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:	*OpenID Foundation*
Name of Submitter/POC:	*Mark Haine*
Email Address of Submitter/POC:	[redacted]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
MH1	63-Base	1	1	346	"a digital identity is intended to demonstrate trust between the holder of the digital identity and the person," - The words "demonstrate trust" in this sentence does not reallly convey what digital identity is for.	Suggest "... communicate reliable attributes about the person presenting information to the person, organization or system..."
MH2	63-Base	1	1	346	"holder" should be defined	Add a definition for the term "holder" or refer to a suitable definition elsewhere
MH3	63-Base	1	1	349	"attacks that fraudulently claim another person's digital identity. "	suggest adding "or real identity." or removing "digital"
MH4	63-Base	1.3.1	5	518-519	"preparing for new technologies (e.g., mobile driver's licenses and verifiable credentials) that can leverage strong identity proofing and authentication" - this strongly implies that other technologies cannot leverage strong identity proofing and authentication; that is incorrect.	Suggest removing "that can leverage strong identity proofing and authentication"
MH5	63-Base	2.1	10	646	"relyin party"	"relyin party" should be "relying party"
MH6	63-Base	2.1	10	656	"Verifier" - Suggest using a different term as this term is already overloaded in identity syatems. "Verifier" is used (and widely accespted) in the W3C Verifiable Credentials data model definition and "Verification" is widely used in the context of ensuring a piece of evidence relates to the person presenting it.	Suggest using "Authentication Verifier" instead of just "Verifier"
MH7	63-Base	2.2.1	12	683	This section only refers to wallets, it would be more general purpose to add mention of IDPs	Add reference to IdPs as well as "subscriber-controlled wallets". Perhaps change "Provision the subscriber account to one or more general-purpose or subscriber-controlled wallets, for use in a federated protocol system" to "Provision the subscriber account to one or more general-purpose or subscriber-controlled wallets or IDPs, for use in a federated protocol system"
MH8	63-Base	2.2.1	12	683	"subscriber-controlled wallet" is different from "user-controlled wallet" that was used on line 158 - a common term should be used throughout.	Suggest consistent use of "user-controlled" as it is slightly more general
MH9	63-Base	2.3.1	12	703	It would be useful to have a definition of "secret" that states the properties of a secret - "known by only one or two entities" etc	Suggest adding definition of "secret"
MH11	63-Base	2.5	19	877	"Step 6: An authenticated session is established between the subscriber and the RP" could be improved	Suggest reword to "An authenticated session is established by the RB with the subscriber."
MH12	63-Base	2.5	19	886-891	There is an component in the Figure 5 model that is not described in the text about Figure 5 the (NIST) Verifier. The term verifier is used in that passage but it is used with the "tree-party model" meaning. For full clarity it would be very informative to describe how the NIST definition of "Verifier" fits with the "three party model".	Suggest adding in some words to describe the role that the (NIST) Verifier component is used in the model; described in Fig. 5.
MH13	63-Base	2.5	20	910	given the context of Step 5 this line should not be referring to the "subscriber"	"The subscriber activates the wallet using an activation factor." should read "The claimant activates the wallet using an activation factor."
MH14	63-Base	2.5	19-21	886-920	This part of the document deserves a separate section number	Add an additional section to contain this part of the document
MH15	63-Base	2.5	19-21	886-920	The verifier component appears in Fig.5 but is not mentioned in the text relating to Fig.5	please add a description of the role it plays and how an AAL is achieved in the context of the sequence described
MH16	63-Base	3	22	942	"e.g., an attacker who compromises or steals an authenticator" does not allow for the case when multiple authenticators are lost	would be improved by saying "e.g., an attacker who compromises or steals one or more authenticators"
MH17	63-Base	3	22	945	(e.g., compromising or replaying an assertion) could be improved by saying (e.g., compromising or replaying one or more assertions)	Suggest replacing (e.g., compromising or replaying an assertion) with (e.g., compromising or replaying one or more assertions)
MH18	63-Base	3	22	954	There is a dimension of risk that should be addad and that is the number of subjects that are likely to be affected by a compromise.	Suggest adding a paragraph about how the number of affected parties can affect the potential impact of a risk.
MH19	63-Base	3	23	968-969	"Federation: What is the impact of releasing subscriber attributes to the wrong online service or system?"	would suggest rewording and adding to say "Federation: What is the impact of releasing real subscriber attributes to the wrong online service or system or releasing incorrect or fake attributes to a legitimate Relying Party?"
MH20	63-Base	3.1	28	1120	gramatical issue with " "At a minimum, agencies SHALL document all impacted when conducting their impact assessments.""	"At a minimum, agencies SHALL document all impacted when conducting their impact assessments." would be improved by adding one word "At a minimum, agencies SHALL document all impacted parties when conducting their impact assessments."
MH21	63-Base	3.3.2.2	36	1375	"AAL2 provides high confidence that the claimant controls one or more authenticators..." is incorrect	"AAL2 provides high confidence that the claimant controls one or more authenticators..." should read "AAL2 provides high confidence that the claimant controls two or more authenticators..."
MH22	63-Base	3.3.2.2	36	1380	"AAL3 provides very high confidence that the claimant controls one or more authenticators" is incorrect	"AAL3 provides very high confidence that the claimant controls one or more authenticators" should read "AAL3 provides very high confidence that the claimant controls two or more authenticators"
MH23	63-Base	3.3.2.2	36	table 2	The table only mentions "multifactor authentication" in the row about AAL2 but according to 800-63B-4 p10 fig 1 "MF cryptographic" is permitted at AAL3 and AAL1 has all AAL2 and AAL3 permitted options. Also "Support multifactor authentication" is not really a control objective	Suggest re-wording this table to more closely describe control objectives and incorrect inplications relating to multi-factor
MH25	63-Base	3.3.2.3	36	1392-13	"FAL2 additionally requires that the trust agreement between the IdP and RP be established prior to the federation transaction,..." this could be interpreted as contrary to the multi-lateral federations described in part C where in reality the trust agreement can be between a party and the federation authority.	Find a way to express that the trust agreement may not be directly between IDP and RP
MH26	63A	Front Page			Ryan Galluzo appears twice on the list of authors	remove one of the Ryans
MH27	63A			24 & 27	Ryan Galluzo appears twice on the list of authors	remove one of the Ryans
MH28	63A	Author ORCID IDs		95 & 99	Ryan Galluzo appears twice on the list	remove one of the Ryans
MH29	63A	1.2	2	425	is there a clear definition or list of what "highly scalabale attacks" are?	Add definition of "highly scalable attacks"

MH30	63A	1.2	2	426	There should be a clear definition of what "synthetic identities" are. They could be readily confused with stage names, honorific names or other legitimate pseudonyms that are legal in some jurisdictions unless there is clarity about the definition.	Add a definition that provides clarity about the difference between synthetic identities and classes of legitimate "other" names
MH31	63A	2.1.1	7	544	"validated address" has not been used before and it is unclear to the reader what it is. Please define or refer	Add definition for "validated address" or refer to external definition
MH32	63A	2.2	9	624	It seems that a significant number of people might not have a Middle Name and it is is qualified with "if available" in the description. This suggests it is not really a "Core Attribute" that "SHOULD be collected by CSPs"	Suggest remove it from "Core Attributes" Section
MH33	63A	2.2	9	626	There will be a number of communities mainly involving foreign nationals where the individual do not have a "Government Identifier" as described. Asylum seekers being an example. It is also the case that one individual may have multiple Government Identifiers. There should be guidance for how to handle both of those cases.	Suggest adding guidance for how to handle a case where an applicant has no Government Identifier and for the case where an applicant has more then one Government Identifier
MH34	63A	2.4	10	645	A clearer more specific heading for this section would be "Identity Evidence Validation and Collection"	Suggest change section 2.4 heading to "Identity Evidence Validation and Collection"
MH35	63A	2.4	10	648	"accurate (the pertinent data is correct, current, and related to the applicant)," The requirement that it is "related to the applicant" is not validation, that is verification and that is covered in section 2.5	suggest remove "and related to the applicant"
MH36	63A	2.4.1	10	660	"The ability to provide confidence in the verification of the applicant presenting the evidence." This statement is about verification verification which is the topic of section 2.5 not 2.4	suggest removal of this requirement from section 2.4
MH37	63A	2.4.1.1	11	680	"digital security features that make it difficult to reproduce" - "difficult" is not quantifiable which is at odds with the statement at the top of section 2 that it is a normative section.	Suggest reword to make this a more quantifiable requirement
MH38	63A	2.4.1.2	11	702	"difficult" is not quantifiable which is at odds with the statement at the top of section 2 that it is a normative section. Suggest a more quantifiable requirement	Suggest reword to make this a more quantifiable requirement
MH39	63A	2.4.2.1	12	747	This section is about validation of evidence yet the wording includes "accuracy" and the phrase "The information on the evidence is accurate". This is not part of evidence validation. - It is also quite unclear how this might be done	Suggest removal of the word "accuracy" from line 741 and removal of the third bullet point "The information on the evidence is accurate."
MH40	63A	2.5.1	14	784-786	The statement that "The individual is able to demonstrate control of a piece of identity evidence" is not really the case unless a piece of evidence is a (from 3.1.8) " postal address, email address, or phone number, for the purposes of future communications.".	Suggest rewording to state something like "Confirmation code verification can be used to increase confidence that an individual has access to a postal address, email address, or phone number. This can support the verification of the relationship between an individual and a piece of evidence that has one of those attributes on it."
MH41	63A	3.1.2.1	18	914	It's not "the length of time a phone" that really gives tenure - it is the phone service subscription.	Modify "Evaluate the length of time a phone or other account has existed without substantial modifications or changes." to include the words service subscription ... "Evaluate the length of time a phone service subscription or other account has existed without substantial modifications or changes. "
MH42	63A	3.1.2.3	20	992	There way that section 3.1.2.3 does not directly address the situation where a ligitimate person who has simply been a victim of identity theft. This should be explicitly mentioned	Suggest Adding in some content to have an explicitly state that CSPs and RPs SHALL have a clearly documented recovery path for legitimate persons who are the victims of identity theft and that they should be supported in a way that minimises their time to innocence.
MH43	63A	3.1.10	26-27	1204	There are no defined constraints around the notifications arising from identity proofing such as any need for a time constraint to be applied or even whether the repudiation cannot be used after a given number of legitimate uses of a proofed identity	Suggest adding some wording about there being a defined period within which repudiation would be normally allowed or whether repudiation is a legitimate path to resolution after the proofed identity has been used a defined number of times (after that it might become a report of identity theft rather than a repudiation of a proofing)
MH44	63A	3.1.13.3	33	1415	"Applicant representatives are not agents of the CSP" - use consistent terminology - it should be "Applicant Reference"	Replace "Applicant representatives are not agents of the CSP" with "Applicant References are not agents of the CSP"
MH45	63A	4.1.9(1)	39	1615	There should not be an un-intended restriction of how the safeguarding may be done because of the use of the word "or"	"All devices SHALL be safeguarded from tampering through either observation by CSP representatives or through physical and digital tamper prevention features" should be slightly changed to "All devices SHALL be safeguarded from tampering through observation by CSP representatives and/or through physical and digital tamper prevention features"
MH46	63A	4.2.2	41	1668	two pieces of STRONG should be permissable as legitimate evidence at IAL too - currently the wording does not permit that option.	Suggest reword of line 1668 or addition of new line to cover this scenario
MH47	63A	4.2.5	41	1693	"Comparing the government identifier and core attributes" - The government identifier" is a "core attribute" so should not need to be mentioned explicitly here	Suggest removing "government identifier" so that "Comparing the government identifier and core attributes against an authoritative or credible source to determine accuracy" becomes "Comparing the core attributes against an authoritative or credible source to determine accuracy"
MH48	63A	4.2.5	41	1699	what happens in the scenario where validation of reference numbers is not possible?	Suggest addition of this case in this section
MH49	63A	4.3.5	46	1836	Is there any guidance on what should happen if the evidence attributes and the authoritative source attributes are not consistent, even by a small amount? - is given name "bob" and "bobby" consistent?	Offer guidance that covers what should happen when these attribute sources are inconsistent
MH50	63A	4.3.6	46	1842	Please clarify whether this is intended to be covering the end-user controlled wallet based case and if so it should be using the term activation rather than authentication in this case	If this is referring to the user controlled wallet case then suggest reword from "Confirming the applicant's ability to successfully authenticate to a physical device or application" to "Confirming the applicant's ability to successfully successfully use an activation factor with a physical device or application"
MH51	63A	7.4	59	2111	Specific mention that victims of ID theft are included in this requirement would be a valuable addition	Suggest adding in some content to have an explicitly state that CSPs SHALL have a clearly documented redress path for legitimate persons who are the victims of identity theft an dthat they should be supported in a way that minimises their time to innocence.
MH52	63A	8.3	67	2414	There is nothing here about addressing the usabiloty of unhappy paths	Suggest adding some content that mentions that the various entities involved should do usability design on failure scenarios as well as success scenarios
MH53	63A	A.1 Table 4	78	2728	In the phone account section it states "Confirm presence of user account with MNO." Does this section allow for all foreign MNOs	Clarify whether this is specific sets of MNOs and or what criteria an MNO has to meet in order to be deemed adequate to be considered FAIR.
MH54	63A	A.1 Table 4	78	2728	In the StudentID Card there is no indication that the existence of the institution should be checked.	Suggest adding some wording such as "Confirm that the issuing organisation is a legitimate academic institution"
MH55	63A	A.1 Table 4	79	2728	In the Corporate ID Card there is no indication that the existence of the organisation should be checked.	Suggest adding some wording such as "Confirm that the issuing organisation is a legitimate company"
MH56	63A	A.2 Table 5	80	2729	It could be clearer if the row about "Driver's License or State ID" more clearly stated that it is referring to a physical card	Suggest changing "Physical Driver's License or State ID"

MH60	63B	Appendix D: Glossa	107	3411-34	The definition of "phishing resistance" should be enhanced to add that that the verifier should be able to determine if an incorrect or replayed secret is being presented	Please enhance the wording to describe resistance to incorrect or replayed secrets
MH178	63B	Whole 800-63B document			There are only two references to "bound authenticators" in 800-63B-4. That seems like a sufficiently important aspect of FAL3 that a sections should be dedicated to it in 800-63B	Suggest adding a section dedicated to "Bound Authenticators" in 800-63B
MH179	63B	2.2.1	6	563-568	In this paragraph it specifically discusses a physical authenticator and states that it acts as “something you have”, however there are multiple real-world cases where bionetric characteristics are not presented to a device belonging to or held by the end-user - example being airport fingerprint scanners and face biometric scanners	Sugggest adding a section or paragraph with guidance on how biometric authentication hould be handled with static or kiosk style authenticators and how AAL2 might be achieved in that context
MH180	63B	2.4	9-Oct	631-676	In this section there are many references to the CSP (a role that does not directly perform authentication functions), yet this document is focussed on AAL so it seems likely that in the context the Verifier might be a more appropriate role to be referrimg to. That being said, authentication functions can also be part of the IDP function (as shown in Fig.4. of the base document) or performed by an RP in the case of "bound authenticators". On balance it is probaby best to use a different term of phrase such as "party performing authentication functions"	Suggest replacing "CSP" throughout this section with some other term as CSP is a role that does not directly perform authentication (verifier)
MH181	63B	Fig.1.	10		the "biometric + something you have" option described in sections 2.2.1 and 2.3.2 is not listed in this table	Suggest adding mention of this option to the table
MH182	63B	3.1.1.1	12	708-709	CSP is used (twice) here when it could be one of several roles that uses a "password authenticator"	Suggest replacing "CSP" with a broader term as it is not only CSPs that might use a "password authenticator"
MH183	63B	3.1.3.1.	20	911-912	The term "activation factor" has been used in part C - is this the same? If this is the case then use consistent terminology	Suggest rewording "(i.e., the device SHOULD require the presentation and verification of a PIN, passcode, or biometric characteristic to view" to say "(i.e., the device SHOULD require the presentation and verification of an activation factor, such as PIN, passcode, or biometric characteristic, to view"). If this is not intende to be considered an activation factor then it seems that the "device unlock" mechanism may need another form of secret described of at least further clarification "device avtivation factor"?.
MH184	63B	3.2.4	32	1324	"CSP" is used in this case when it could also be an IDP that requires an attestation	Suggest starting with "The CSP or IDP..."
MH185	63B	3.2.6	34	1394-13	In this case its may be that an IDP also needs secure communications with the verifiier	Suggest changing mentions of "CSP" in this section (and heading) with "CSP or IDP..."
MH186	63B	5.3	52	1992-20	This section would benefit from direct mention of shared signalling mechanisms that are mentioned in 800-63C-4 and referenced in 800-63A-4. A similar shared signalling mechanism would permit standardised signalling of authentication related events enabling the "continuous authentication" mentioned	Suggest adding guidance in a sub-section on shared signalling use within the context of authentication events.
MH57	63C	Note to Reviewers	ii	153	in other parts of the document set "user-controlled" was presented inside inverted commas and again in oter places the same component is called a "Subscriber-controlled wallet"	Suggest putting user-controlled inside inverted commas More generally suggest deciding whether "user-controlled" or "subscriber-controlled" (or some other term - see comment MH153) is the preferred term and use it consistently.
MH58	63C	2. Table 1	4	492	in the table row about Trust Agreement Establishment it states this is done "A priori". This term has a few dictionary definitions and it would be useful to clarify which one applies (see https://www.merriam-webster.com/dictionary/a%20priori). It is also unhelpful for a number of readers to use Latin when this could be expressed in clear English. Currently the assumption is that "formed or conceived beforehand" is the intended meaning of this.	Suggest using English and being clearer about what is meant
MH59	63C	2. Table 1	4	492	In the row about "Identifier and Key Establishment" it states that these should be "static". But this would seem to be a bad thing for security if that is an absolute statement. Key rotation is generally a good thing although it introduces other challenges. If it is not absolutely static then it is "dynamic" in some way and the requirements should be more clearly stated.	Suggest re-word this to be clearer about the intent behind this.
MH61	63C	2.3	5	538	This being a normative section "a variety of attacks" should be more explicit potentially by referring to a section of these guidelines or another document	Suggest adding a reference that defines what is meant by "a variety of attacks"
MH62	63C	2.3	6	542	editorial - the word "be" is missing	this line should read "At FAL2, the assertion SHALL be audience restricted to a single RP."
MH63	63C	2.3	6	543	Remove "a priori" as it is duplicative of "established prior to" and its removal improves readability	remove "a priori" from this line
MH64	63C	2.4	6	549-552	"FAL3 provides a very high level of protection for federation transactions, establishing very high confidence that the subscriber asserted by the IdP is the subscriber present in the authenticated session." This statement crosses the concerns of Federation, Identity Assurance and Authentication. It should be re-worded to simplify and focus on matters of federation only.	Suggest reword to "AL3 provides a very high level of protection for federation transactions, establishing very high confidence that the information communicated about IAL and AAL matches what was established by parties such as CSP and/or IDP"
MH65	63C	2.4	6	559-560	"static fashion" if taken in it's absolute sense precludes key rotation - similar to comment # MH59	Suggest re-word to express what is intended without precluding periodic key rotation
MH66	63C	2.4	6	560	This being a normative section "trusted mechanism" should be defined more explicitly.	Suggest adding a reference that defines what is meant by "trusted mechanism"
MH67	63C	2.5	7	606	The sentence "Similarly, an RP could restrict management functionality to only certain subscriber accounts which have been identity proofed at IAL2," should not be so restrictive as to be only "management functionality".	Suggest a reword to say ""Similarly, an RP could restrict higher risk functionality to only certain subscriber accounts which have been identity proofed at IAL2,""
MH68	63C	2.5	7	612	an "intended FAL" does not seem very practical as the FAL is necessarily a combination of factors that depend on the configuration of the various federation partners along the path of the end-to-end federation journey that the assertion or attribute bundle takes before delivery to the RP. Surely the RP needs to know the outcome of the FAL that arises from the federation journey not the FAL intended by the IdP.	Suggest deletion of "consequently, the IdP declares the IAL, AAL, and intended FAL for each federation transaction."
MH69	63C	2.5	8	613-616	This paragraph fails to mention the potential for a proxy federation layer to exist (section 3.2.3) and its potential impact on the resulting end-to-end FAL. It also seems possible that for some reason an RP cannot meet it's obligations or that a proxy federation component has not met the given FAL requirements. What should the RP do in this scenario? Decline service and delete the assertion or attribute bundle?	Suggest a reword that includes allowance for the issues described
MH70	63C	3	10	669	The sentence "The verification of the subscriber’s identity by the IdP and subsequent issuance of an assertion to the RP." could be generalised by changing one word	Suggest replacement of "The verification of the subscriber’s identity by the IdP and subsequent issuance of an assertion to the RP." with "The verification of the subscriber’s identity by the IdP and subsequent communication of an assertion to the RP."

MH71	63C	3	10	674	small improvement to sentence	Suggest replace "The exact order in which that happens, and which parties are involved in which steps, can vary depending on deployment models and other factors." with "The exact order in which that happens, and which parties are involved in which steps, can vary depending on deployment models, protocol choices, and other factors."
MH72	63C	3.2.1	11	701	The responsibilities of establishing a trust agreement and representing it through a federation authority can (and quite often) are delivered by different entities. This paragraph should be reviewed and reworded to allow for a clearer split between the two functions which may be delivered by one or two entities. The first sentence can be subtly modified to reflect this.	Suggest reword from "The trust agreement (see Sec. 3.4) can be managed through a dedicated party, known as a federation authority." to "The trust agreement (see Sec. 3.4) can be represented through a dedicated party, known as a federation authority."
MH74	63C	3.2.1	11	701	There is no definition of "federation authority" and without that this section is unclear	Please add a definition of a "federation authority"
MH75	63C	3.2.1	11	704	associated with MH72 a subtle reword is suggested	Suggest reword from "This management provides a transitive trust to other parties in the agreement." to "This federation authority provides a transitive trust between parties to the agreement."
MH76	63C	3.2.1	11	705	The trust agreement is between IDPs and RPs in this case not necessarily "with a federation authority". This should be improved to clarify the different roles.	Suggest reword of "For example, an RP can enter a trust agreement with a federation authority and decide that any IdP approved by that federation authority is suitable for its purposes." to "For example, an RP can sign up to a trust agreement represented by a federation authority and decide that any IdP approved by that federation authority is suitable for its purposes."
MH77	63C	3.3.1.1	15	854	It states that "The proxy SHALL NOT disclose the mapping between the PPI and any other identifiers to a third party ". This precludes cases where there is a legal requirement to share that information to law enforcement authorities. Is that the intent?	Suggest adding a clause that allows for "... unless required by law" scenarios
MH78	63C	3.4	18	932	It states that "As such, the terms of the trust agreement need to be made available to subscribers in clear and understandable language.". There will be a range of terms in the trust agreement that are probably not relevant to the subscriber, for example, commercial terms, protocols used, liability concerns, service levels. Suggest a slight reword to clarify this.	Suggest change "As such, the terms of the trust agreement need to be made available to subscribers in clear and understandable language." to "As such, the terms of the trust agreement that concern the subscriber need to be made available to subscribers in clear and understandable language."
MH79	63C	3.4.2	19	951	First sentence could be improved to clarify the roles of trust agreement and federation authority	Suggest change from "In a multilateral trust agreement, the federated parties look to a federation authority to assist in establishing the trust agreement between parties." to "In a multilateral trust agreement, the federated parties often look to a federation authority to represent the trust agreement between parties by making operational data about the trust agreement and the parties that participate in it available in a secure fashion."
MH80	63C	3.4.2	19	957	Vetting of parties can be and often is done by an entity other than the federation authority	Suggest adding a sentence saying "Vetting of parties can be and often is done by an entity other than the federation authority" and modify Fig2 to show a capability that may be separate from the federation authority
MH81	63C	3.4.2	20	970	How are the profiles of federation protocols "approved"? This being a normative section "approved" should be defined more explicitly. If this is not done then the normative guidance will be very difficult to test in implementations.	Please provide guidance or specific references about how this approval is done, which parties are involved and what the process is
MH82	63C	3.4.2	20	971-975	This being a normative section it should be defined more explicitly. This paragraph does not provide any measurable requirements.	Suggest tagging this paragraph as a non-normative implementers note
MH83	63C	3.4.2	20	978	This line is the only place in the full set of guidance documents that referrs to sharing "between CSPs". This scenario needs further elaboration generally.	Please provide further guidance on sharing information between CSPs, in what circumstances should this happen and what requirements are there to control this sharing?
MH84	63C	3.4.2	20	979	It states that "the federation authority can define the policies that apply for the transfer of this information.". However, it is not the role of the federation authority to define policies. This should be in the trust agreement	Suggest replace "the federation authority can define the policies that apply for the transfer of this information." with "the trust agreement SHALL define the policies that apply for the transfer of this information."
MH85	63C	3.4.2	20	985	The use of federation authority could be improved in this sentence to avoid conflation of federation authority and trust agreement.	Suggest changing "A federation authority MAY incorporate other multilateral trust agreements managed by other federation authorities in its trust agreement," to "A trust agreement MAY establish trust with other multilateral trust agreements managed by other entities,"
MH86	63C	3.4.2	20	987-989	The wording here could be improved to avoid convlation of trust agreement with federation authority	Suggest changing "In order to facilitate connection between IdP1 and RP2, a new federation authority FA3 can provide a multilateral agreement that accepts IdPs from FA1 and RPs from FA2. " to "In order to facilitate connection between IdP1 and RP2, a new federation authority FA3 can provide operational data that demonstrated participation tin the interfederation and enables IdPs from FA1 and RPs from FA2 to connect."
MH87	63C	3.4.2	20	984-991	This paragraph allows significant scalability of federations but will be difficult to deliver when there is a requirement for "static" identifier and key establishment. This will effectively preclude interferderation at FAL3	Confirm whether interfederation at FAL 3 is permitted and mention how interfederation might achieve static identifier and key exchange as it scales.
MH88	63C	3.5.1	22	1055	How does "any cryptographic keys and identifiers SHALL be defined by the trust agreement and SHALL be executed using an authenticated protected channel, as in the initial cryptographic key establishment" meet the requirement for "requirement for static identifier and key establishment." described earlier in this document?	Please clarify how cryptographic key rotation can be performed when there is a requirement for static identifier and key establishment
MH89	63C	3.6	23	1096	It states that "A subscriber's attributes SHALL NOT be transmitted for any other purposes, even when parties are allowlisted". Is the intention to preclude this even when the law requires it or for IDPs and RPs to be required to break the terms of the digital identity guidelines when there are legal requirements?	Suggest adding a clause that allows for "... unless required by law" scenarios
MH90	63C	3.7	24	1111	It states that "An active RP subscriber account is bound to one or more federated identifiers from the RP's trusted IdPs." that is only the case when federation is used and so this statement should be qualified.	Suggest modify this sentence to say "When an RP uses federation an active RP subscriber account is bound to one or more federated identifiers from the RP's trusted IdPs."
MH91	63C	3.7	24	1117	It states that " The RP subscriber account SHALL be bound to at least one federated identifier" - this depends on the RP using Federation so this should be a qualified statement	Suggest modify this clause to say " When using Federation to provide attributes about the subscriber the RP subscriber account SHALL be bound to at least one federated identifier"
MH92	63C	3.7	24	1123-11	It is worth adding that there may be a disabled state that exists independant of termination where access is removed but the data is preserved for a period for records retention, or perhaps investigarion reasons.	Add passage to express the possibility of a disabled status existing
MH93	63C	3.7.1	24	1136	The word "manage" seems incorrect here as those federated accounts are not really managed from the RP.	Suggest replace the work "manage" with either "link" or "connect"
MH94	63C	3.7.1	25	1145-11	It states that "In such cases, the RP subscriber account SHOULD be terminated and information associated with the account in accordance with Sec. 3.10.3." but this precludes retention of records that may be required for various purposes. There is also a missing word after "information"	Suggest change this sentence to say "In such cases, the RP subscriber account SHOULD be disabled or terminated and any information associated with the account should be handled in accordance with Sec. 3.10.3." Also will be suggesting a re-word of 3.10.3 to allow for subscriber account to be diabled

MH95	63C	3.9	27	1218-12	It states that "Federation involves the transfer of personal attributes from a third party that is not otherwise involved in a transaction — the IdP". However the IDP is not necessarily a 3rd party. There are often implementations where the IDP and RP are operated by the same entity and this should not be precluded	Clarify the wording such that RP and IDP operated by the same entity is not precluded
MH96	63C	3.10.2	30	1352	Please consistent terms, in this paragraph the term "full attribute values" is used but in section 3.11 it would appear to use the term "attribute values"	Suggest removing the word "full"
MH97	63C	3.10.3	30	1356	What about cases where data needs to be retained either to comply with record retention policies, regulatory requirements or in the case of an investigation?	This section should include allowance for a "disabled" subscriber account status
MH98	63C	3.10.3	31	1367	In this paragraph it states "unless required by legal action or policy." This is open to any entity stating a "policy" and is therefore a very weak requirement.	Suggest a much more quantifiable requirement be written to express which entity may define such policies. Perhaps the RP only?
MH99	63C	3.11	31	1373	An improvement to the wording for consistency and clarity is desirable	Suggest change "(presented directly by the IdP)" to "(presented as an assertion directly by the IdP)"
MH100	63C	3.11	31	1379	The wording and use of defined term "Assertion" does not alllow for the user-controlled wallet case as the definition of "Assertion" is "A statement from an IdP to an RP"	Suggest change from "Attributes SHALL be either presented in the assertion" to "Attributes SHALL be either presented either directly by the IDP or by a User-Controlled Wallet"
MH101	63C	3.11.1	31-32	1368-13	The features that define what is an "attribute bundle" are not clear and probably deserve a clear definition and there is a great deal of similarity with an assertion which leaves the reader uncertain. Defining by example is not ideal. Through inference it is understood to be a set of attributes that are somehow combined within a signed wrapper and that can only be created by a CSP (and perhaps does not contain information about authentication?).	Suggest adding a definition for an "attribute bundle" and describing its unique features.
MH102	63C	3.11.1	32	1406	It currently states "such as by verifying that the public key used to sign the assertion is included in the signature of the attribute bundle." This would be improved with a slight edit.	Suggest changing from "such as by verifying that the public key used to sign the assertion is included in the signature of the attribute bundle." to "such as by verifying that the CSP identifier and public key used to sign the assertion is included in the signature of the attribute bundle."
MH103	63C	3.11.3	32	1423	This section contains no reference to push based models for creating subscriber accounts at the RP as can be done through th euse of SCIM. It would be valuable to add a section on this topic as it seems likely that agencies may wish that option.	Add a section to describe "push based" or pre-provisioning (as described in section 4.6.3) subscriber provisioning
MH104	63C	3.11.3	32	1424	This being a normative section "profile information" should be defined more explicitly.	Suggest adding a reference that defines what is meant by "profile information".
NS1	63C	3.11.3	33	1448	Current text states: "Access to the identity API SHOULD be limited to the duration of the federation transaction plus time necessary for synchronization of attributes, ". From the explanation in 4.6.4, it seems to be just intending the attribute synchronization at login. However, Identity API is useful when continuous access evaluation is considered: when the security event notification comes in, the party may want to pull the attribuve value from the Identity API to make a fresh access decision. This means that limiting the access to the identity API to the duration of the federation transaction plus time necessary for synchronization of attributes is too limiting.	Suggest changing to: Access to the identity API SHOULD be limited to the duration of the federation transaction plus time necessary for achieving the purpose of use of such API.
MH105	63C	3.11.3.1	34	1468	This section could make regerence to a technique described in a relatively new specification called "OpenID Attachments" under the OpenIF Foundation eKYC & IDA Working Group whereby an "external attachment" is reffered to and a hash of the content that should be provided is included in the referring assertion.	Suggest describiny the potential for strongly associate statements in an assertion with content available from "External API" through the use of a digest of the target being provided in the assertion from the IDP.
MH106	63C	3.12.3	35	1519	It states that "Subject identifiers are meaningless outside of their target systems," - that is not the case. They can be exploited for tracking purposes and potentially used as part of blended attacks.	Suggest a reword of this paragraph to remove the false assertion that "Subject identifiers are meaningless outside of their target systems,". It may be appropriate to state that subject identiofiers may be a lower risk attribute that SSN etc.
MH107	63C	3.14	37	1575-15	This paragraph seems to be fairly unrelated to holder-of-key assertions and would be better placed in section 4.6.3. It also uses the words "unique pairwize identifier" which I think really means an "ephemeral identifier"	Suggest move this paragraph int section 4.6.3 and change "unique pairwize identifier" to "ephemeral identifier"
MH108	63C	3.14	37	1581	It states that "Since the authenticators used in holder-of-key assertions are presented to multiple parties" - they are not necessarily "presented to multiple parties"	Suggest reword from "Since the authenticators used in holder-of-key assertions are presented to multiple parties" to "Since the authenticators used in holder-of-key assertions might be presented to multiple parties"
MH109	63C	3.15	38	1594	It states that "All bound authenticators SHALL be phishing resistant." however the definition of "phishing resistant" describes features of an authentication protocol rather than features of an authenticator	Suggest reword from "All bound authenticators SHALL be phishing resistant." to "All bound authenticators SHALL use phishing resistant mechanisms."
MH110	63C	3.15	38	1596-15	It states that "The RP SHALL accept authentication from a bound authenticator only in the context of processing an FAL3 assertion for a federation transaction." and the way this is worded makes an implementation non-compliant if they were to use a bound authenticator in the context of an FAL2 federation transaction. This seems like an un-intended restricton of the RP implementation.	Suggest a reword from "The RP SHALL accept authentication from a bound authenticator only in the context of processing an FAL3 assertion for a federation transaction." to say "The RP SHALL require authentication from a bound authenticator when processing an FAL3 assertion for a federation transaction."
MH111	63C	3.15	38-39	1609-16	It states that an RP "SHOULD notify the IdP using a shared signaling system (see Sec. 4.8), if any of the following events occur". That wording implies that there will only be one IDP however there should be allowance made for multiple IDPs being linked to a single RP subscriber account as described in section 3.7.1. In turm this may result in additional privacy concerns as multiple IDPs might get visability of subscriber activities at an RP.	Consider and provide clearer guidance on what the requirements are relating to bound authenticator signalling in the context of account linking and how an RP should balance the signalling requirement with subscriber privacy requirements
MH112	63C	3.15.2	40	1659	It states that "the binding ceremony makes use of the existing ability to reach FAL3." this clause implies a singular path to FAL 3 but there may be more than one through the use of account linking.	Suggest changing "the binding ceremony makes use of the existing ability to reach FAL3." to "the binding ceremony makes use of any existing ability to reach FAL3."
MH113	63C	3.15.2	40	1663-16	This paragraph covers removal of a bound authenticator but does not cover the case wheer it is the only bound authenticator and it does not seem to be covered elsewhere	Suggest add guidance on how the removal of the only bound authenticator should be handled
MH114	63C	3.15.2	40	1647	This paragraph starts with "This option" and some readers may be left wondering "which option?"	Suggest changing "This option..." to say "The option of removing a bound authenticator..."
MH115	63C	3-May	#####		There appears to be no mention of a hybrid model where an entity can act as both a CSP that delivers bundles to subscriber-controlled wallets and has a general purpose IDP as an alternative. This model might turn out to be a useful and powerful combination and may deserve some coverage	Suggest adding a section that describes a hybrid deployment for General purpose IDP and subscriber-controlled wallet
MH116	63C	4.2	44	1731	It would be useful to add an element to "Fig. 6. Federation Overview" that indicates Discovery and redistration between the IDP & RP	Suggest adding an interaction to the diagram that shows discovery and registration

MH117	63C	4.2(3)	45	1743-17	The sentence "This stage can occur before any subscriber tries to access the RP or as a response to a subscriber's attempt to use an IdP at an RP." is not the case in the context of FAL 3	Suggest rewording from "This stage can occur before any subscriber tries to access the RP or as a response to a subscriber's attempt to use an IdP at an RP." to "This stage can occur before any subscriber tries to access the RP, at any FAL, or as a response to a subscriber's attempt to use an IdP at an RP at FAL1 or FAL 2."
MH118	63C	4.2(4)	45	1746-17	The passage "the set of attributes that is to be passed to the RP is selected from a subset of what the RP has requested, what is allowed by the trust agreement, and what is permitted by the authorized party. If necessary, the authorized party is prompted at runtime to approve the release of attributes." realistically takes place in step 6 of the journey being described.	Suggest taking the passage in step 4 "the set of attributes that is to be passed to the RP is selected from a subset of what the RP has requested, what is allowed by the trust agreement, and what is permitted by the authorized party. If necessary, the authorized party is prompted at runtime to approve the release of attributes." and move it to step 6
MH119	63C	4.2	45	1761	It states that "In all transactions, the parties involved enter into a trust agreement, " This implies that the act of "entering into a trust agreement" is done every time there is a transaction.	Suggest a reword of "In all transactions, the parties involved enter into a trust agreement, " to "In all federations, the parties involved enter into a trust agreement, "
MH120	63C	4.2	45	1764	The text "The list of available subscriber identity attributes is established in this step" and its context implies that the the "available subscriber attributes" are agreed as p[art of the trust agreement whereas there may be optional attributes that not all subscriber accounts maintain. Suggest a subtle reword.	Suggest changing "The list of available subscriber identity attributes is established in this step" to "The list of supported subscriber identity attributes is established in this step"
MH121	63C	4.3.1	46	1790	punctuation needed	Suggest modifying "What if any identity APIs are made available..." to "What, if any, identity APIs are made available..."
MH122	63C	4.3.1	46	1795	An RP might have several use cases and thus several different sets of subscriber attributes they need at run-time so stating "The set of subscriber attributes that the RP will request" is too definitive	Suggest modify "The set of subscriber attributes that the RP will request" to say "The set of subscriber attributes that the RP may request"
MH123	63C	4.3.1	46	1797	In the case that an RP has several use cases there might be several purposes that a specific attribute is needed for so writing "The purpose for each attribute requested by the RP" is too definitive	Suggest modify "The purpose for each attribute requested by the RP" to ""The purposes that the RP may have for each attribute requested"
MH124	63C	4.3	46-48	1773-18	There is no mention of multilateral trust agreements in this section - It would seem that there should be some specific requirements or guidance for multi-lateral federation in the context of General Purpose IDPs	Suggest add some guidance for multilateral federation in the context of General Purpose IDPs
MH125	63C	4.3.1	47	1807-18	It states that "The terms of the trust agreement SHALL be made available to subscribers upon request to the IdP or RP." but it seems likely that there will be terms in that agreement that have no relevance to the subscriber and may in fact be commercially sensitive. Things like how fraud is handled, the commercial arrangements	Suggest a reword from "The terms of the trust agreement that are relevant to subscribers SHALL be made available to subscribers upon request to the IdP or RP."
MH126	63C	4.3.1	47	1821	The clause "Whether bound authenticators are supplied by the RP or by the subscriber" suggests that those options are exclusive whereas it is perfectly plausible for an RP to offer both options	Suggest reword of "Whether bound authenticators are supplied by the RP or by the subscriber" to say "Whether bound authenticators are supplied by the RP and/or by the subscriber"
MH127	63C	4.3.1	47	1828-18	It states that "The IdP and RP SHALL exchange only the minimum data necessary to achieve the function of the system." - This is a very general statement about data minimisation yet is in a section about Trust Agreement establishment. As a result it seems out of place	Suggest removal of "The IdP and RP SHALL exchange only the minimum data necessary to achieve the function of the system." either completely or to another part of the document that is focussed on data minimisation if it is of use there.
MH128	63C	4.4	48	1869-18	In this passage "If these are retrieved over a network connection, request and retrieval SHALL be made over a secure protected channel from a location associated with the IdP's identifier by the trust agreement. In many federation protocols, this is accomplished by the RP fetching the public keys and configuration data from a URL known to be controlled by the IdP or offered on the IdP's behalf. " it describes requirements and describes how keys may be exchanged. It would be very useful if there were a clear statement that this does not count as a static registration process as required in FAL3 (if that is the case).	Suggest an explicit statement that fetching public keys over the network is or is not permissable as part of a static registration process as required at FAL3
MH129	63C	4.4	49	1880	It states that "In all of these requirements, the IdP MAY use a trusted third party to facilitate its discovery and registration processes". Please clarify that an independant entity providing a federation authority is an example of this.	Suggest a reword from "In all of these requirements, the IdP MAY use a trusted third party to facilitate its discovery and registration processes" to "In all of these requirements, the IdP MAY use a trusted third party acting as a federation authority to facilitate its discovery and registration processes"
MH130	63C	4.4.1	49	1887-18	In this section it does not state whether this is describing the "static registration process" described in section 2.4 and required for FAL 3. If this is the case then it should be stated clearly.	Suggest adding a statement that this would meet the requirement described in section 2.4 for a "static registration process" - if that is what is intended. If not then clarify which of the sections in 4.4 can meet that requirement
MH131	63C	4.4.2	49-50	1900-19	The decision to require a "static registration process" at FAL3 is difficult to understand from a risk mitigation process perspective. In te real world these things cannot be static due to the need to rotate secrets or keys on a regular basis. The net result of this split between static and dynamic is that it becomes a split between human process managed or an automated process. Both of these options have risks and either could potentially have sufficient controls and countermeasures put in place. It might even be harder to implement stronger controls and countermeasures in the human process managed case.	Suggest a look again at the discovery and registration requirements and the prohibition of "dynamic registration" at FAL3 as it will necessarily be dynamic in all cases and it should be possible to construct strong controls around "dynamic registration", that is essentially what has been done with many x.509 PKI instances.
MH132	63C	4.6	50	1935-19	It states that "a runtime decision, which allows the authorized party to decide if the transaction can proceed and under what precise terms. Note that a runtime decision can be stored and applied to future transactions." This and the other options above do not seem to allow the IDP to make a risk based fraud decision. This should be an allowed scenario and should be explicitly stated.	Suggest adding a bullet to this section that allows the IDP to make risk based decisions at run-time that are intended to mitigate transactions that are determined to be likely fraud.
MH133	63C	4.6.1.1	51	1950	It states that "IdPs MAY establish allowlists of RPs authorized to receive authentication and attributes from the IdP" but this may be contrary to the statement on line 1929 that "The decision of whether a federation transaction proceeds SHALL be determined by the authorized party stipulated by the trust agreement. "	Suggest modification to either section to make this consistent and provide clear guidance
MH134	63C	4.6.1.2	51	1973	Same comment as MH133 but applied to this line	Same suggestion as MH133
MH135	63C	4.6.1.3	52	1984-20	This section does not allow for risk based decions by the IDP when a transaction is determined to be potential or actual fraud. This scenario should be allowed and should have specific guidance provided	Suggest addingcontent to this section that provides guidance on how the IDP can make risk based decisions at run-time that are intended to mitigate transactions that are determined to be sufficiently suspicious or actual fraud.
MH136	63C	4.6.2.3	53	2034	This sentence "Every IdP that is in a trust agreement with an RP but not on an allowlist with that RP SHALL be governed by a default policy" does not allow for the multi-lateral trust agreement. Please re-word	Suggest changing "Every IdP that is in a trust agreement with an RP but not on an allowlist with that RP SHALL be governed by a default policy" to say "Every IdP that is in a trust agreement with an RP (whether Bilateral or Multilateral or via an interfederation) but not on an allowlist with that RP SHALL be governed by a default policy"

MH137	63C	4.6.3	54	2057-20	It states that "An RP subscriber account is created automatically the first time the RP receives an assertion with an unknown federated identifier from an IdP." and as a result it is not possible to do account linking as there is a requirement that "An RP subscriber account is created"	Suggest that some additional wording is needed to allow for the account linking option. Maybe change "An RP subscriber account is created automatically the first time the RP receives an assertion with an unknown federated identifier from an IdP." to say "An RP subscriber account is created or linked automatically the first time the RP receives an assertion with an unknown federated identifier from an IdP."
MH138	63C	4.6.3	54	2067-20	Similar comment to MH137 except appplied to the following sentence... "An RP subscriber account is created by the IdP pushing the attributes to the RP or the RP pulling attributes from the IdP. " In this case it would seem harder to link accounts and the intent of the guidance is less clear so please clarify and add suitable wording that either allows for account linking or states that it is not possible in this scenario.	Suggest some rewording to address whether account linking is possible in this case and if so provide guidance
MH139	63C	4.6.4	56	2114-21	It states that "The IdP SHOULD signal downstream RPs when the attributes of a subscriber account available to the RP have been updated, and the RP MAY respond to this signal by updating the attributes in the RP subscriber account. " This description does not cover how the RP gets those attributes to update	Suggest a slight reword from "The IdP SHOULD signal downstream RPs when the attributes of a subscriber account available to the RP have been updated, and the RP MAY respond to this signal by updating the attributes in the RP subscriber account. " to say "The IdP SHOULD signal downstream RPs when the attributes of a subscriber account available to the RP have been updated, and the RP MAY respond to this signal by requesting the updated attributes and/or updating the attributes in the RP subscriber account. "
MH140	63C	4.6.4	56-57	2125-21	It states that "The IdP SHOULD signal downstream RPs when a subscriber account is terminated, or when the subscriber account's access to an RP is revoked. ...". This has the implicit assumption that RPs will always be integrated via a shared signalling mechanism. Also, some shared signalling mechansms allow for the RP to register for only events they wish to receive so that ais a second layer of optionality in some implementations that might be permitted - the guidance is not clear on this.	Suggest clarification in the document somewhere when shard signalling is required or optional and adjust wording to reflect the possibilities that arise from any optionality that is permitted.
MH141	63C	4.6.5	57-58	2135-21	This section does not provide any guidance on whether an RP or IDP involved in provisioning are required to or may notify the subscriber. This would seem sensible and would be good to add guidance about	Suggest add guidance about notification of subscribers when using API based provisioning. Whether it is required or optional, and where the responsibility lies (IDP or RP). RP
MH142	63C	4.6.5	58	2168-21	It states that "When a provisioning API is in use, the IdP SHALL signal to the RP when a subscriber account has been terminated. " but there are other events that might be useful to communicate such as "disabled"	Suggest broading the guidance here to allow for "signalling of agreed IDP subscriber account state changes described in the trust agreement occur"
MH143	63C	4.6.6	58	2189	It states that "These attributes SHALL be used solely for the stated purposes of the RP's functionality and SHALL NOT have any secondary use, including communication of said attributes to other parties.". Is the intention to preclude any other purposes even when the law requires it or for IDPs and RPs to be required to break the terms of the digital identity guidelines when there are legal requirements?	Suggest adding a clause that allows for "... unless required by law" scenarios
MH144	63C	5	69-77		The section on subscriber-controlled wallets only covers the case where the wallet is provisoined by the CSP. The cases where a wallet is used that is not provisioned by the CSP is not mentioned at all in this major section.	Suggest adding guidance on what is required when the CSP is not involved in provisioning of the wallet.
TS1	63C	4.8.	61	2283	In order to protect the digital wellbeing of subscriber from cybersecurity threat, it is vital that federated parties continuously monitor the status of subscribers' accounts and the session during the use of that account in real time throughout the duration of the subscribers lifetime. If such security event occurs, then a party should immediately send security signal to other party for that party to mitigate the breach into the account of subscriber by revoking the session and temporarily disabling the account to go into remediation process. Without this shared signal mechanism to share these information's, it is not possible for RP nor IdP to act to protect their subscriber. To enable this kind of mechanism, IdP and RP should, both, continuously monitor the subscribers and its accounts' digital wellbeing, place a secure communication mechanism between the two that is connected continuous and signals sent at real time with enough information for these parties to mitigate and remediate the security breach or potential breach. OpenID Foundations Shared Signal Framework is an identity industrywide open technical standard which enables this mechanism. This framework defines how to establish Webhook based communication mechanisms that is authorized using industry standard OAuth 2.0 protocol. Webhook mechanism enables both Push and Polling messages system to send Security Event Token that can be sent in encrypted machine-readable standardized format defined by IETF RFC 8417. In this section, in order for the parties to share security signal, these following points needed to be pointed out first: 1. Two parties SHALL monitor the wellbeing of subscribers, continuously, from cybersecurity breach or potential of breach. 2. Two parties established authorized continuous communication line that machine readable signals can be sent encrypted. 3. Once either party receive such signal, they act immediately to mitigate and remediate to secure subscribers' digital wellbeing.	In order to protect the digital wellbeing of subscriber from cybersecurity threat, it is vital that federated parties such as IdP and RP, continuously monitor the status of subscribers accounts and the session during the use of that account in real time throughout the duration of the subscribers lifetime. If such security event occurs, then a party SHALL immediately send security signal to other party in order for that party to mitigate the breach into the account of subscriber by revoking the session and temporarily disabling the account to go into remediation process. To enable these process:- 1. Two parties SHALL monitor the wellbeing of subscribers, continuously, from cybersecurity breach or potential of breach. 2. Two parties SHALL establish authorized continuous communication line that can transmit machine readable signals to be sent encrypted. 3. Once either party receive such signal, they SHOULD act immediately to mitigate and remediate to secure subscribers' digital wellbeing.
TS2	63C	4.8.	61	2286	These security signals involving subscribers are utmost important and involves privacy and data protection. Thus in the Trust agreement between the parties, there should be a clause regarding exactly how these signals are used by the receiving party and what acts they cannot do with these information. In previous instance at SSF WG between major companies, when implementing SSF, they could not agree on the use of these signals because of privacy concerns. Specifically, they did not want these signals to be used for marketing and financial scoring purpose. By defining how these signals can be used at NIST level, it will be easier for parties to implement shared signal knowing that wrongful use of these signal outside of Trust agreement will be a serious breach of the guideline and also their Trust agreement.	The use of shared signaling SHALL be only for the purpose of mitigation and remediation of cybersecurity situation and SHALL be subject to privacy policy under the trust agreement.

TS3	63C	4.8	62	2290	CSRB Review of the Summer 2023 MEO Intrusion report Final 508C recommends in 2.1.3 that auditable logs of events should be standardized and that records maintained at least 6 months. Record of shared signals should follow the same six months or more and also set a standard format and data contents defined.	Any use of shared signaling SHALL be recorded as log data file and documented and made available to the authorized party stipulated by the trust agreement for the purpose of analysis and audit of these security incidents. This shared signal log data documentation SHALL include the events under which a signal is sent, the information included in such a signal (including any 61 NIST SP 800-63C-4 2pd August 2024 Digital Identity Guidelines Federation and Assertions 2293 attribute information), and any additional parameters sent with the signal. These documents SHALL be encrypted and kept for duration of more than 6 months from the date of the event.
TS4	63C	4.8	62	2292	It is necessary to define the need to have clear operational guideline and policies between the two parties, described in the trust agreement and system build accordingly. Thus this document should make sure that these operational policies are created and documented in such manner that programmer can write code that will comply with this guideline.	Prior to running a shared signal system, two parties SHALL create a clear operational policies for the use of signals and actions to be taken. The operational policies SHALL be part of the trust agreement. These policies SHALL be:- 1. At what kind of event or situation, each of these signals should be sent. 2. What kind of mitigation and remediation action should be taken when receiving such signal. 3. What kind of attributes should be included in each of these signals to make it clear and effective to take action in 2.
TS5	63C	4.8	62	2295-23	In order to build shared signal system, not only do you need incident reporting but also have clear policy of how to mitigate and how to remediate. There are three kinds of signals that will be useful and necessary to protect subscribers. These are A) account status B) Incident report, and 3) Mitigation and remediation. See OpenID F. Shared Signal Framework CAEP and RISC protcols.	mitigation and remediation of account takeover. These are A) account status B) Incident report, and 3) Mitigation and remediation. A. Status of Account signals 1. Status of the account 1.1 Account is deleted 1.2 Account does not exists 1.3 Account is dormant 1.4. Account is held in custody of guardian, IT admin, etc 2. Changes in Status of Accounts 2.1 Credential Change 2.2 Assurance Level Change (including IAL, AAL, FAL) 2.3 Device complaint Change 2.4 Identifier Change 2.5 Addition and removal of Bounded Authentication Incident report signals In a cybersecurity incident involving the subscriber, following signals are to be exchanged 1. Session Revoked 2. Account compromised or suspected of being compromised 3. Credential Compromised or suspected credential compromise 4. Device compromise or suspected device compromise 5. Communication line compromise or suspected Mitigation and Remediation action signals 1. Session Revocation Request 2. Account disable or suspension request
MH145	63C	4.8	62	2296-23	Other signals might be appropriate too and might be established as part of the trust framework	Suggest adding the following bullets to the list: - Authenticators have been updated - Account has been disabled - Core attributes have changed - Any additional events defined in the trust framework
MH146	63C	4.8	62	2300	It states "The possible range of IAL, AAL, or FAL for the account has changed." However AAL is an attribute derived from the authentication event and the FAL is derived from characteristics of the protocol implementations along the presentation path; so neither of these AAL or FAL are directly related to the account.	Suggest removal of AAL & FAL from "The possible range of IAL, AAL, or FAL for the account has changed."
MH147	63C	4.8	62	2305-23	Other signals might be appropriate too and might be established as part of the trust framework	Suggest adding the following bullets to the list: - Any additional events defined in the trust framework Also suggest a slight reword of 2nd bullet from "The account is suspected of being compromised." to The account is suspected of being, or has been confirmed as, compromised.
MH148	63C	4.9	62	2316-23	It states that "An assertion is a packaged set of attribute values or derived attribute values about or associated with an authenticated subscriber that is passed from the IdP to the RP in a federated identity system." This is a definition of an assertion that is different from the assertion definition in the glossary. This one is better!	Suggest taking this sentence and re-use it as the definition of "Assertion" in the Glossary
MH149	63C	4.9	63	2354	Essentially the same comment is MH68 - Intended FAL is not really very useful	Suggest deletion of "The IdP's intended FAL of the federation process represented by the assertion."
MH150	63C	4.9	64	2365	It states that the assertion may include "Additional details about the authentication event, such as the class of authenticator used". This implies a singular authenticator and this would be improved by using the plural or re-wording further	Suggest change "Additional details about the authentication event, such as the class of authenticator used" to say "Additional details about the authentication event, such as the class of authenticators used"
MH151	63C	4.9	64	2390-23	It states that "This window needs to be large enough to allow the RP to process the assertion and create a local application session for the subscriber, but should not be longer than necessary for such establishment.". This requirement does not allow for any material clock drift that can and does occur in real implementations	Suggest add wording to say that "This window needs to be large enough to allow the RP to process the assertion and create a local application session for the subscriber and tolerate a small amount of clock drift between IDP and RP, but should not be longer than necessary for such establishment."
MH152	63C	4.11.2	67	2476-24	It states that "As a consequence, it is recommended to not use front-channel presentation when other mechanisms are available" this should be reworded to me much more direct	Suggest reword to say "As a consequence, front-channel presentation SHALL NOT be used when other mechanisms are available"

MH153	63C	5	69	2494-24	Heading "Subscriber-controlled Wallets" and paragraph text "When the IdP runs on a device controlled by the subscriber, whether as a digital wallet or as a self-issued identity provider, " - In reality subscriber control over a device is not an absolute fact and is a significant over-simplification to imply that the digital-wallet or other software is synonymous with the device. There are usually multiple actors who exert some form of control over the behaviour of a device (network operator, hardware manufacturer, OS provider, Enterprise MDM application, and app provider at least) and the average user has no way of telling what the device or the various layers of software are going to do on their behalf. They simply have the outcomes they want delivered to them most of the time.	Suggest coming up with a different term that does not imply complete control by the subscriber and using that consistently throughout the document in place of "subscriber-controlled" and "user-controlled" Suggest a reword to avoid over-simplifying the reality of subscriber/user control in a multi-layered technical context. Perhaps change "When the IdP runs on a device controlled by the subscriber" to say "When the IdP runs on a device used by the subscriber"
MH154		5	69-77	2494-27	The term "wallet" has been used almost exclusively through this section when it should be "wallet or self-issued IDP"	Suggest rewording the initial sentence on lines 2496-2498 from "When the IdP runs on a device controlled by the subscriber, whether as a digital wallet or as a self-issued identity provider, the IdP is known as a subscriber-controlled wallet and the following requirements apply." to say "When the IdP runs on a device controlled by the subscriber, whether as a digital wallet or as a self-issued identity provider (henceforth collectively referred to as "wallet"), the IdP is known as a subscriber-controlled wallet and the following requirements apply." OR Suggest adding "self-issued IDP" throughout the section whenever "wallet" is mentioned
MH155	63C	5	69	2499-25	It states that "Subscriber-controlled wallets SHALL require the presentation of an activation factor in order to perform any actions requiring the use of the wallet's signing key". There are almost certainly multiple keys associated in various ways to the wallet instance on the end-users device. In this case it would seem to be important to highlight that the key is only available to sign a payload when the activation factor is presented and that it is ideally not directly accessible to the wallet application itself. It should also be separate from any signing key that my be used for authentication of non-repudiation of statemens made by the wallet alone.	Suggest a reword of this sentence to say "Subscriber-controlled wallets SHALL require the presentation of an activation factor before being able to have a signature generated that indicate a subscriber interaction took place such as onboarding of the wallet and release of attributes to an RP."
MH156	63C	5	69	2501	"and release of attributes to an RP." should include some additional wording to mention assertions and bundles	Suggest modifying "and release of attributes to an RP." to say "and release of attributes, in any assertions or bundles, to an RP."
MH157	63C	5.1	69	2505	"Providing proof of the signing key to the CSP during the provisioning process" is unclear about which signing key may be used. There may in fact be several keys that might be used in the context of a wallet. It seems likely that the intent is that a signing key bound in some way to an activation factor. There could also be several of these in the context of a wallet app	Suggest reword from "Providing proof of the signing key to the CSP during the provisioning process" to say "Providing proof of the signing key associated with the use of an activation factor to the CSP during the provisioning process"
MH158	63C	5.1	69	2507-25	"The subscriber-controlled wallet SHOULD require presentation of an activation factor before any other operations that involve use of the wallet's signing keys." is duplication of the statement on lines 2499-2500 except this is "SHOULD" not "SHALL" so there is an additional risk of mis-understanding what the Normative requirement actually is.	Suggest deletion of "The subscriber-controlled wallet SHOULD require presentation of an activation factor2507 before any other operations that involve use of the wallet's signing keys."
MH159	63C	5.1	69	2512-25	"Submission of the activation factor SHALL be a separate operation from the unlocking of the host device (e.g., smartphone), although the same activation factor used to unlock the host device MAY be used in the activation operation. ". This is probably not quite the intent. It us suspected that the intent is "unlocking of the OS User Interface". This should be precise as it is a normative requirement.	Suggest re-word from "Submission of the activation factor SHALL be a separate operation from the unlocking of the host device (e.g., smartphone), although the same activation factor used to unlock the host device MAY be used in the activation operation. ". to say "Submission of the activation factor SHALL be a separate operation from the unlocking of the underling operating system user interface (e.g., smartphone home screen), although the same activation factor used to unlock the user interface MAY be used in wallet activation operations. "
MH160	63C	Figure 13	70		An additional interaction to show CSP performing proofing would be informative	Suggest adding an additional interaction where CSP performs proofing
MH161	63C	Figure 13	70		The interaction labelled "Authenticator" implies a single authenticator.	Suggest re-labelling interaction from "Authenticator" to "Authentication"
MH162	63C	5.2	71	2532	Incorrect word used in "5. The subscriber activates the wallet through an authentication factor."... it should be "activation factor"	Suggest change "authentication factor" to "activation factor"
MH163	63C	5.2	71	2533-25	Addition to "6. The wallet creates an assertion based on the attribute bundles available to the wallet." to ensure accuracy	Suggest change from "6. The wallet creates an assertion based on the attribute bundles available to the wallet." to say "6. The wallet creates an assertion based on request parameters, user input, and the attribute bundles available to the wallet."
MH164	63C	5.3	71	2553	"The xALs available from the wallet" implies that this is something static but in reality it depends on the attribute bundles that a specific wallet instance has had provisioned and for FAL in particular it also depends on the wallet implementation itself and specifics of the RP as well.	Suggest a reword from "The xALs available from the wallet" to "The xALs potentially available via the wallet"
MH165	63C	5.3	72	2564-25	It states that "If FAL3 is allowed within the trust agreement and authenticators other than the wallet itself are allowed for use at FAL3...". This appears to be the first mention of the wallet itself being an authenticator. This concept (if intended) needs additional guidance or this implication should be removed through some rewording.	Suggest reword to clarify whether the wallet is an "authenticator" (The definition of "Authenticator" does not directly indicate that) or if it is not the intent then a reword to remove that implication.
MH166	63C	5.6	74	2629-26	It states that "The decision of whether a federated authentication can occur or attributes may be passed SHALL be determined by the subscriber, acting in the role of the authorized party.". This implies that only the subscriber can decide however there should be allowance for the there may be policies or data availabel to the wallet that enables it to act in the interests of the subscriber perhaps by having access to a list of legitimate RPs established in the trust agreement between CSPs and RPs. There may also be a restricted set of RPs that a CSP is willing for an attribute bundle to be shared with, and in the context of a CSP provisioned wallet ther emay be CSP policies implemented to prevent presentation of CSP issued bundles to entities that are undesirable from the perspective of the CSP. Question... Would a bundle issued by a US government agency be something that should be used to access adult content or to be presented to an enemy state operated RP?	Suggest a re-word of this paragraph to clarify the guidance in a wider set of contexts and that in some circumstances a decision by the subscriber is not the only decision required before attributes are passed
MH167	63C	5.8	75	2662	"8. Authentication time: A timestamp indicating when the subscriber last used the wallet's activation factor." - for consistency and precision this should probably be "Actiation time"	Suggest reword to say "8. Activation time: A timestamp indicating when the subscriber last used the wallet's activation factor."
MH168	63C	5.8	75	2671	"2. The wallet's intended FAL of the federation process represented by the assertion." - Essentially the same comment is MH68 - Intended FAL is not really very useful	Suggest deletion of "2. The wallet's intended FAL of the federation process represented by the assertion."

MH169	63C	5.8	75	2679	"1. A public key or key identifier for the key used by the subscriber-controlled wallet to sign the assertion" - this could be improved to more closely reflect the key used and the context	Suggest reword of "1. A public key or key identifier for the key used by the subscriber-controlled wallet to sign the assertion" to say "1. A public key or key identifier for the key used to sign the assertion following presentation of the user's activation factor"
MH170	63C	5.8	75	2678-26	It would seem that the CDP identifier would be needed	Suggest ad "CSP identifier" to the list of things required in the attribute bundle
MH171	63C	5.9	76	2704	It states that "... the assertion SHOULD be encrypted." This leads to the question of how encryption keys should be managed. There should be guidance and a reference to other documentation to ensure this is performed in a way that mitigates risk sufficiently.	Suggest adding guidance about how "the assertion SHOULD be encrypted." and how the crypto keys involved should be managed.
MH172	63C	5.9	76	2710-27	It states that "Since assertions from a subscriber-controlled wallet always contain a reference to the wallet's signing key inside the signed attribute bundle from the CSP", this implies there is only one wallet signing key whereas there may be many for different purposes including reduction in privacy risks relating to tracking. There is also a question about whether the intent is for a wallet bound key or an activation factor bound key is what is intended	Suggest change the wording from "Since assertions from a subscriber-controlled wallet always contain a reference to the wallet's signing key inside the signed attribute bundle from the CSP" to say "Since assertions from a subscriber-controlled wallet always contain a reference to one of the wallet or activation factor bound signing keys inside the signed attribute bundle from the CSP"
MH173	63C	5.1	77	2731-27	It states that "Additionally, the issuer MAY make available an online mechanism to determine the validity of a given attribute bundle, such as a status list queryable by the RP", perhaps there should be normative language to require that the RP uses this mechanism as part of its assertion validation process if it is available? ALSO - perhaps issuer should be replaces with CSP for consistency	Suggest rewording to say "Additionally, the CSP MAY make available an online mechanism to determine the validity of a given attribute bundle, such as a status list queryable by the RP. TThe RP SHALL validate any attribute bundles presented should the CSP provide an online mechanism to determine their validity."
MH174	63C	5	69-77	2494-27	The only wallet provisioning model mentioned in this major section about "Subscriber-controlled wallets" is CSP provisioning of the wallet. yet there are several other cases potentially including "subscriber-provisioned wallet"(Bring your own wallet?), "RP Provisioned wallet", and "3rd party provisioned wallet" (Apple, Google). There should be guidance provided for each of these cases.	Suggest adding sections to provide guidance on each of these wallet provisoining approaches
MH176	63C	5	69-77	2494-27	There is no mention of shared signalling in the section on "Subscriber-controlled wallets". However it may well be very useful for parties involved in a federation (whether IDP centred or wallet centred) to be able to share signals for risk mitigation purposes	Suggest adding a sub-section under "Subscriber-controlled Wallets" that provides guidance about the utility, requirements and prohibitions relating to the use of shred signals in that context as has been done in the previous major section about "General Purpose IDPs"
MH177	63C	4-May	77	1704-27	It is possible that a single entity could provide both a GeneralPurpose IDP and a "Subscriber-controlled wallet" and through that approach deliver the CSP, IDP and Verifier capabilities. There is no mention of this hybrid deployment model and there should be guidance on this approach	Suggest adding a section somewhere in the document that decribes this hybrid deployment scenario and any specific guidance or normative requirements arising
MH175	63C	10.1	97	3264-32	Mention of OID4Verifiable Credential Issuance and OID4Verifiable Presentations would be valuable to add as emerging protocols that may be profiled to achieve FAL levels in the context of a "subscriber-controlled wallet". It should be possible to write an informative example to a similar level of detail as those that have been provided for SAML and OIDC.	Suggest writing informative guidance on the use of OID4VCI and OID4VP as a way of delivering FALx in the context of a "subscriber-controlled wallet" oriented solution.
MH10	63C	10.3	98-99	3312-33	It would be useful to provide informative guidance on the use of some specific protocols to deliver an operational multi-lateral Federation. Suggest examples using x.509 and OpenID Federation	Suggest writing informative guidance on the use of specific standard protocols with a table similar to Table 5. Suggest using x.509 and OpenID Federation as the two "federation protocols" given as examples.