERIOR. If this is accepted, then there will need to be an mDL reader in place	
71	63A	5.5.2.1	30	1159	Would one piece of SUPERIOR and two pieces of FAIR be permitted? Some may not have a state ID/driver's license but have a passport. a utility bill, and a bank statement.	
72	63A	5.5.6	31	1197	Shouldn't this also state that the biometrics are retained?	
73	63A	5.5.7	31	1205	I assume that fingerprints are captured at a kiosk in controlled spaces or in-person.	
74	63A	5.5.4	31	1190-1191	I assume that this is for IAL2 accounts if the applicant can log into a digital account with an AAL2 authentictor. I also assume that this IAL2 account is in control or the CSP? Else how would the CSP confirm that the applicant is in control of that account (from a purely NON federated perspective)? Also, will there be some attribute associated with the version (revision 3 or revision 4) of what level this person was identity proofed at from a federation perspective?	
75	63A	5.5.8	31-32	1214-1218	IAL3 is intended to be as close to being in person as possible. It is highly recommended that the kiosk be in controlled spaces where it is extremely difficult from it being tampered in any way. Having a kiosk in a shopping mall defeats the confidence that the kiosk hasn't been tampered with. I would use stronger language here to express this issue. I think that the outcome of a risk assessment will help determine placement of the kiosk. For example, a H/H/H MUST be in controlled spaces. I think having a kiosk at a shopping mall is perfectly appropriate for lower risk use cases and for IAL1 and IAL2 and will allow equitable access for those who do not have Internet. Public location for kiosk is better suited for IAL1; semi-public or restricted or monitored: IAL2 or IAL3	
76	63A	5.5.8	32	1228	Please clarify what you mean by "restricted area" vs. "monitored by a trusted individual" vs. semi-public vs. public spaces. Otherwise it is subject to interpretation	
77	63A	5.6	33	Table 1	Is Biometric Collection actually Biometric Retention?	
78	63A	6.1	34	1249	In addition to stating "Maximum IAL successfully achieved for the identity proofing of the subscriber" one should also state at what revision of 800-63 was used to identity proof the subscriber. Without this knowledge, how do I know if IAL1 was revision 3 or revision 4?	
79	63A	6.3.2	35	1280-1281	Consider adding a bullet regarding death of the subscriber via due notice period from the RP	
80	63A	6.3.2	35	1283-1290	Who or what provides notice to the CSP regarding any of the use cases listed in this section? I assume the RP.	
81		7	36	1301-1308	Add definitions for Impersonation, False or Fraudulent Representation, and Infrastrucutre to Appendix A.	
82	63A	7	37	Table 2	Add Video injection attack. Attacker creates a fake video feed of an individiual associated with a real person. Example could be: Deepfake video is used to impersonate the individual portrayed on the stolen driver's license.	
83	63A	7.1	37-38	Table 2 & Table 3	The mitigation stategies in table 3 are based on the examples in table 2. I think it may be easier to combine the two tables.	
84	63A	7.1	38	Table 3	I know the purpose is to not be redundant in these mitigations but I would suggest adding check vital statistics such as Birth records or Death Master File to Synthetic Identity Fraud as another check.	

85	63A	7.1	38	Table 3	Social engineering is a tough one to mitigate against especially since fraudsters love to target call centers with this attack. If something seems off (in the typing speed, copy/paste, etc), then I would suggest as another mitigation to just require the applicant to go in person if the CSP offers this as another option for proofing applicants..	
86	63A	10.1	52	1742	Why not provide an option to allow upload of another form to show change in name such as what is required with REALID (show proof of name change, gender, marital status) to show linkage of current name to what was provided previously. This proof of documentation also applies for change in gender as well as marital status.	
87	63A	10.1	52	1741-1742, 1758	I would be very careful regarding the use of Applicant Reference vouching for an individual. If it is for something like a passport, one CANNOT use an Applicant Reference to vouch for a name mismatch. There are clear requirements that everything must match and show a paper trail for a change in name or gender. For something lower risk, sure use an Applicant Reference. In summary, I don't understand what an Applicant Reference will vouch for if documentation is missing or not matching what is in official records. A paper trail must be provided to show the change in name.	
88	63A	10.1	53	1768-1774	I believe the number one mitigation of a victim of identity fraud/theft is to have the applicant come in-person. I don't know how a TR or an AR can make that determination. Even for the IRS, they have these individuals come in-person.	
89	63A	10.1	53	1790-1791	I need an example of what a risk-based alternative would be as a possible mitigation for poor capture of facial image. Is this going in person or to a kiosk?	
90	63A	10.1	53	1795-1796	Compare iris of the applicant to the identity evidence should be another mitigation. Add "Employing robust image capture technologies that are able to capture iris"	
91	63A	10.4	54	1828	Is a helper an Applicant Reference? Please clarify. Also state whether the helper is identity proofed at the level of the applicant.	
92	63A	10.4	54	1827-1834	Additional mitigations: I find that having autocapture of image of identity evidence and capture of facial portrait better from a usability aspect for those who are challenged in taking pictures. It also helps to ensure the lighting is correct and all 4 edges of the identity evidence is captured.	
93	63A	10.4	54	1846-1847	If in-person, why would there be equipment and workstations that need to be adjusted for heights and angles? I think you mean for the use of a kiosk?	

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: MITRE

Name of Submitter/POC: ***Russ Reopell***

[REMOVED]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
1	63B	2	3	373	Revocation term generally focuses on PKI certificates. Consider using "invalidation."	
2	63B	2	4	399	AAL3 seems to require use of public-key cryptography. If so, consider making explicit.	
3	63B	4.2.2	9	531	How is the authenticated channel created before the claimant authenticates?	Clarify what type of channel is needed? Is authentication of the verifier by the claimant primary?
4	63B	4.4	12	645	Are there separate provisions for PII of biometric catagories?	
5	63B	4.5	13	Table 1	Entries in this row are difficult to read. Types seem to repeat in columns, in different order, complicated by word wrap	Recommend list types that are accepted at only the AAL Then add item for any type accepted at a higher level. So explicit types listed are only accepted at that level. Types explicitly listed at lower AAL are not accepted. Explicit types should only appear in one column.
6	63B	5.1.1	14	672	Is "authenticated" the proper techncial term? "secure" or "encrypted"? Or should the word "channel" be replaced by "session"	
7	63B	5.1.1.2	16	756	Define memory-hard and compute-hard (or give references) if not otherwise defined.	
8	63B	5.1.2.1	17	793	The delivery should involve mutual authentication of subscriber and deliverer.	
9	63B	5.1.3	18	819	Set up of the out-of-band must use mutual authentication to ensure integrity of shared secrets. This applies to the second channel in Figure 1	
10	63B	5.1.4.2	25	994	TOTP systems may need to maintain a drift factor for a device whose clock has drifted and recall the device if the drift is extreme.	
11	63B	5.1.6.1	27	1081	Should hardware devices that import private keys rather than generate on board also be categorized as software? Applies to line 1155 also.	
12	63B	5.2.1	31	1230	Are there IOCs associated with this?	
13	63B	5.2.3	32	1259	Technology may improve over time. Are there currently differing reliable benchmarks for FMR given the biometric challenge technique?	
14	63B	5.2.3	32	1257-1258	"For a variety of reasons, this document supports only limited use of biometrics for authentication." This section begs a NIST responsibility. The reasons for limited use of biometrics suggests that biometric standards should be developed or sanctioned by NIST to define biometric assurance levels (BALs) in the same way that the other assurance levels are defined and utilized.	
15	63B	5.2.3	32	1262-1263	"Biometric comparison is probabilistic, whereas the other authentication factors are deterministic." True, but of no value. This statement assumes there's something valuable about deterministic factors, but this is all a probabilistic exercise regardless. As the document says when discussing AALs in the beginning, stronger authenticators improve the likelihood the claimant is legitimate. Ironically, the section goes on to state those criteria.	
16	63B	5.2.5.1	35	1381	The most current version of TLS is 1.3 which is considered to be more secure than 1.2. A reference to the most "up to date" version may be prudent.	
17	63B	5.2.11	38	1492	These 10 seem arbitrary. There are infinite permutations and combinations that can be made with the word "password" alone. Should there be a standard blocklist?	
18	63B	6.1	41	1562-1564	The term "authenticator binding" is not defined I Appendix A of 800-63.	
19	63B	6.1.1	42	1618-1619	" ... through use of a biometric that was recorded during a prior encounter." The biometric could be used for authentication. It would seem that in-person enrollment would provide an opportunity to provide a biometric to the CSP [whose template] could be used for further authentication modalities.	

20	63B	6.1.2.3	43	1654-1656	"If a subscriber that has been identity proofed loses all authenticators necessary to complete authentication, that subscriber SHALL repeat the identity proofing process described in [SP800-63A]." Agree, however this languauge is not consistent with the language used in 800-63A, page 15, lines 715-717.	
21	63B	6.2	46	1767	Perhaps reports should go through channels rather than directly to the CSP. Local actions may be necessary to mitigate possible damages.	
22	63B	8.1	52	1917	"Authenticator Threats". Shouldn't this be "Authenticator Attacks"? Rigorous threat models distinguish between the threat actors (threats) and the actual attack itself.	
23	63B	8.1	52	1940	Table 3 "Authenticator Threats". Should be labeled "Authenticator Attacks"? Threat refers to the actor while attack describes the action. These are actions	
24	63B	8.1	52	1936-1937	"This document assumes that the subscriber is not colluding with an attacker who is attempting to falsely authenticate to the verifier." For what it's worth, biometrics can thwart some collusions. If the Verifier has access to a biometric collected at registration, collusion can be thwarted because while the legitimate subscriber can hand over something they have and something they know, handing over a biometric is much harder. (Obviously, little can be done if the subscriber authenticates for the attacker and walks away).	
25	63B	A.2	81	2694	should there be a minimum standard for blocklists (size or number of entries)? Is there a known standard of unacceptable passwords?	
26	63B	A.4	82	2730	Are there multiple throttling techniques that are prioritized? timing backoff windows?	
27	63B	A.5	83	2739	Is rate limiting the only throttling technique? Are there standards for timing and backoff windows?	

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: MITRE

Name of Submitter/POC: ***Russ Reopell***

[REMOVED]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
1	63C	Note to Reviewers	iii	170-173	The section describing FAL2 and FAL3, including "bound authenticators" is not clear enough to implement. Many available binding types are not adequately addressed: channel, verifier name, authenticator, session, token, and unauthorized.	Describe bindings in more detail.
2	63C	Notes to Reviewers	iii	170-173	"Is the updated text and introduction of "bound authenticators" sufficiently clear ..." No. The reviewers felt that the discussions related to bound authenticators with 800-63C are not sufficiently clear. The glossary lacks a definition. The glossary should be the authoritative source for all terms.	
3	63C	Notes to Reviewers	iii	179-183	"Does the guidance sufficiently address equity?" Although Section 2.3.3, page 8 does a good job of defining equity and identifies groups or individuals that may be affected by inequtites. Lines 574-586, pages 9 leave it up to each organization to consider inequities and remedy on their own, no clear guidance is provided. These are difficult issues to address, however, the reader feels that without providing some clearer guidance organization may wind up with IAL proofing results that are not equivalent, making federation agreements more difficult to negotiate.	Suggest adding example of how certain inequities can be mitigated.
4	63C	Notes to Reviewers	ii-iv	170-243	Lines 170-243 do not follow the flow of the Digital Identity Guidelines volumes	Suggest rearranging the content of lines 170-243 to align with the 4 volumes of the Digital Identity Guidelines to improve flow. Lines 201-208, then 170-200, then 209--243 (Risk Management, Ideneity Proofing and Enrillment, Authentication and Lifecycle Management, Federation and Assertions, and General.
5	63C	1	2	330	Consider including Federation Authority.	
6	63C	2	3	338	The CSP acronym is not defined in this document	Define
7	63C	2	3	346	Would be helpful to list justification for using Federation within a singe security domain as stated: "though federation can be applied within a single security domain for a variety of reasons."	Since his section is "informative", it would be useful to list some examples and rational for using Federation in a single domain
8	63C	2	3	338-340	"In a federation scenario, the CSP provides a service known as an identity provider, or IdP. The IdP acts as a verifier for authenticators issued by the CSP." This is backwards from the main document. Figure 2, line 658 of the main document, shows the IdP encompassing the CSP and the Verifier. Here the CSP is supreme, providing the IdP function.	
9	63C	4	6	417-418	"These levels can be requested by an RP at runtime or required by the configuration of both the RP and the IdP for a given transaction." Is the RP an end relying party providing information, or is the RP an agency's interface in a Federation? This depends on a better understanding of FALs and just what the RP can request. In the old version, the RP drove the FAL.	
10	63C	4	6	431	Signature detects modification but not necessarily forgery (signer key compromise or signer "tricked"). Also does not preclude copying	Delete forged
11	63C	4	6	432-435	"Audience Restriction" is not defined in Appendix A.	
12	63C	4	6	427-431	"Cryptographic Verifiability" is not defined in Appendix A.	
13	63C	4	6	436-438	"Injection Protection" is not defined in Appendix A.	
14	63C	4	6	439-442	"Trust Agreement" is not defined in Appendix A.	

15	63C	4	6	440-442	"The IdP and RP have agreed to participate in a federation transaction with each other for the purposes of logging in the subscriber to the RP." This is anathema to the ICAM concept of separting ICAM from RP information providers. The purpose of single sign-on and the last two decades is to get RPs providing [mission] functions from managing an account for each user. Yet here the subscriber logs in to their account.	Change the purpose to something to the effect that the IdP and RP agree to some set of practices that assures the other needed they are adhering to whatever cybersecurity and other policies.
16	63C	4	6	444-445	"The IdP and RP have exchanged identifiers and key material ..." is ambiguous. "Key" has multiple meanings, including "important".	Add "security" prior to "key". Or "cryptographic"
17	63C	4	6	446-448	"Presentation" is not defined in Appendix A.	
18	63C	4	7	448	Bound authenticator not defined sufficiently at this point	Define better here or provide forward reference to definition
19	63C	4.1	8	482-483	"In this example, the trust between the IdP and RP is driven entirely by the desires and actions of the subscriber." The subscriber's desire would seem to be irrelevant. The FAL, as described earlier, is a function of the trust agreement and mechanics between the IdP and the RP. The subscriber should be oblivious to the behind-the-scenes security.	Delete the sentence. Or reword "driven entirely by" to "developed with consideration of"
20	63C	4.1	8	485-486	"In existing federation protocols, FAL1 can be implemented with the OpenID Connect Implicit Client profile [OIDC-Implicit], ..." perhaps should be deleted. Is this not deprecated?	
21	63C	4.3	9	519-520	"At FAL3, the subscriber SHALL authenticate to the RP by presenting an authenticator directly to the RP in addition to presenting an assertion."	Question: Does this prevent break & inspect?
22	63C	4.3	9	519-530	The "bound authenticator" concept is not federation. It describes an independent authentication event using an authenticator directly with the RP. As described, the authenticator would be "dually-bound", with both the IdP and RP subscriber accounts, but the authentication events are sequential. Without additional novel communication between the RP and the IdP, the IdP cannot determine if FAL3 was achieved, or if the federation transaction on its own is FAL2. If this requirement has assurance merit, it should be socialized with standards bodies prior to using it to establish an assurance boundary in US Government policy.	Recommend adopting "proof of possession" as the replacement criteria for FAL3. Extensions to common protocols with vendor implementations such as mTLS binding, Private JWT, and Demonstrated Proof of Possession provide token constraint with cryptographic proof of possession.
23	63C	4.4	9-10	544-549	"The RP SHALL be informed of ... the FAL of the federated transaction". The FAL is somewhat under the control of the RP as well as the IdP. The RP knows (or could / should /may) know whether there's a trust agreement. This is the only difference distinguishing FAL1 from FAL2. FAL3 is under the control of the RP and whether it authenticates the subscriber directly. The IdP does not know this.	Delete.
24	63C	4.4	10	550-555	"The RP gets this xAL information from a combination of parameters in the trust agreement as described in Sec. 5.1 and information included in the assertion as described in Sec. 6." This is not true and regardless, contradicts the previous line that the IdP provides the FAL. The previous line claims the FAL is provided by the IdP yet here it says the IdP can identify the FAL from the Trust Agreement. Whether the connection is FAL3 or not is solely under the control of the RP.	
25	63C	5	12	591	This figure appears to show a situation where interactions with both IdP and RP are within the subscriber's computing environment.	Address situations where the RP is in a different computing environment.

26	63C	5	13	606-607	"Next, the IdP and RP determine that they want to engage in a federated authentication transaction to authenticate the subscriber." should be reworded. The singular "subscriber" is applicable only in the second case (probably the less common) in the prior sentence where negotiation takes place in real time between the IdP and RP. Where the establishment of credentials and identifiers occur before any subscriber logs on would be determined for all [in a class] of subscribers.	Make subscriber plural.
27	63C	5.1	14	643-644	"... when the RP and IdP first contact each other for the purposes of a subscriber's login." "Login" is the wrong word. Login implies the user has an account with the RP. ICAM principles of single sign-on expect that RPs accept the authentication from an IdP and then allow access.	Change "login" to "authentication". NOTE: The RP may need some apriori knowledge of the subscriber in order to allow access to RP resources.
28	63C	5.1.1	15	704	Who or what will be federation authorities? What is their likely motivation or incentive?	Give explanations or examples.
29	63C	5.1.1	16	710	Will there be an approval authority for IdPs or does each federation authority have to evaluate IdPs?	Clarify
30	63C	5.1.3	17	742	There is no reference to Figure 3 in text	Reference it where appropriate
31	63C	5.1.3	17	742	What trust agreements are involved in the proxied arrangement? Does Final RP know that assertion originated with original RP? Does Proxy IdP modify or wrap original assertion in its own assertion. There could be a chain of proxies. The chain my be to the intended RP or the intended RP could rely on a set of RPs of which the subscriber is not aware.	Address the chains of calls and the implications on trust agreements and knowledge of the identities of the intermediaries.
32	63C	4.3.3	20	819	Consider equating well-designed protocols with challenge-response protocols.	
33	63C	5	24	922	The analysis and process described in this section appear very subjective. Some may view that the risk assessment uses dubious inputs to produce dubious outputs.	
34	63C	6	34	1243	If the signature is supposed to encompass all of the listed attributes, recommend making it the last item in the list.	Move item
35	63C	6	35	1261-1262	"Additional information about one or more subscriber attributes,such as those described in NIST Internal Report 8112 [NISTIR8112]." Isn't this superseded? Shouldn't SP 800-205 be cited instead of NISTIR 8112? 800-205 states it extends 8112 and it was this commenter's understanding that SPs had more gravitas than NISTIRs.	Change reference to SP 800-205.
36	63C	6	35	1263-1265	"Assertions SHOULD specify the ... IAL when identity proofed attributes (or values derived from those attributes) are being asserted." This is too restrictive. The IAL should be provided regardless of whether and identity proofed attributes are included in the assertion. If the IdP knows the IAL it should be provided. Indeed, Section 4.4, line 545, makes no such restriction.	
37	63C	6	35	1282-1283	"... an assertion represents a discrete login event to the RP." "Login" is the wrong term. An assertion represents an authentication, not a login. Note that four sentences later the wording says: "... for a repeated authentication ...".	
38	63C	6.1	36	1302-1305	"Assertion binding can be classified based on whether presentation by a claimant of an assertion is sufficient for binding to the party currently in session with the RP as the subscriber ..." seems to be wrong. 1) "currently in session" would seem to be premature if the session is not establsihed until the RP receives the assertion. 2) It would seem that if presentation of the assertion is sufficient for the RP, which would be a bearer assertion, then it's not bound at all.	
39	63C	6.1.1	36	1307	What is the "bearer's identity?" Id of the original principal or the identity of the proxy bearing the assertion on behalf of the principal?	Clarify

40	63C	6.1.2	36	1319-1320	"A bound authenticator is an authenticator presented to the RP by the subscriber alongside the assertion." What does it mean to present an assertion alongside an authenticator? "Present an authenticator" can be understood to be a physical action by a clamaint, but claimant's cannot physically present assertions. If this is meant to be a software protocol action, then the subscriber is not presenting.	Recommend using NIST 8122 and SP 800-205 to provide both attribute expiration and last updated in the identity API data returned. This allows the RP to operate as it likes. Should any attribute change prior to expiration, the IdP could use the signaling mechanism in Section 5.7 or possibly include the updated attribute value in the assertion.
41	63C	6.1.2.1	37	1356-1357	"... since the IdP knows the subscriber's key to be used at the RP and includes the key information in the assertion ..." could be more precise.	
42	63C	6.1.1.2	39	1359	What value does the IdP provide when the RP-manages the Bound Authenticator? How does the Bound Authenticator get bound to the identity associated with the Primary Authenticator?	Clarify more clearly in following discussion.
43	63C	6.1.2.1	39	1363-1364	"... RP subscriber account must include a bound authenticator." Accounts do not include authenticators. The cornerstone of 800-63-3 and this version is the definition of authenticator: "Something the claimant possesses and controls ...". The RP cannot include the authenticator; it belongs to the clamaint. Lines 644-645 of the main document include: "The subscriber maintains their authenticators."	
44	63C	6.1.2.1	40	1374-1375	",,, the RP SHALL perform a binding ceremony to establish the connection ...". "Ceremony" is a peculiar word choice.	
45	63C	6.1.2.1	41	Figure 11	Figure 11's depiction of a FAL3 Assertion is confusing. The "FAL3 Assertion: RP-Managed Bound Authenticator" is an assertion, but is depicted as if it's an authenticator itself.	
46	63C	6.1.2.1	41	Figure 11	Figure 11's caption, "Binding Ceremony", should be further clarified. Given there are are least seven types of binding, more specificity is warranted.	
47	63C	6.2.2	43	1454	A reference is needed for "approved cryptography"	Add reference
48	63C	6.2.3	43	1456	Give a reference for how to encrypt (e.g., Crypto Msg Syntax RFC).	
49	63C	6.2.3	43	1467	A reference is needed for "approved cryptography"	Add reference
50	63C	6.2.5	44	1509	The list does not adequately address the legal authorities under which pseudonymity must be revealed. Agency policies may differ substantially in their policies and regulations.	"The proxy SHALL NOT disclose the mapping...or use the information for protected communication categories established by agency policy. Protected categories MUST be disclosed to subscribers and relying parties. Protected categories vary by agency and may include attorney-client privilege, doctor-patient confidentiality, and whistleblower protection."
51	63C	6.3	45	1537-1538	"... MAY be provided to the RP through a protected attribute API known as the identity API ..." creates an unnecessary term. There is no need to define attribute API only to define identity API.	Change to "through a protected API known as the identity API."
52	63C	6.3	46	1152 & 1555	"authentication(s)" would be a better word than "login(s)".	
53	63C	6.3	46	1558-1560	"The IdP can indicate in the assertion when the last time the subscriber's attributes have been updated in the subscriber account, allowing the RP to decide if it needs to fetch the attributes anew or if those in the RP subscriber account are sufficient." defeats much of the purpose of backchannel attribute retrieval. Adding one additional parameter to the assertion, when the latest attribute was updated forces the RP to query for all of its needed attributes whenver any attribute changes, perhaps not even one it uses. If this were to be further decomposed for each attribute, providing a last updated date, it would be more cumbersome.	
54	63C	11	68	2118-2119	"... allows the binding of additional federated identifiers to an RP subscriber account ...". This type of binding seems to be undefined / unqualified. Binding types include, at least: channel, verifier name, authenticator, session, token, and unauthorized. If identifier binding is an additional type, it should be defined more explicitly.	

55	63C	12	69	2127	Section 12 discussion includes Kerberos and SAML which seem to be legacy standards whose future new use may be limited. Also the discussion omits federations using WS-Security standards which should be considered if SAML remains. MS still uses WS-Security.	
56	63C	12	69	2127	There are no examples of bound authenticators.	Include if available (e.g., FIDO)
57	63C	4. FAL; References - Standards		461; 2282	"...the IdP SHALL employ appropriately tailored security controls (to include control enhancements) from the moderate or high baseline of security controls defined in [SP800-53] or equivalent federal..." The latest Version is 5, December 2020, this is the version that should be required for the Security and Privacy Controls implemented.	Change NIST SP800-53 Revision 4 to Revision 5. While no specific implementation date required by FISMA & NIST of the latest baseline, Revision 5 now incorporates several Privacy Controls which should be implemented given the sensitive and PII information stored and transmitted.