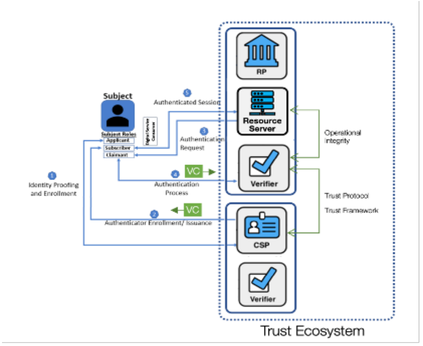
Comment Template for: NIST SP 800-63-4 Suite (Initial Public Draft)

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

Organization:	*Equideum Health*
Name of Submitter/POC:	*Debbie Bucci, Chief Data Officer & Doug Bulleit, VP Consumer LOBs*
Email Address of Submitter/POC	[REMOVED]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
1	63-Base11	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?" Equideum agrees with others who say decidedly no: the guidelines do not sufficiently address or accomodate Verifiable Credentials: digital attestations that can be cryptographcially validated by a Relying Party without the need to interact directly with the CSP 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. Moreover, we assert much potential productivity and privacy improvements, prospectively enabled via decentalization, will be truncated if not lost altogether by effectively freezing the aging Non-Federated and Federated models oultined in the current NIST draft. *where validation means that the authenticity, integrity, and revocation status can be determined	Equideum Health endorses the Linux Foundation's Trust-over-IP (ToIP herein) request: i.e., 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. Further, we respectfully submit that the IETF and W3C's fully-vetted DID/VC standard, which has been worked through the Decentralized Identity Foundation (DIF) and other authoritatve bodies, provides a solid foundatiion for this proposed "revsion." Similarly, decentralized approaches are well advanced in the European Union (under the aupsices of iEDAS); indeed this approach has already been widely implemented by some foriegn nations and is under serious consideration by several American States and Canadian provinces for univeral adoption. Equideum contends that America can ill-afford to place itself palpably behind the curve of this watershed developent in digital trust evolution. Fully embracing W3C DID/VC data models and ToIP protocols in the NIST Digital Identity Model would guide industry to the re-use of Identity Assurance outcomes. It would allow public/private sector collaboration in specific digital trust context as demonstrated in the industry approach for the US Drug Supply as well as numerous other organizations, institutions and government agencies. (see also note expanding upon this prposal under "Other Thoughts" endorsing this same "3rd-Model" recomendation)
2	63-Base11	Note to Reviewer	iv	178	NIST asks "Are these technologies supported by existing or emerging technical standards?" Yes! W3C's DID/VC, OpenIDv2/SIOP, JSON-LDw/BBS+ to name but three.	NIST should consider these and other emerging standards as it devlops a "3-Way (decentralized) Model" alternative
3	63 Base	Note to Reviewer	iv	216	NIST asks "How are session management thresholds and reauthentication requirements implemented by agencies and organizations? Should NIST provide thresholds or leave session lengths to agencies based on applications, users, and mission needs?"	Later in the document (e.g., in sec 5.1.3 @ line # 1055) NIST goes to some lenghts describing "Low, to Moderate, to High Potential Impact Levels." Equideum believes that, at least in cases of High Impact (e.g., pertaining to Protected Health Information access) long-lived Access Tokens represent a backdoor attack surface that NIST should consider minimizing. Inasmuch as both Access and Refesh tokens are typically held outside of Trusted Compute Environments (and are therefre vulnerable to all maner of malware attacks) NIST might consider restricting Access token durations to some number of minutes and Refresh to hours (vs the indefinite durations typicall employed today)
4	63 Base	Note to Reviewer	iv	222	NIST asks "What additional privacy considerations (e.g., revocation of consent, limitations of use) may be required to account for the use of identity and provisioning APIs that had not previously been discussed in the guidelines?" Equideum concurs others that assert "Privacy and RP-dependency on the IDP are among the main concerns with Federated Identity models: i.e., the IDP will know about all authentications a user does and the RP will not be able to function without the IDP. The Decentralized Identity model, however, caters to both of these concerns."	The quesiton of revocation invariably crosses into an assortment of other business and regulatoy domains (e.g., GDPR, CCPA, etc). Moreover, the persitance of a given tranasaction (i.e., and exchange of ID credentials in this case) should not negate to criticality of an effective and auditable Revocation process. In other words, a irrefutable ability to prove the that a credential had once been granted should not obviate and ability to show theta the original Issuers (or CSP) has since revoked it. For example, and expired or "revoked" driver's license credential couls still be summomend by a subject (e.g., as proof of age) even though it's cuurent revoked status (also avilable to the RP) would not faciltate renting a car. We beleive, therefore, that NIST should expand requirements pertianing to authentication provenance and audit provisions
5	63 Base	Note to Reviewer	iv	230	NIST asks "Is there an element of this guidance that you think is missing or could be expanded?" Equideum wonders whether this over-due re-look at Authentication may be overlooking one of, if not the, primary purposes of a more trustworthy Digital Identity--i.e., to enable protected access to sensitive data (aka, to authorize discretionaty access to personal data. Consequently, but one of the advantages of DID/VC subtending protocols like BBS+ is in enablement of Selective Disclosure (aka, fine-grained cosnent). Similarly, decentralized archtectures facilitate more effectuve risk management via advanced Audit & Provenance capabilities. Finally, even though the proposed Guidline points to OpenID Connect as a/the federated identity exemplar (at line 836) , it fails to note its newer ODICv2/SIOP descendent--which opens the decentralized door to the types of privacy and productivity innovations alluded throug out these comments	In additon to its appeal for NIST to open this standard to the "3rd-way" model--along decentralized DID/VC along W3C setandard lines, Equideum also suggests that NIST consider JSIN-LD & BBS+ (as means of supporting Selective Disclosure) if protected personal information as well as more powerfreul Audit & Provenance methods and OIDCv2/SIOP potential roles going forward

6	63 Base	Note to Reviewer	iv	233	NIST asks "Does the guidance sufficiently address privacy?"	Equidium concurs with others' assertion of "No. It is lacking handling privacy of interaction metadata as called above in Federation model –IDP knows about every authentication. That is problematic in healthcare mixed with the notion that government agencies operate IDP brokers. Better guidance across all documents on a “privacy by design” approach across all actors may be helpful for consumers and implementers. Of particular importance is the storing of evidence material –including biometric scans—after ID proofing has occurred. The notion of a subscriber account at the CSP (ID proofer) is concerning as it leads to storing more private data for long period of time that is needed."
7	63 Base	Note to Reviewer	iv	239	NIST asks "What specific implementation guidance, reference architectures, metrics, or other supporting resources may enable more rapid adoption and implementation of this and future iterations of the Digital Identity Guidelines?" Equideum strongly endorses the adoption of a "3rd Way" Decentralized Identity Model sugegsted below  Subject Subject Roles Applicant Subscriber Claimant Digital Service Consumer 5 Authenticated Session 3 Authentication Request 1 Identity Proofing and Enrollment 4 VC Authentication Process 2 VC Authenticator Enrollment/ Issuance RP Resource Server Verifier CSP Verifier Operational Integrity Trust Protocol Trust Framework Trust Ecosystem	In accordance with W3C DID/VC data models and Linux Foundation Trust-over-IP (TOIP), the model is adjusted showing the RP as a Resource Server (RS) with a Verifier function. Each actor (subject, RP, CSP) controls one or more Decentralized Identifiers (DID) which enables symmetrical mutual authentication. This model conceals the knowledge about with whom a subject authenticates while still allowing for trusted and governed 3rd parties in the role of CSP/ID proofers. It does, however, remove the role of an IDP as an authentication function. This allows for authoritative first-source actors to directly issue Verifiable Credentials (VC) to subjects attesting specific identity attributes (claims). As digital service consumers, subjects then present these VCs to register their DID with the RP which inherently registers a cryptographic authenticator. Decentralized Identity as a 3rd model could take on several governance functions already specified by TOIP. Subjects themselves can also issue self-signed Verifiable Credentials which could be used as directives or data-sharing and usage authorizations. This would significantly simplify proposed approaches to sector-wide challenges for Open Banking and Health Information Exchange: the subject wants to grant one RP (e.g. a health app) access to data in a resource server of another RP (e.g. the hospital). The subject simply issues an authorization-VC to the health app which presents it in the data request to the hospital. This highly composable pattern can also apply to education diplomas and in credentialling of professionals. Similarly, health plans could issue standardized digital insurance cards as VCs which would simplify real-time eligibility verification for providers –particularly when there is no prior business relationship between provider and payer (e.g. urgent care, emergency).
8	63 Base	Note to Reviewer	iv	239	NIST asks "What specific implementation guidance, reference architectures, metrics, or other supporting resources may enable more rapid adoption and implementation of this and future iterations of the Digital Identity Guidelines? Equideum also concurs with others that assert "Add a volume for Decentralization and Verifiable Credentials with DAL1-3 covering assurance levels for “digital trust”	The definition for these levels should be vetted in a broader outreach to W3C Credential Community Group, Linux Foundation TOIP, Open Identity Foundation, and Decentralized Identity Foundation (potentially others). The following suggested Decentralization Assurance criteria could be used in a similar combinational form as provided by FAL: criteria for cryptographic qualities assuring privacy, confidentiality, and non-repudiation; criteria for qualities associated with the trust ecosystem’s governance model assuring transparency and operational excellence; criteria for decentralization qualities assuring sustained funding sources, fair power distribution and participatory rights of all stakeholders. For example, in document C, line 486: “Implicit Client profile” –OAuth2.1 may appears to depreciate “Implicit Flow” while the reference provided may divert. It will be very helpful to clarify.
	63 Base	Note to Reviewer	iv	242	NIST asks "What applied research and measurement efforts would provide the greatest impact on the identity market and advancement of these guidelines?"	Equidium concurs with others that assert "Similar efforts or collaboration as put forward by the EU for Digital Identity Wallets. Also, Province of British Columbia funding Open Source Software projects in the area of Self-Sovereign Identity, e.g., VON, Verified Organization Network. Zero-knowledge cryptography to improve privacy and image provenance. The creation of a 3rd Identity Model for “Decentralized Identity” as it would significantly simplify Digital Identity and Trust ecosystems with enhanced protection against identity theft. Arguably, with the progression of digitalization, this is of national interest from a cybersecurity and an economic competitiveness perspective."

10	63A	2	2	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., social 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. .	Equideum agrees with the Linux ToIP Foundation's requests that NIST create a revision of SP 800-63-4 that emphasizes that establishing uniqueness 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. Equideum, however, would also submit that duly certified Electronic Health Records contain hightly secure granular data on individuals--fully equivalnet if not superior to previously cited utilities and fiancila institutions, that shpuld qualify themn as bone-fide CSp candidates. For example, The Fast Health Interoperability Resource (FHIR) standard now mandaate by HHS provides for an array of Demographic Resources that can be cryptographically verified and, therefore, could comprise Verifiable Credentials
11	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."	Equideum concurs with ToIP on this point and 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.