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

Please submit responses to dig-comments@nist.gov by March 24 April 14, 2023

Organization:	*ForgeRock*
Name of Submitter/POC:	*Kelvin Brewer*
Email Address of Submitter/POC:	[REMOVED]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
1	63-Base	4.2	15	722	Submitted by Eve Maler. The reference to "unexpired authenticators" is using terminology that does not match the language used in Part 63B (which only talks about "revocation" of authenticators, and also "inactivity" – akin to expiration – of sessions). Suggested Change: Clarify what is meant. Guessing the intention is "unrevoked authenticators". (See also our comment on Part 63A Section 2.1.)	
2	63-Base	2.3.3	8 and 9	555-586	Submitted by Steve Venema. An important part of equity and fairness is the ability of an affected individual or community to seek an explanation and request redress when a process fails. This becomes particularly important in today's age of AI-based automation where seemly faceless processes can bring with them a feeling of powerlessness for the affected indivual or community. A key component of this is so-called "explainability": where appropriate, a automated decision process should be engineered to allow someone to understand what went wrong and why. The mere presence of explainable processes can help reduce some of the user anxiety and pushback commonly associated with such automated systems. Relevant references: NIST SP 2170, NISTIR 8312 In a similar vein for user data entry requests, implementers of identity systems SHOULD expose drill-down capabilities where users can discover the "why" of an particular information request. Suggested Change: Augment section 2.3.3 "Equity" to become "Equity and Explainability" or, alternatively, create a new section called "Explainability".	
3	63-Base	Appendix A	59	2151	Submitted by Eve Maler. There is no definition of "trust", which is used throughout in a couple of different senses. Here, "confidence and trust" is used, and in many other locations, "trust" is used to mean "confidence" specifically (judging by context). Suggested Change: Recommend using "trust" exclusively here, and "confidence" exclusively elsewhere when meant as measurable confidence in a business/technical outcome. Recommend defining the word "trust" in the glossary if it is to be used in any more measurable sense than general public confidence in a service.	
4	63A	Introduction	iii	178	Submitted by Steven Jarosz Should the 800-63a-4 starting on line 178 state IAL2 is the same as IA3? Instead of stating that IAL2 is the same as IAL? It is either confusing or incorrect. Suggested Change: Assuming the question is to mitigate IAL2 remote with stronger in-person IAL3, federation with authorative providers such as passport agencies, other agencies or corporation that conduct IAL3 services, could assert their perspective of IA level. Existence of an IAL3 assertion could mitigate risk at an IAL2 service provider. To be clear this proposial is not an end-user federation as SSO with an CSP and a RP, but rather a use of back-end federation across a CSP (IAL3) and another CSP (IAL2) on behalf-of an asserted identity.	
5	63A	2.1	4	398	Submitted by Eve Maler. The concept of "unexpired" identity evidence is mooted here for the first time, and also used extensively in Section 4.3 of this Part. It has inexact analogues in Part 63B in the concept of "inactivity" (in reference to session timeout) and "revocation" (in reference to authenticator invalidation). Given a coming paradigm of a wide variety of verifiable credentials with a likely plethora of issuers functioning something like CSPs, both concepts – expiration and revocation – may be applicable particularly to digital identity evidence, but possibly to both physical and digital identity evidence. Suggested Change: Consider describing a alternative status of inapplicable digital evidence called "revoked" and incorporate it into the descriptions of fair/superior/strong evidence requirements (Part 63A Sections 4.3.3.1 through 4.3.3.3).	