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:	*AWS*
Name of Submitter/POC:	*Jean-Francois "Jeff" Lombardo*
Email Address of Submitter/POC:	[redacted]

Comment #	**Publication** (Base, 63A, 63B, 63C)	**Section**	**Page #**	**Line #**	**Comment** (Include rationale for comment)	**Suggested Change**
01	63B	3.1.1.2	14	746	"The entire password SHALL be subject to comparison, not substrings or words that might be contained therein." Stil we should look at "Context-specific words, such as the name of the service, the username, and derivatives thereof" that means we should look at substrings.	
02	63B	3.1.6	25	1089	Sections always have some example, here we could cite may RFC of HTTP Message Signature	
03	63B	3.1.6.2	26	1124	why is this section does not have a recommendation pointer for asymmetric keys ike for symmetric keys: "The secret or symmetric key and its algorithm SHALL provide at least the minimum"	
04	63B	3.1.7.1	26	1154	"Sync fabric" sounds like a marketing term. Can't we do better? Synchornization service sounds more functionally accurate	
05	63B	4.2.2.2	45	1778	At which IAL? While it is mention in 4.2.2.3, it is not into this section	
06	63B	5.1.2	50	1947	We are in 63B, should we not focus on the IDP here instead of the RP? In this case does not the Identity Token has more value to be considered here for guidance on relation to session?	
07	63B	8.2.6	70	2402	Miss the most used one, usage of a passphrase on the private key	
08	63C	Global			No requirement at any levels for rotation associated keys related to trust establishment in between IDP and RP as per 3.5.1. This sounds strange for FAL3 to not force rotation at a minimum period of time through the usage of multiple keys with overlapping lifetimes	
09	63C	2.1	4	499	"assertions used in federation protocols include the ID Token in OpenID Connect [OIDC]" ID Token are meant as a prood of authentication for the IdP and should not be sent to the RP. How the RP could establish a session based on it then? Pretty sure you mean "the Access Token in OpenID Connect [OIDC]"	
10	63C	2.1	5	514	the document mentions two times notion of RP's risk while the rest of the document is more aligned a level of assurance expcting RP, or level of protection requried by RP. The FAL is not here to mitigate risk of the RP but for supporting a sensitive operation at the RP requiring a high assurance. Risk here has a tendency to converge towards maliciousness of the RP, which is not the point.	
11	63C	2.1	5	515	"the suscriber to reauthenticate through FAL3". Is this not AAL3 instead here? Or "presenting a higher assurance proof through FAL3" ?	
12	63C	2.2	5	525	"approved cryptography" might require some hyperlinking to other NIST guidance document	
13	63C	3.1.2	11	393	First time I hear " this is also known as the offering party (OP)."	
14	63C	3.2.3	12	728	Should mention that thisis also know nas Broker	
15	63C	3.2.3	12	728	No mention of translation of format by the proxy and the potential impact or not on the FAL	
16	63C	3.3.1.1	15	844	If privacy policy are here to mitigate risk on non PPI attribute, they should exist a separate definition than PPI as we can define privacy policies even if we don't use PPI	
17	63C	3.3.1.1	15	852	" such cases, the proxy will be able to track and determine which PPIs represent the same subscriber at different RPs" even if the Proxy can generate a PPI upstream it can reidentify the suscriber alogn multiple RP as it proxyfying all	
18	63C	3.6	23	1098	this is not possible outside of privacy policy and consent bound AAL at the IDP which is a specific object that might not always exist	
19	63C	3.7	24	1107	This section is too moot compared to the other one that expect "shall not use attributes outside" again it calls out to privacy policy expectation, right to be forgotten, and other privacy notions. Maximum lifetime of information, for which the subscriber never manifested again should be included. Exemple of exemption of such cleanning should mention other regulation like SOX and general use case for use cases not requiring explicit consent	
20	63C	3.9.1	28	1262	"The IdP SHALL limit transmission of subscriber information to only that which is necessary for functioning of the system". While Line 1267 makes a MAY reference to "if stipulated and disclosed by the trust agreement", the notion of Trust Agreement shall be set as a governing and mandatory requirement for the whole seciton. Cause if not disclosed on the trust agreement then it is not needed for processing, therefore it shall not be transmitted.	
21	63C	3.10.2	30	1344	"configuration management. If so, it may be a good idea to pass this information along to": May is not formatted as a **MAY**	
22	63C	3.11.1	32	1389	No mentionning W3C DID sounds like an opiniated omission	
23	63C	4.3.1	46	1779	This section does not re-emphase the importance of Data Processing per susbcriber attribute requirements, this will be important for the IdP as it will have to provide the consent mechanism for	
24	63C	4.6.5	57	2156	While the Identity information API definition had an example from OIDC, it would be consistently good to have an example with SCIM for this section.	
25	63C	4.9	63	2345	"8. Nonce: A cryptographic nonce, if one is provided by the RP." is a SHALL but is optional as the RP is not forced to provide one. This sounds inconsistent.	

26	63C	4.1	65	2400	See comment above, now the nonce is mandatory again through SHALL	
27	63C	5.7	74	2641	See comment above, now the nonce is mandatory again through SHALL	
28	63C	5.8	75	2664	"9. Nonce: A cryptographic nonce, if one is provided by the RP." is a SHALL but is optional as the RP is not forced to provide one. This sounds inconsistent.	
29	63C	Table 2	79	-	the first two lines of federation Threat / attacks should disjoint the "Assertion Manufacture and Modification" is two distinct threat for readability. "Assertion Manufacture" and "Assertion Modification"	
30	63C	8.2.2	90	3101	Here, there is no mention of sending an update of the consent to the Authorized parties involved for application of the new consent. Also Consent through this document is not always called with the same name, sometimes it is called "Control over Attribute disclosure"	
31	63C	References	105	3534	All OIDC references, where applicable, should at least point also to the newly ISO standardization and corresponding URL for the ISO Standard	