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

Please submit responses to dig-comments@nist.gov by October 7, 2024.

Organization:	*Self*
Name of Submitter/POC:	*Ann West*
Email Address of Submitter/POC:	

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
1	63-Base	2.5		861	It is common for IdPs to maintain authorizations to RPs for the federation internal to an organiztion - that's a benefit of integrating a comprehensive access management system with the IdP. But it is uncommon when IdP and RP are in separate security domains. As stated elsewhere, access decisions at the RP are ABAC style, using attributes from the IdP, in part, to determine access. IdP does not know the outcome of that RP decision.	Revise statement
2	63-Base			886-88	This model doesn't seem to accommodate what InCommon presumes will be a common use case: CSP for user authentication differs from CSP (Issuer) of attribute bundle selected for the RP. Different Sources of Authority for different attribute bundles. More is said about this in comments on 63C.	
3	63A				The term "trust agreement" is used in several places in a manner that might not always be consistent with its use in 63C. Indeed, the glossary entry in 63A and in 63-base refers to its use specifically in federated context. In 63A context it appears to refer to a contract between an RP and a CSP to establish the CSP as the outsourced provider of RP's proofing and authentication functions. These two contexts, and two uses, should be distinguished from each other. In particular, under 63C a trust agreement need NOT take the form of a contract between RP and CSP.	Use a different term for an obligation required to be met by a contract between an RP and its outsourced CSP.
4	63A	2.2		628-31	Consider defining in bold "Address," including statements about Physical Address and Digital Address, to clarify the term used throughout the document.	Revise accodingly. Also consider adding "address" to the Glosssary in 63 base doc.
5	63A	3.1.1		861-62	This makes sense when CSP is under contract with RP to act as RP's 3rd party CSP provider. However, in a multilateral federation with many IdPs and RPs, the IALx claims provided by IdPs are to be trusted by RPs, which have satisfied themselves that federation policy and procedure provide adequate basis for that trust. Without this trust, RPs face a significant operational burden of needing to review normal changes across many IdPs to satisfy themselves that these changes do not contradict the IALx claims. This should be managed by the federation, not each of its entities.	Amend requirement to pertain to RPs that are clients of the CSP, ie, that have contracted with the CSP as an outsourced provider of authentication and proofing services.

6	63A	3.1.2.1		945	Shared signaling is great in some contexts but far less so in a federated context as the scale increases beyond a few handfuls of IdPs. Cost of its deployment it in an environment of thousands of organizations across many dozens of countries, like global R&E federation, outweighs benefit. Furthermore, some segments have standardized on one of a couple of popular (among security people!) security event management platforms for accomplishing what shared signaling does and more.	Reduce to MAY.
7	63A	3.1.2.2		969-72	Applicable only when RP has contracted with CSP as outsourced provider of authentication and proofing services.	Revise language to clarify applicability of this SHALL.
8	63A	3.1.7		1140-44	There is a difference between an agency ***contracting*** with a CSP to provide proofing and authentication services and that agency ***relying on*** federated IdPs for that purpose. Both of these may be understood with them term "uses". Clarify which is intended, or if both are intended. If federated IdPs are intended to be in scope, these and similar requirements, that entail manual review of lengthy and non-standardized plain language and complex legal terms, will impose serious headwind to adoption.	Replace both occurances of "uses" with a clearer verb, or otherwise clarify context of applicability.
9	63A	3.1.13.3		1420-22	CSPs internal to an enterprise do not serve the public - they only proof and credential members of the enterprise: employees, perhaps students.	Modify requirement to pertain to CSPs offering their service to the public at large.
10	63A	3.1.13.3		1432-34	This criterion seems applicable only to RPs that will contract with a 3rd party CSP. If that is the idea, say so explicitly.	Revise language to clarify applicability of this SHALL.
11	63A	4.1.1		1509-11	How does this being required bear on mitigating risk of fraud? Shouldn't a CSP that only does attended proofing be able to meet IAL1? This criterion seems better suited as a term in a contract an RP may have with a CSP than as an IAL1 requirement.	Omit these requirements.

12	63A	4.1.5		1543-44	Collection of a government identifier is not elsewhere required, but this language appears to implicitly do so. If it is to be required, make that explicit, perhaps in 2.2 above. If not, then remove this phrase since government identifier is already listed as a core attribute.	Revise accordingly.
13	63A	4.1.9		1617-18	What is the purpose, normatively, of including this clause? If only mitigations of these types is to be required, then say so.	
14	63A	4.1.10		1632	Consistently use only "address" in order to avoid misunderstanding.	Omit "of record".
15	63A	4.2.1		1658-60	How does this being required bear on mitigating risk of fraud? Shouldn't a CSP that only does attended proofing be able to meet IAL1? This criterion seems better suited as a term in a contract an RP may have with a CSP than as an IAL1 requirement.	Omit these requirements.
16	63A	4.2.2		1668	Does adding 1 FAIR to 1 STRONG accomplish any additional risk mitigation? Core attributes presented on STRONG evidence are checked with credible or authoritative sources. These same attributes would be checked again if they appear on FAIR evidence. Since fabricating a convincing piece of FAIR evidence is not very difficult (many forms have no physical or digital security features) and CSPs are already required to rely on the stronger form of evidence for collecting core attributes, it's hard to see any additional fraud mitigation value here.	Consider revising to require only 1 STRONG for IAL2.
17	63A	4.2.5		1693	Collection of a government identifier is not elsewhere required, but this language appears to implicitly do so. If it is to be required, make that explicit, perhaps in 2.2 above. If not, then remove this phrase since government identifier is already listed as a core attribute.	Revise accordingly.

18	63A	4.4		1920	The table cell for Evidence Collection at IAL1 lists FAIR with photo as a requirement for attended proofing, yet the criterion in 4.1.2 says SHOULD, not SHALL.	Since Table 4 is in a normative section, align that cell with 4.1.2.
19	63B	2		472-74	There are use cases in which the identifier should NOT be the same each time the subscriber authenticates to an RP. Eg, access to online library materials licensed to a university or public library.	Amend statement to say only that authentication produces an identifier. Perhaps clarify that it might not be the same each time that subscriber authenticates to that RP, depending on the requirements of the use case.
20	63B	2.2		572-73		Clarify that this statement applies to RPs.
21		2.2		582-83		Clarify that this requirement pertains to verifiers that function as part of an RP, either directly or under contract, not necessarily to verifiers integral to a CSP that interacts with the RP using federation.
22	63B	2.2		585	How can a verifier encourage?	Replace "verifiers" with "CSPs".
23	63B	5.1		1888	This statement does not conform to a federated authentication scenario, in which the verifier is disjoint from the application.	Replace "verifier" with "session host", as in the following paragraph.
24	63C	2 thru 5			The 2nd public draft of 63C continues to include topics that have little to do with mitigating risk associated with use of federating technology: provisioning and shared signals. Provisioning has always had potential impact on security of application systems, and perhaps guidelines focused on mitigating risk associated with provisioning should be developed. But it is unnecessary to address it in 63C context. And while shared signaling is a Good Thing in certain contexts, its	Omit statements or sections as noted in separate rows below.
25	63C	4 and 5			63C is meant to address security risks to be managed in operation of federation. There is a difference between managing liability and managing security risk that appears to have been blurred in places here, as seen in some of the obligations placed on trust agreements. Any organization's Legal Department is extremely unlikely to permit a 3rd party, such as a fedration authority, to be a party to any contract in which they either accept or assign liability. Hence trust	Omit trust agreement requirements that serve to manage liability rather than operational security.
26	63C	3 thru 5			Some requirements of trust agreements apparently call for plain language text to be included addressing this or that. Just FYI, the InCommon Federation used plain language expressions in its original federation agreement format, the Participant Operating Practices statement which was required to be posted by each participating member. This approach didn't acheive our goals in large part because use of plain language impedes scaling. As the federation grows, RPs must review greater numbers of extensive plain language statements, which gets to be very burdensome. Likewise, the ability of the federation to ensure that all POPs are maintained in a timely fashion is a huge on-going support effort mostly due to normal staff turnover at member organizations. As new people take over, they don't have their predecessor's understandings and things slide until the federation operator notices. Then they must compete with member organization's newly established priorites to make time for re-education and support of new employees in matters federation, including updating their POP.	Minimize, if not eliminate, use of plain language terms in trust agreements, and replace with standardized expressions and formats that are machine readable. Where standards do not yet exist, make the trust agreement requirement a MAY. As one means of minimizing use of plain language, consider simpler formulations of terms that accomplish much the same as a lengthy explanation. Eg, an acknowledgement that some identifed common terms, perhaps identified by a federation authority,
27	63C	3.3.1 onwards			The term "subject identifier" is used in a specfic way to help define "federated identifier" in section 3.3. Unfortuantely, "subject identifier" is used in many places subsequently where "federated identifier" or "subscriber identifier" should be used instead.	Replace most occurances of "subject identifier" after the start of section 3.3 with "federated identifier." InCommon has not noted each occurence here. Containing sections should be reviewed to ensure proper use of normative terms.

28	63C	3.2.1		705-6	Belonging to a multilateral federation does not obligate an RP to accept transactions from all IdPs in the federation	Insert "potentially" before "suitable".
29	63C	3.2.2		717	63C is not meant only for federal agencies.	Use "enterprise" instead of "agency".
30	63C	3.2.3		738-40	In practice, there are proxies for which this statement is true and some for which it is not. Examples of the former tend to be internal to a single enterprise, providing outboard federation support to the downstream RPs. Research community and infrastructure proxies, on the other hand, tend to operate as a joining of two different federations, each with their own federation authority. It remains true that in these cases the RP side facing the upstream federation is a party to its trust agreement, and likewise for its IdP side facing the downstream federation.	Omit this statement.
31	63C	3.3.1.1		843-45		Say that the ***RP's*** privacy policies SHALL ...
32	63C	3.3.1.3		881-86	The paragraph is only informative. Perhaps it belongs in section 10. Also, this reviewer wondered what impression may be left on the reader when most examples inserted into normative sections refer to OIDC and few involve SAML. Would they think SAML is unable to address the exemplified matter? That would generally be inaccurate.	Omit. Consider refctoring most exemplary material in normative sections into section 10, and try to balance use of the major federating technologies among examples.
33	63C	3.4		888		Replace "defined" with "constrained".
34	63C	3.4		888-9	This language is clear that there may be multiple trust agreements bearing on federated transactions between an IdP and an RP, yet all statements in subsequent sections about trust agreements refer to a singular trust agreement.	Amend language in subsequent sections accordingly, so that readers might not infer that one authority must have perspective and responsiblity over all matters assigned to trust agreements in 63C, or that all trust agreements of necessity must be bilateral contracts.
35	63C	3.4		897-99	An RP may have a specific reason for needing this information and can include it in associated trust agreements, but in general the IALx attribute should suffice. Else why have a standard? Furthermore, details of the proofing process may contain clues to the subscriber's identity that are not meant to be shared.	Reduce from SHALL to MAY.
36	63C	3.4		927-38	Non-normative language is used here. The privacy/informed consent value of these statements accrue mainly in consumer/citizen service use cases (C2B). For an enterprise (B2B) there will be some means quite apart from its IdP/CSP operations by which it informs its members of what it believes it must inform them. Please ensure that if this material is to continue to the final 63C-4 that it does not constrain enterprises in a needless way.	Use normative language to articulate requirements and articulate applicability to use cases in which the authorized party is the subscriber, ie, C2B use cases.

37	63C	3.7.3		1179-86	Since these requirements do not bear on any federated transaction, they do not belong in a trust agreement.	This is strictly 63B territory, so remove from 63C.
38	63C	3.9		1250-58	Provisioning material, as well as liability managing material such as this, should be omitted.	Omit.
39	63C	3.9		1255-58	Since IdPs are not required to provide a provisioning API, this statement must be modified. Furthermore, a common use for account linking is to provide a subscriber continuity of service at an RP as their organizational affiliations change. If they no longer retain a subscriber account at IdP1, they may still have a qualifying subscriber account at IdP2 and the RP should NOT deprovision the subscriber's RP subscriber account.	Amend requirement to avoid undermining the value of account linking.
40	63C	3.10.2		1342-45	This statement is well-intentioned but only informative. Besides, there are as yet no standard means of "passing this information along". Maybe for 63C-5...	Omit.
41	63C	3.11.1		1405	The language "is able to be presented by the IdP that created the assertion" is unclear. Perhaps it means that RPs should check if an IdP is sneaking something into an assertion for which it has no authority??	Clarify.
42	63C	3.11.3			This section should be constrained to requirements of identity APIs when used as part of a federating technology, ie, specifically as back-channel alternative to providing subscriber attributes via a front-channel assertion. Pre-provisioning is not a federating technology and should not be addressed here. It is the domain of contracts between service providers and enterprises using their services. Indeed, an enterprise exposing all PII held by their CSP via an identity API to an outside party had better have their liability addressed in a contract - that cannot be handled by a compliance specification.	Restrict requirements about identity APIs to their use as a back channel for presenting federated assertions. Any use made of the same API for provisioning operations should be covered by contract and be out of scope for 63C.
43	63C	3.11.3		1459-60	What is the relevance of where the identity API is hosted?	Clarify or omit.
44	63C	3.11.3.1		1481-89	This example is NOT one of an attribute providing service under contract to an IdP. Of course an IdP cannot be responsible for accuracy of medical license details - that's the domain of the medical licensure agency. Instead of this spec trying to make the IdP responsible in ways that it cannot be, treat independent Attribute Authorities like in this example as first class actors in federation, treated the same as an IdP, just one that need not issue authentication assertions. An RP that wants to rely on assertions provided by an Attribute Authority should have its own trust agreement with it, or both AA and RP should belong to the same federation whose trust agreement covers the relevant terms.	Omit entire section as it contributes nothing over the preceeding section. Consider whether adding Attribute Authorites to the set of federation entities in scope for 63C would resolve some of the misaligned responsibility and authority issues with sections like 3.11.3.1.
45	63C	3.12.3		1518-21	These uses of "subject identifier" are at odds with its use in section 3.3, and the statement that they are necessarily meaningless outside of a target system is often untrue.	Amend first sentence to say "... excluding opaque identifiers such as the federated identifier or a PPI". Omit the next two sentences.
46	63C	3.14		1575-77	Provisioning-based requirement, so omit. Further, some RPs with ephemeral provisioning may need to know returning subscribers. Examples abound in the sciences. Also, why is this statement in this section?	Omit.
47	63C	4.1			This section is not baked. It uses undefined terms, is almost void of normative language, and seems to reflect an architecture more specific than what 63C should be applicable to, especially, there is no provisioning of CSP accounts to an IdP when the two functions are integrated.	Revise or omit.

48	63C	4.1		1713-14	What risk mitigation does this perform?	Omit requirement.
49	63C	4.2		1736-7	Subscriber accounts need not be provisioned to the IdP - it may have direct access to them. Also note non-normative use of "subject identifier".	Revise.
50	63C	4.2		1748-8	As noted in a comment below on 4.6.1.3, a runtime decsion at the IdP concerning attribute release need not be undertaken by a human, in which case there is no prompting.	Revise to "If necessary, the authorized party makes a runtime decision to approve the release of attributes".
51	63C	4.3.1		1783-85	Only the 2nd bullet appears to have significance to the RP. Any other attributes used between CSP and its IdP are not the concern of any RP.	Omit the first bullet.
52	63C	4.3.1		1786-89	What federated risk mitigation do these two bullets provide? What do they mean, precisely, and how are they to be expressed in a standardized way?	Omit these two bullets.
53	63C	4.3.1		1792	What standardized language can be used for this purpose? Also, should the approach instead be that there is a separate trust agreement for each subscriber population, or subsections of one trust agreement each addressing specific terms applicable to associated subscriber groups?	Revise this bullet to a MAY. Revise this and other bullets to allow more flexible reporting of how an IdP's assertions vary for each of its various subscriber subgroups.
54	63C	4.3.1		1793-4	What federated risk mitigation can this provide, given that it's expressly "beyond providing the identity service"?	Omit.
55	63C	4.3.1		1797	What standardized language can be used for this purpose?	Revise to a MAY. Or revise the term to say RP agrees to the limited set of uses permitted by the IdP.
56	63C	4.3.1		1798-99	Reorient this concern towards the IdP - let it stipulate use of its subscribers' attributes rather than having to evaluate every RP's practices to see if they confiorm. That's lots of unnecssary work. Should this bullet explicitly say that a federation authority may determine uniform constraints on attribute storage by RPs?	Revise the term to say RP agrees to the attribute storage constraints required by the IdP or the federation authority.
57	63C	4.3.1		1800	Shared signaling requirement.	Omit
58	63C	4.3.1		1803	Plain language explanation can be replaced by an acknowldgement that subscribers are informed about attribute release to the RP in a manner compliant with 63C.	Revise as suggested.
59	63C	4.3.1		1804	Link this with subscriber subgroups.	See comment on line 1792 above.
60	63C	4.3.1		1809-12	Rather than lengthy plain text reporting on assessment results, have each IdP and RP acknowledge compliance of their redress mechanisms with 63C, or with another standard that suffices (perhaps set by the federation authority).	Revise as suggested.
61	63C	4.4		1880		Add "or RP" to "IdP".
62	63C	4.6, 4.6.1, 4.6.2			These sections, ie, 4.6, 4.6.1, and 4.6.2, are unnecessary and should be omitted. Requirements elsewhere already express under whose authority what attributes can be released to a given RP. These sections push such requirements down to the level of several imagined implementation environments, yet other operational environments not envisioned in this section already exist to manage federated transactions. Hence this material is overly prescriptive and should be omitted.	Omit these sections entirely.
63	63C	4.6		1936-7	This statement appears to explicitly permit storing of runtime decisions to be applied to future transactions, yet that is contrary to the proper operation of an access management system that extends to federated transactions. Omit this statement - it depends on aspects of the encompassing operational architecture that are outside of 63C's purview.	Omit statement (if entire section is not removed).
64	63C	4.6		1945-47	Repeats a requirement already given in 3.4.3.	Omit.
65	63C	4.6.1.3		1986-89	Why should a runtime decision necessarily need to be made by a human? When organizational authority applies to the transaction, automation may be used, eg, by integrating the IdP's actions with an access management system. This section should be rewritten to better address enterprise, B2B scenarios.	Revise entire section, if it is not entirely omitted.
66	63C	4.6.2.3		2036-43	The issues with this non-normative language include: . posits only one of many possible solution implementations . encourages use of email for purposes at best suited only to C2B use cases and very ill-suited to B2B use cases . fails to indicate that a federation service may provide a solution . repeats the error that only direct human interaction can represent an organization's authority. As there is nothing else of substance in this section, omit it entirely.	Omit section 4.6.2.3
67	63C	4.6.3			Provisioning should be out of scope for 63C.	Provisioning section should be out of scope and omitted.
68	63C	4.6.3		2098-99	This requirement is absent from the list of terms required of a trust agreement in 4.3.1. Please consider consolidating such requirements in one place in 63C. Also, this requirement has no bearing on mitigating risks associated with use of federating technology.	Omit requirement.
69	63C	4.6.4		2128-31	A common use for account linking is to provide a subscriber continuity of service at an RP as their organizational affiliations change. If they no longer retain a subscriber account at IdP1, they may still have a qualifying subscriber account at IdP2 and the RP should NOT deprovision the subscriber's RP subscriber account.	Amend requirement to avoid undermining the value of account linking.
70	63C	4.6.4		2131-34	This is another example of how scope is creeping beyond risk mitigation associated with use of federation. Sharing of some PII has already been permitted in this draft spec for purpose of security incident response. Consider leetting other specifications and agreements determine how security incident response proceeds.	Omit requirement.
71	63C	4.6.5			Provisioning should be out of scope for 63C.	Provisioning section should be out of scope and omitted.
72	63C	4.6.6			This section addresses circumstances that are independent of federation, hence beyond what 63C should try to address.	Omit section.
73	63C	4.6.7			This section has little to do with risk mitigation due to federation. The situation addressed in this section occurs with or without federated access to an RP's services.	Omit section.

74	63C	4.7		2229-31	This statement is inconsistent with the statement at lines 1448-1450 above.	Rewrite, remove idea of independence from the federation transaction because that defines the start of a limited time window during which access is permitted.
75	63C	4.7		2251-56	It is also sufficient if the federation protocol supports the RP initiating a reauthentication request and the IdP is required to oblige. Consider not requiring that both entities mind the same session. It should be the RP's responsibility, not left up to a 3rd party in some other security domain.	Revise statements to focus on RP requesting reauthentication and requiring IdP to act on it when the federation protocol supports reauthentication requests.
76	63C	4.7		2266-72	Need this be said? Anything not addressed in this spec is outside of its scope, tautologically.	Omit.
77	63C	4.8			Since shared signaling is outside of the use of federation, why should anything about its operation be addressed in 63C? Parties so willing can create their own trust frameworks in which operation of shared signaling among them is defined.	Omit section.
78	63C	4.9		2324-26	This statement is needless. Consider removing the first paragraph of this section given it does not add clarity.	Omit.
79	63C	4.9		2383-95	All of this info is stated elsewhere. Omit these redundancies.	Omit.
80	63C	4.10		2402-04	Is there a standard way of expressing "purpose of use at the RP" or "requirements for the authentication event at the IdP"?	As these are meant to be SHALLs in an authentication request, the values MUST be machine readable if they will serve any purpose. Either remove these elements of these two bullets or restrict their use to where standards have been established. Eg, to request MFA authentication (without specifying which MFA technologies are permitted, for which there is no standard to this reviewer's knowledge).
81	63C	4.11		2415-16	Already covered in 3.2.3 and serves no further purpose in this section. Assertions are presented to a proxy's RP side as with any RP.	Omit.
82	63C	4.11.1		2419-21	It is required elsewhere for the entire assertion to be resistant. If there is nothing specific that should further protect an assertion reference, then omit this statement.	Omit.
83	63C	4.11.1		2442-25	Non-normative statements should be omitted. Both front-channel and back-channel presentation are permitted. It is not true that one is "more permitted" than the other, nor is it true that the attack surface is strictly smaller with back-channel presentation because then the back channel itself is exposed to attack, unlike in a front channel architecture. The purpose of this spec is to define what's good enough, leaving the choice of implementation architecture up to those responsible for it.	Omit.
84	63C	4.11.2		2473-77	See above comment re lines 2442-45	Omit.
85	63C	5		2499-2501	This stipulation appears to be more precisely defined immediately below. Omit this less precisely defined form.	Omit.
86	63C	5.1 - 5.5			The current draft spec only contemplates a wallet architecture in which all bundles in a subscriber's wallet, and the wallet itself, are controlled by a single CSP. Other acceptable wallet architectures are possible and may in fact be under development or testing as of this writing. Consider the medical licensure attribute provider example of section 3.11.3.1. If that provider wants to provide attribute bundles to licensees, must it then also manage their wallets entirely, or engage in contracts with all CSPs in which any of their licensees may be subscribed, only to satisfy 63C requirements pursuant to this constrained architecture? That seems untenable. Does this architecture lead to the necessity of people needing to manage many wallets, one for each facet of their lives?	Rethink the constrained wallet architecture contemplated in 63C. Might recognition of Attribute Authorities as federation entities resolve some of this?
87	63C	5.4		2581	Avoid conflicting meanings.	Pre-pend "attribute bundle" to "provisioning system" if you do not remove other provisioning material from 63C. Avoid conflicting meanings.
88	63C	5.4.1		2592-97	Apparently, the second and third SHALLs are one means of achieving the first SHALL, but not necessarily the only means.	Either reduce the second and third SHALLs to MAYs, or omit the first SHALL altogether if you do not believe any other means of deprovisioning bundles from wallets is possible.
89	63C	5.5		2605-08	This statement doesn't appear to leave room for a federation service that provides this information.	Rewrite statement so as to not exclude a federation service
90	63C	5.8		2671	Please discuss what an "intended FAL" is and how a wallet should compute it. How does the wallet know when the subscriber is acting in different federations?	Clarify requirement.
91	63C	5.9		2703-04	The analogous requirement of a general IdP is SHALL. What is the reason for this difference? If none, the requirements should be the same.	Align requirements or explain why they are different.
92	63C	5.11		2734-35	Why? Enterprise uses of wallets are just as likely to use pre-provisioning, as are scientific use cases in which an allocation or authorization decision must have occurred prior to first access by the subscriber. Another example of why provisioning should be out of scope for 63C.	Omit.
93	63C	5.11		2738-41	This requirement has already been given earlier.	Omit duplicate stating of requirement.
94	63C	6.1		2760-62		Omit "agency's" in both places.