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

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

Organization:	*Accenture*
Name of Submitter/POC:	*Daniel Bachenheimer*
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	Note to Reviewers	ii	156-161	"This draft ... opens the door to new technology such as verifiable credentials."	NIST should either remove this statement or demonstrate how this "This draft ... opens the door to new technology such as ... verifiable credentials."
2	63-Base	2.1	4	418-421	2.1. Scope & Applicability "... this guidance applies to all online transactions for which some level of digital identity is required, regardless of the constituency (e.g., citizens, business partners, and government entities)."	This scope of this document remains focused on traditional Identity and Access Management (I&AM) where centralized, enterprise authorities are in control of an individuals digital identity. There is no decentralization, where the individual can access online services, without the credentialing authority being part of any and all transactions. This is true for what NIST labels non-federated and federated. The scope section should clearly state that decentralized digital identity, where privacy enhancing, secure, peer-to-peer transactions require no intermediation, is out of scope.
3	63-Base	4.1	4	607-608	"The SP 800-63 guidelines use digital identity models that reflect technologies and architectures currently available in the market."	The SP 800-63 guidelines use digital identity models that reflect technologies and architectures currently available in the market for traditional Identity and Access Management where centralized, enterprise authorities are in control of an individuals digital identity.
4	63-Base	4.3.1	17	741-743	If something I have is one of the three types of authentication factors, how is device identity not considered an authentication factor as stated here: "Other types of information, such as location data or device identity, may also be used by a verifier to evaluate the risk in a claimed identity but they are not considered authentication factors."?	please provide a definition of device identity and why it is not considered an authentication factor
5	63-Base	4.3.1	18	771	***"In either of these cases, the activation secret remains within the authenticator and its associated user endpoint."***	please provide a definition of a user endpoint and how it may differ from other endpoints (1691, 1817, 2128) refenced in the document
6	63-Base	4.3.1	18	796-799	It is not clear what a "possession-based authenticator" is in the context of: "...However, biometrics authentication can be used as an authentication factor for multi-factor authentication when used in combination with a possession-based authenticator."	please provide a definition of a possession-based authenticator as it relates to biometric authentication along with the associated risks of such a remote, unsupervised probabilitic authentication method that may utilize undisclosed matching technology, undisclosed matching thresholds, and match against a non-authoritative source (e.g., a selfie of unknown quality)
7	63-Base	4.3.2	19	804-805	"As described in the preceding sections, a subscriber account binds one or more authenticators to the subscriber via an identifier as part of the registration process."	please provide a definition of identifier and how it may differ from subject identifier refenced elsewhere in the document [line 1876] but defined nowhere in the document
8	63-Base	4.4	20	831	"In general usage, the term federation can be applied to a number of different approaches involving the sharing of information between different trust domains."	please provide a definition of trust domains.
9	63-Base	4.4.1	20	873	Federation Benefits	The Federation section in general, and section 4.4.1 specifically, is silent on the benefits of decentralized digital identity which, in many cases listed in section 4.4.1, over lap. Given that the "Digital Identity Guidelines, intends to respond to the changing digital landscape that has emerged since the last major revision of this suite was published in 2017....", it is recommended that the decentralized digital identity constructs (e.g., verifiable credentials) be represented in this document.
10	63-Base	A.1	49	1793	"A credential is issued, stored, and maintained by the CSP"	"A credential is issued by the CSP; additionally, a CSP may also store, maintain, or revoke credentials"
11	63-Base	A.1	49	1798-1799	A CSP is defined as "A trusted entity whose functions include identity proofing applicants to the identity service and the registration of authenticators to subscriber accounts."	How is CSP trust established?
12	63-Base	4.4.3	22	912-913	"An RP relies on results of an authentication protocol to establish confidence in the identity or attributes of a subscriber for the purpose of conducting an online transaction."	"While using this guidance, an RP relies on results of an authentication protocol to establish confidence in the identity or attributes of a subscriber for the purpose of conducting an online transaction."
13	63-Base	5.1.4	29	1148-1149	"- The impact of providing a service to the wrong subject (e.g., an attacker successfully proofs as someone else)."	"- The impact of providing a service to the wrong subject (e.g., an attacker successfully proofs as someone else, errors in establishing uniqueness in the target population, proofing against inaccurate identity that was not captured live by a trusted entity and determined to be of sufficient quality for automated recognition). - The impact of enrolling inaccurate identity data during the identity proofing and enrollment process (e.g., not capturing biometric data live by a trusted entity and determined to be of sufficient quality for automated recognition)."
14	63A	1	2	357-359	On the one hand NIST states that identity proofing is "...the process of establishing, to some degree of certainty or assurance, a relationship between a subject accessing online services and a real-life person." While on the other hand NIST claims the Expected Outcomes of Identity Proofing include: • Identity resolution: determine that the claimed identity corresponds to a single, unique individual within the context of the population of users the CSP serves; • Evidence validation: confirm that all supplied evidence is genuine, authentic, and unexpired; • Attribute validation: confirm the accuracy of core attributes; • Identity verification: verify that the claimed identity is associated with the real-life person supplying the identity evidence; and • Fraud Prevention: mitigate attempts to gain fraudulent access to benefits, services, data, or assets. NIST seems to use the term Identity Proofing to mean different things in different sections of the document and assurance levels do not apear to align.	Identity Proofing, based on the documented expected outcomes, should remain the same and Identity Validation should be used elsewhere. Additionally, if the primary desired outcome of Identity Proofing is to establish uniqness within the context of the population the CSP serves, how is this reflected in Identity assurance levels? That is, how does IAL reflect a strong versus weak de-duplication process?

15	63A	2.1	4	395-396	"Identity resolution: determine that the claimed identity corresponds to a single, unique individual within the context of the population of users the CSP serves; "	There is no delination between Foundational Identity and Functional Identity in NIST SP 800-63-4 which should start here. Identity Proofing, where uniqueness is established within a population, is typically THE means for an authority to establish Foundational (or Legal) identity. What NIST is describing here is identity VERIFICTION for Functional Identity (i.e., in the context of a specific CSP) using Foundational Identity as a proof point. The Federal government looks to these standards for guidance and NIST is silent on the risks associated with establishing Foundational Identity instruments in ways that allow fraud (e.g., photo morphing) and inaccurate (e.g., poor quality) data. How accurate are the identity resolution processes used to create US Passports and Driving Licenses that NIST recommends agencies use? Where does NIST highlight the associated risks in their guidance?
16	63A	4.1	6	446-449	"This document describes the common pattern in which an applicant undergoes an identity proofing and enrollment process whereby their identity evidence and attributes are collected, uniquely resolved to a single identity within a given population or context, then validated and verified."	Suggestion as above with the additional comment that here the conext of the population differs from that above and consistency among definitions is paramount.
17	63A	4.1	6	446-449	"This document describes the common pattern in which an applicant undergoes an identity proofing and enrollment process whereby their identity evidence and attributes are collected, uniquely resolved to a single identity within a given population or context, then validated and verified."	This document does not describe nor reflect " the common pattern[s] in which an applicant undergoes an identity proofing and enrollment process". As stated in comment #13 above, there is no delination between Identity Proofing in the context of Foundational Identity and Functional Identity. The "common pattern" for identity proofing in the context of Functional Identity is to use a Foundational Identity construct (e.g., cryptographically verifiable identity information) to establish uniqueness and verify the identity claim against it. The "common pattern" for identity proofing in the context of Foundational Identity is a National Identity the imparts certain rights and responsibilities. In the US the closest we have are Passports and REAL ID driving licenses. Uniquessness in the former is done through biometric and demographic deduplication and, in the latter, it is a illegal to have an active driving license in more than one state. NIST should emphasize the difference beween Foundational Identity and Functional Identity and highlight that Foundational Identity, at the highest assurance levels, MUST ensure that the biometric used to binf the credential holder to the credential is taken live by a trusted entity and is of sufficient quality for automated recognition for it to be broadly
18	63A	4.1	8	472-473	"The CSP also collects one or more pieces of identity evidence, such as a driver's license or a passport."	US Passports are vulnerable to photo morhping, de-duplication errors, age, and quality isues; therefore the biometric contained within, even if cryptographically validated, has associated risks. Physical US Driving Licenses have only surface personalized photos which are vulnerable to de-duplication errors, age, and quality isues; therefore the biometric contained on the document, which cannot be cryptographically validated, has associated risks. NIST should provide guidance on these risks - awareness and mitigation strategies
19	63A	4.1	8	479-482	"3. Verification a) The CSP asks the applicant to take a photo of themself, with liveness checks. b) The CSP compares the pictures on the license and the passport to the photo of the live applicant's photo from the previous step and determines they match."	This 'verification' process should have the same/simlar authentication assurance levels described in this series and should contemplate the Presentation Attack Detection (PAD) levels described in ISO/IEC 30107-3 As above in comment #16, using the US Passport as an authorative source for automated facial recognition introduces risk that should not be overlooked*. The comparison process to determine if the live photo matches the credential photo should be defined and associated risks should be documented. Further, it should be highlighted that NIST has provided evidence that modern atomated facial recognition has shown to be more accurate in matching unfamiliar faces than humans. *The Europeans, for an example, deal with this risk in their Entry/Exit Legislation https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R2226&rid=1 Article 15 Facial image of third-country nationals 1. Where it is necessary to create an individual file or to update the facial image referred to in point (d) of Article 16(1) and point (b) of Article 17(1), the facial image shall be taken live. 2. By way of derogation from paragraph 1, in exceptional cases where the quality and resolution specifications set for the enrolment of the live facial image in the EES cannot be met, the facial image may be extracted electronically from the chip of the electronic Machine Readable Travel Document (eMRTD). In such cases, the facial image shall only be inserted into the individual file after electronic verification that the facial image recorded in the chip of the eMRTD corresponds to the live facial image of the third-country national concerned.
20	63A	4.3.3.2	11	574-575	4. The evidence contains a facial portrait or other biometric characteristic of the person to whom it relates.	How (e.g., impact on quality), where, when, and by whom the biometric charateristic was captured, and its integrity, needs to be contemplated here.
21	63A	4.3.3.3	12	592-593	5. The evidence contains a facial portrait or other biometric characteristic of the person to whom it relates.	How (e.g., impact on quality), where, when, and by whom the biometric charateristic was captured, and its integrity, needs to be contemplated here.
22	63A	4.4.1	14	677-683	Automated biometric comparison. Biometric system comparison may be performed for in-person or remote identity proofing events. The facial portrait, or other biometric characteristic, contained on identity evidence is compared by an automated biometric comparison system to the facial image photograph of the live applicant or other biometric live sample submitted by the applicant during the identity proofing event. The automated biometric comparison system uses a mathematical algorithm for the comparison.	In the context of Identity Proofing, automated biometric comparison can be used for identity resolution (e.g., biometric deduplication) to establish uniqueness within a poloulation by performing 1-to-many comparisons. It can also be used in the identity verification sub-process within identity proofing. It should be noted that automated biometric comparison is impacted by the quality of both the reference and the probe biometric samples as well as their age. Additionally, the demographics of the subjects may impact the results of automated biometric comparison which is why NIST-IR 8280 states that "While publicly available test data from NIST and elsewhere can inform owners, it will usually be informative to specifically measure accuracy of the operational algorithm on the operational image data, perhaps employing a biometrics testing laboratory to assist."

23	63A	5.1.8	23	913-915	"As applied to the identity proofing process, CSPs may use biometrics to uniquely resolve an individual identity within a given population or context,..."	This de-duplication process is a 1:N identitfication search and the associated Type I and Type II errors are measured not with FNMR (937) and FMR (936) but with FNIR and FPIR. This should be made clear as should the associated risks - especially as the gallery grows.
24	63A	5.1.8	23	933-934 943	"7. Testing of all algorithms SHALL be consistent with published ISO/IEC standards for the given modality." "10. CSPs SHALL make all performance and operational test results publicly available."	These two are related and NIST should make it clear that the ISO biometric testing standards call for Technology, Scenario, and Operational testing.
25	63B	2	3	363-368	"The ongoing authentication of subscribers is central to the process of associating a subscriber with their online activity (i.e., with their subscriber account). Subscriber authentication is performed by verifying that the claimant controls one or more authenticators (called tokens in some earlier versions of SP 800-63) associated with a given subscriber account."	This is the definition of NOT decentralized digital identity friendly and it remains unlear why NIST claims that "This draft ... opens the door to new technology such as ... verifiable credentials." [Base 156-161] Please create a model that supports decentralized digital identity to include issuance, verification (disintermediated), and user-centric control of their cryptographically verifiable attributes.
26	63B	5.2.3	32	1306-1308	"Biometric comparison can be performed locally on the claimant's device or at a central verifier. Since the potential for attacks on a larger scale is greater at central verifiers, comparison SHOULD be performed locally."	NIST failed to highlight the benefit of central verification (e.g., contol of the matching technology and thresholds, control of the reference biometric) and the risks of local verification (e.g., potential lack of control / transparancy of matching technology and reference biometric [e.g., selfie versus an authoritative source])