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:	*Trust Over IP Foundation*
Name of Submitter/POC:	*Judith Fleenor, Executive Director*
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 Reviewer	iv	210-213	NIST asks, "Are emerging authentication models and techniques – such as FIDO passkey, Verifiable Credentials, and mobile driver's licenses – sufficiently addressed and accommodated, as appropriate, by the guidelines?" The ToIP response is no, the guidelines do not sufficiently address or accomodate Verifiable Credentials. Verifiable Credentials are digital attestations that can be cryptographcially validated by a relying party without the need to interact directly with the Issuer. In both the Non-Federated and Federated paterns described in NIST SP 800-63-4 the CSP is required to retain information in a centralized fashion that a relying party must access to authenticate an identity claim. We see no accomodation for decentralization of the authentication process. *where validation means that the authenticity, integrity, and revocation status can be determined	ToIP requests that NIST create a revision of SP 800-63-4 that is supportive of user-centric identity constructs where an intermediary is not required for each transaction.
2	63-Base	2.1	4	419-421	In the Scope & Applicability section, NIST states that "...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)." With this in mind it is difficult to understand the efficacty of a model where citizens would need to rely on one or more CSPs to enroll, store, and maintain their authenticators to access corresponding services. This centralized model that the NIST 800-63-4 suite describes doesn not apear to be user friendly in that they need to register with a multitude of CSPs nor does it seem to be privacy preserving in that the CSP is part of each transaction.	ToIP requests that NIST creates a revision of SP 800-63-4 that is supportive of user-centric identity constructs where the individual is in possession and control of cryptographically verifiable claims from one or more providers that they may share using privacy enhancing technology and relying parties can validate said claims without direct interaction with the signer(s) of the claims.
3	63A	2.1	4	394-396	NIST states that, "The expected outcomes of identity proofing includes: • Identity resolution: determine that the claimed identity corresponds to a single, unique individual within the context of the population of users the CSP serves;" Furthermore, NIST presumes that another entity (e.g., soscial security administration, passport office, motor vehicle administration) performed sufficient identity resolution and offers no guidance on the identity resolution process itself and the how risk varies based on which process is used. To this end, biometrics are likely best suited for establishing uniquess within a population and NIST makes no mention of the associated One-to-Many (1:Many) Comparison, de-duplication, and defines only One-to-one (1:1) Comparison in NIST SP-800-63-4 Appendix A. Definitions and Abreviations.	ToIP requests that NIST create a revision of SP 800-63-4 that emphasizes that establishing uniquess within the context of the target population is a Foundational Identity construct that will could significantly impact risk to all down-stream Functional Identity processes. Furthermore, where Foundational Identity credentials do not include cryptographically signed biometric data captured live, by a trusted entity, of sufficient quality for automated recognition, NIST should quantify and quality the impact on the aforementioned Functional Identity process. For example, NIST should make it clear that US Passports are inherently NOT authoritative sources of identity as the photos can be, and have been, easily manipulated and not detected by humans or automation prior to being cryptographically signed.

4	63A	4.1.1	8		NIST states that "The CSP validates the authenticity, accuracy, and currency of the presented evidence." The photos in US Passports, for one example, are susceptible to photo morphing as photos are not taken live by a trusted authority, putting authenticity in doubt. ISO quality standards are not strictly enforced on the submitted photos putting accuracy in doubt. Passports are typically valid for 10 years which puts identity currency in doubt. US drivers licenses are not cryptographically verifiable since only the biographic elements are source verifiable, so relying on surface personalized photos, where the authenticity cannot be confirmed and the quality (accuracy) is questionable due to its size (resolution) and surface abrasion creates a higher than acceptable risk position.	ToIP requests that NIST create a revision of SP 800-63-4 that makes it clear how authenticity, accuracy, and currency of the presented evidence is validated and how to record the associated risks at the corresponding levels, for each category.
5	63A	4.4.1	14	677-683	NIST describes Automated biometric comparison as "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." Comparing a "facial portrait, or other biometric characteristic, contained on identity evidence" is risky and this is not made clear. As stated in Comment #4, even using biometrics contained in cryptographically verifiable documents (versus on non-cryptographically verifiable docuements) presents risks in certain cases - such as US passports - which are not highlighted.	ToIP requests that NIST create a revision of SP 800-63-4 that is reflective of the reliance on Foundational Identity documents to enable Foundational Identity transactions that includes the risks of relying Foundational Identity processes that may result in documents that are not authoritative thereby adding risk to all down-stream Functional Identity operations.
6	63A	5.1.8	22	913-916	As a derogation to Comment #3, NIST does state that "As applied to the identity proofing process, CSPs may use biometrics to uniquely resolve an individual identity within a given population or context, verify that an individual is the rightful subject of identity evidence, and/or bind that individual to a new piece of identity evidence or credential." but does not include the associated error rates (FNIR, FPIR) and risks as they do for biometric verification in section 5.2.3 .	ToIP requests that NIST create a revision of SP 800-63-4 that is reflective of the Type I and Type II error rates that are expected for identification or de-duplication searches relative to the size of the gallery or population.
7	63B	6.1	41	1562-1564 1570-1571	"Authenticator binding refers to the establishment of an association between a specific authenticator and a subscriber account, enabling the authenticator to be used—possibly in conjunction with other authenticators — to authenticate for that subscriber account." "Throughout the digital identity lifecycle, CSPs SHALL maintain a record of all authenticators that are or have been associated with each subscriber account."	ToIP requests that NIST create a revision of SP 800-63-4 that is supportive of user-centric identity constructs where Authenticator Binding does not rely on a centralized authority.