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

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

Organization:	*Peraton*
Name of Submitter/POC:	*George Hsieh*
Email Address of Submitter/POC:	[REMOVED]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
0					Ryan Galluzzo's 1 February 2023 presentation (NIST Personal Identity Verification (PIV) Workshop for Derived PIV Credentials and PIV Federation) inspired me to included comments comparing the draft SP 800-63-4 series with NIST artifacts for PIV credentials.	Be very clear when one or more biometric modality (or cryptographic keys/digital signature) are attributes of the identity evidence that can be used to assess (proofing process to examines or evaluates) the applicant's identity evidence for satisfying strong or superior status for meeting IAL2 and if assessment is different for IAL3. Would NIST consider specifying a baseline set of identity evidence and how to evaluate them at strong and superior levels mapped to IAL2 and IAL3, so that federal agencies (their ISSO and RMF auditors) can properly defined requirements for an RFP or audit a Trusted Referee (section 5.1.9 of 800-63-4A ipd). For example, a PIV applicant presents their ePassport during the enrollment process in-person to be a superior form of identity evidence that meets IAL3, but an American citizen can have their ePassport read (using NFC interface) from a smartphone for IAL2 and have the ePassport's chip verified with ICAO PKD to be considered a superior form of identity evidence (otherwise its a strong from of identity evidence without ICAO PKD verification).
1	63-Base		ii	173	IAL2 identity proofing relies on the acceptance of strong or superior identity evidence presented by the applicant. Currently the American public's primary choice of strong or superior identity evidence (state issued drivers license/identification card or US ePassport) do not have a non-face biometric modality binding themselves as the authorized bearer of the identity evidence. However, federal employees and contractors have their face and fingerprint biometrics encoded in their PIV credential. Fingerprint biometric collected during enrollment for a PIV credential can be used to verify the authorized PIV credential holder requesting a replacement PIV credential when it has been lost, stolen, or expired.	Over time, other types of identity evidence (perhaps this fall into the category of Verifiable Credentials [VC] - line 183, page ii of 800-63-4 base document) issued by U.S. government entities are eventually accepted as identity evidence (with corresponding verification checks) at the appropriate IAL level.
2	63-Base		iv	175 - 176	Current consumer grade mobile devices and personal computers do not support biometrics capture of iris or FBI/Interpol quality fingerprints out-of-the-box. An unattended remote kiosk (or purpose-built mobile workstation) placed in a semi-private location (similar to self-checkout at grocery store) could be deployed with the necessary biometric capture sensor (or device) for capturing quality biometric data already recognized by international governments for IAL2.	NIST to permit IAL2 that does not rely solely on face recognition. If a PIV credential can be used for IAL2 identity proofing, then fingerprint biometrics can be used (either from PIV credential itself) or with PIV Issuer. Common Access Card are PIV compliant.
3	63-Base		iv	178	NIST has already written a standard with supporting SP 800 series artifacts for PIV credentials. ICAO standard for ePassports enrolls fingerprint or iris biometrics to support extended access control (EAC) commonly found with ePassports issued by European Union (EU) countries.	
4	63-Base		iv	182	If NIST if considering mobile driver's license (mDL) as identity evidence; why not let the State DMV's be IdP (or CSP) where the mDL is the digital identity credential at some AAL number?	Suggest NIST provide a U.S. Federal profile of government issued identity credentials to be accepted as "strong" or "superior" identity evidence. I think this community would like to clearly know if DHS programs for green card or trusted traveler's could be accept as identity evidence or be CPS (or IdP) issuing digital identity credentials with a few modifications (described in the final SP 800-63-4 series).
5	63-Base		iv	184-186	Should the CSP (or IdP) run a biometric check to confirm the new applicant does not already exist with the CPS (or IdP) already? A biometric match of the new applicant with an existing subscriber with dramatically different biographical identity data would be suspicious. Last thing we want is one human being issued two credentials with very different biographical identity data from the same CSP (or IdP) .	NIST should speak with the GSA USAccess contractors who had perform this activity for new PIV applicants, if this is a serious consideration. There is a cost for operating an automated biometric identification system (on live scan fingerprints) and may not be worth the trouble unless this activity elevates the assurance level of the CSP (or IdP) trustworthiness as seen by the RP.
6	63A		iii	199 - 201	My observation the past 3 years of RFIs or RFPs from federal agencies seeking Digital Identity (sometimes lumped in as IdAM or ICAM) services; agencies do not specify a desired PAD level as part of their solicitations (sources sought, or RFI/RFP) for services.	Additional PAD performance metrics maybe necessary because an iBeta level number may not be a fair indicator. For example, if an iBeta level 2 evaluation for an active face liveness presentation attack detection (PAD) is considered superior (at least by the technology/service vendor) to iBeta level 2 evaluation for a passive face liveness PAD. Currently it cost more (say $0.20 per transaction) for active face liveness PAD versus passive face liveness PAD. A federal agency is more likely to choose the low cost provider thinking all technology products/services at iBeta level 2 provide the same performance capability.
7	63-Base	4	iii 11	211	If Verifiable Credentials (assuming its from W3C), then why isn't W3C Decentralized Identifiers (DID) included as one of your emerging standard/protocol/specifications... (next comment line)	If NIST plans to include Verifiable Credentials in the final version, then they should also include Decentralized Identifiers and be further along towards self sovereign identity (SSI) for enhanced privacy.
8	63A	8	40		(previous comment line)...being considered for enhancing privacy along the line of Self Sovereign Identity (SSI) in your Digital Identity Model?	Expand your Digital Identity Model to support decentralized identity ecosystem advocated by Self Sovereign Identity (SSI) concepts for enhanced privacy.
9	63-Base	4.1	11 - 14		Your Digital Identity Model could be modernized to better address the availability of digital identity services from a cloud-driven economy. Legacy entities, like CSP and RP, seems to have come from the FICAM Trust Framework Solutions (TFS) Component Services Model, figure 1 of section 3.4 FICAM Trust Framework Solutions (TFS): Trust Framework Provider Adoption Process (TFPAP) for all levels of assurance of SP 800-63-2.	Next several comments provide more specific suggestions.
10	63-Base	4.1	11	623	Name the entities in your Digital Identity Model from the perspective of the human subject (yellow page concept). The subject seeks services to be performed. An IdP authenticates the subject to other service providers (what NIST calls RP). The Service Provider (SP) authorizes the subject to access its service. It's possible for an IT systems to have both roles of (internal enterprise) IdP and SP and support external IdP from their mission (or business) partners.	Consider replacing Relying Party (RP) with Service Provider (SP). This is a modern description of the IdP's federation relationship with a SP where the subject identity (subscriber known to the IdP) is requesting a specific service from the SP to be provided to them. An SP can rely on an external IdP to authenticate a subscriber when it doesn't have that capability and simultaneously support an internal enterprise IdP for its own employees and contractors.
11	63A	4.1	11	618	Consider renaming the CSP entity. Why does he IdP needs to be different from CSP just because one entity object (IdP) is in a federation relationship and the other entity object (CSP) isn't in a federation relationship. Some IT systems may support both Authentication (the IdP role) and Authorization (the SP or RP role) services from the subscriber's point of view [employee to enterprise system]. The Authorization services of the same IT systems may have a federation relationship with an external IdP from a different subscriber's point of view [business partner to same enterprise system].	Perhaps CSP can be replaced with credential issuer (CI) patterned after NIST's existing PIV artifacts, specifically SP 800-79 for PIV (card or derived PIV credential) Issuer. Emphasize CI is responsible for "binding" the authenticator (regardless of authenticator's form factor) with an identity proofed subject as its subscriber. The subscriber may wish to bring their own authenticator that maybe provide an email or social media account or preferably a phishing-resistant security key that the IdP can accept as part of onboarding a new subscriber. The IdP or CI should not be required to provide authenticators to their subscribers, but this can as an optional service. Another advantage of replacing CSP in 800-63x-4 is to prevent confusion between Credential Service Provider with Cloud Service Provider as many of the digital identity services are increasing provided from cloud environments.

12	63-Base	4.1	11		Today's digital identity ecosystem has numerous Know Your Customer (KYC) firms specializing in remotely verifying an applicant's identity that corresponds with a strong or superior government issued identity credential for financial institutions regulated by anti-money laundering (AML) regulations. These KYC firms can offer their existing online services at IAL2 to the American public using their consumer grade mobile devices and those that are General Data Protection Regulation (GDPR) compliant will not retain sensitive personal information once the identity proofing transaction has been completed.	Consider including an object entity that performs the identity proofing activities for IAL 2 or 3 on behalf of IdP or CSP. This object entity is not responsible for enrollment on behalf of the IdP (or CSP) described for trusted referee (section 5.1.9 of 800-63A-4).
13	63A	5.1.9	24	962	Trusted referee description to "facilitate the identity proofing and enrollment on individuals" goes beyond the proposed new object entity (row describing availability of "KYC" service) to be added to the Digital Identity Model.	The KYC service only conducts identity proofing against identity evidence provided by subject (new applicant) enrolling with IdP. IdP is responsible for enrollment and collecting identity proofing data from KYC service for its own audit trail supporting IAL audit.
14	63A	10.1	51	1725	A trusted provider of "attributes" can have a trusted relationship with either the IdP or SP (or RP in 800-63-4): i) It makes more sense if the AP has a trusted relationship with the IdP when the subscriber's attribute is shared with multiple SPs. The example would be where the AP is the authoritative source for active licensure, registration, or certification of interest to multiple SPs. ii) It makes more sense if the AP has a trusted relationship with the SP when the subscriber's attribute is used for on-demand authorization decision. The example would be where the AP is the sources for knowing if the subscriber has completed annual training to access the SP's service offering or execute specific functions within the service offering.	Consider including an object entity to section 4.1 digital identity model that is an authoritative source for an attribute about the subscriber that neither the IdP or SP (or RP in 800-64-4 idp) controls. For this discussion, let's call this object entity an Attribute Provider (AP).
15	63-Base	4.4	20	838	With the inclusion of SCIM protocol, does NIST intend the IdP be able to support account creation, modification, and deletion with the SP (or RP in 800-64-4 idp)?	Looking for the business purpose for why NIST added SCIM as part of Federation.
16	63-Base	4.4.2	22	901	No SCIM (or account sharing) example like there is for SAML, Kerberos Tickets , and OpenID Connect.	
17	63C	12			No SCIM example.	Can NIST provide a SCIM example in this section of 800-63C-4? This section has examples of SAML, Kerberos Tickets , and OpenID Connect. Or cross references to section 5.4.1 and/or 5.4.3 if they are NIST's example of using a provisioning protocol or API.
18	63-Base	4.4	20	839	As much as I like the idea of sharing authorization decision as part of identity federation, it isn't supported with the rest of 800-63-4 suite (see next two comments). The Digital Identity Model does not call out a reference source of authorization information to share with the SP (or RP in 800-64-4 idp) from the remaining 4 object entities. Is NIST's effort around NGAC (SP 800-178, section 2.3) another choice to XACML?	Here are some suggestions to further support this bullet: i) Modify definition of Federation (page 51 of SP 800-63-4 idp) to include conveyance of authorization information as well. ii) Add additional object entities to your Digital Identity Model (in section 1) to support policy driven authorization management. Perhaps NIST can reference figure 6 XACML Reference Model from SP 800-178 or more simplified version
19	63-Base	4.4.2	22	901	No XACML (or authorization decision sharing) example.	Can NIST provide a XACML example in this section of 800-63C-4? This section has examples of SAML, Kerberos Tickets , and OpenID Connect.
20	63C	12			No XACML (or authorization decision sharing) example.	Can NIST provide a XACML example in this section of 800-63C-4? This section has examples of SAML, Kerberos Tickets , and OpenID Connect.
21	63-Base	5 5	23 24	925- 927 979	Citing FISMA and using the same impact levels (Low, Moderate, and High) invites confusion when federal agencies are compelled to implement this section with their FIPS 199/RMF SP 800-53/SP 800-53A security and privacy controls for ATO. Has NIST considered adding the equivalent of 800-53A to guide the DIRM auditors for determining compliance with this section?	Provide guidance so a federal agency's ISSO can be certain when section 5 is mandatory for ATO? Some example situations for consideration: i) Only applies when a federal agency offering identity services for object entities listed in the Digital Identity Model (section 4 of 800-63-3) outside of federal government? ii) Does it apply to all federal enterprise IT applications when (employee/contractors or mission/business partner) subscribers authenticate themselves without a PIV (or derived PIV) credential? The enterprise IT application is not an object entity listed in the Digital Identity Model. iii) If the agency's FIPS 199 for a citizen facing mission system has an overall risk impact level of High, then should the Digital Identity Risk Management (DIRM) impact level be High also? Unless its NIST intention that the RMF and DIRM impact level be completely independent of each other.
22	63-Base	5.1	24	979	Suggest NIST adds some additional guidance to determine the impact assessment of High, Moderate, or Low; so there will be some resemblance of consistency of the impact assessment among federal agencies operating any of these digital identity services.	Please confirm and explain rationale if the DIRM impact assessment of High, Moderate, or Low are (or are not) related to 800-63 assurance levels of 1, 2, or 3. Please confirm and explain rationale if the 800-63 DIRM impact assessment of High, Moderate, or Low are (or are not) related to NIST RMF 800-53 High, Moderate, or Low impact level.
23	63-Base	Table 1 5.1.4	29 30	1163	This table could use a better explanation that the far left column accounts for section 5.1.3. The "Harms to individuals" and "Harms to Organizations" columns come for the bullets found in section 5.1.2. Seems to me the 2 columns on the right [(Harms to individuals) and Combined Impact Level] are not explained in sections 5.1 or 5.1.x.	Need guidance for completing Combined Impact Level column of this table. For example, is the Combined Impact Level column In table 1 (page 30 of 800-63-4) determined by the highest impact level from the columns on the left (like we do using the FIPS 199 form for determining overall risk impact for 800-53 RMF evaluation)?
24	63-Base	A.1	60	2152	Seems to be a duplicate of line 2153	
25	63-Base	A.1	61	2206	..confirming "the a" set... should be corrected.	
26	63A	5.1.8	7	930	This requirement should be re-worded; the IdP (or CSP) shall ensure the biometric algorithms they use (developed in house or purchased/licensed from a commercial biometrics vendor) be tested by an independent entity. That way multiple IdPs (or CSPs) can accept the independent entity's test result for a specific biometric algorithm.	The independent entity testing biometric algorithms should be listed on a pre-approved list of biometric testing labs or organizations.
27	63A	5.1.8	7	933	Testing of "all algorithms" to a specific standards organization seems overly broad and restrictive. Perhaps it would be better to specify the type of algorithms mandating conformance to ISO/OEC standards. For example, is NIST specifying the presentation attack detection (PAD) algorithms for a supported biometric modality conform to ISO/IEC 1989-3 standard? Does NIST intend to cover other algorithms related to biometric technologies, such as biometric collection or matching algorithms to ISO/IEC standards only?	Could other recognizable standards bodies such as ANSI/NIST-ITL or IEEE standards related to biometric technologies be included when ISO/IEC standards do not exist?
28	63A	5.1.8	7	934	Is NIST only concerned with only biometric modality (see lines 907-908 and 911-912, page 22) that can be matched to the government issued identity evidence that are considered strong or superior for determining identity assurance levels? Perhaps enrollment of the subject's biometric can be seen at 2 levels: i) Primary biometric is used to biometrically verify the subject is the authorized owner of the identity evidence's embedded biometric data (part of IAL process) ii) Alternate biometric(s) are captured by IdP (or CSP; trusted referee?) during enrollment to support non-repudiation or re-proofing in the future (part of FAL process or renewing AAL credential)	What are NIST's thoughts for collecting other biometrics that the IdP can collect during the enrollment process to be used for non-repudiation, re-proofing, or step-up authentication purposes? These following other biometric modalities are not bound to strong or superior government issued identity evidence currently. Some possible biometrics modalities using consumer grade products include: - contactless fingerprint; several SP 500 series publications from NIST with at least two competing developer kits supporting both iOS and Android mobile devices - Palmprint (or palm crease) with competing developer kits supporting both iOS and Android mobile devices or webcam of Windows computer - Heartbeat (FDA approved ECG app) for continuous authentication using fitness band, smartwatch, or ring in conjunction with the subscriber's endpoint device.
29	63A	5.5.6	31	1196 - 1197	In the use cases where biometrics are used to verify the subjects (in any of the 3 roles from the Digital Identity model); there not seems to be any guidance to securely storing the biometric data to be used for the purposes of non-repudiation and re-proofing.	Can NIST get to the same level of technical specificity like they did for managing biometric data for the PIV (includes Common Access Card [CAC]) credential? Reference SP 800-76-2 and 800-156 for managing biometric data for PIV.

30	63-Base		54		Missing definition for "non-repudiation". Would this include a means to biometrically verify a subscriber as a form of step-up authentication (boost AAL level from original authentication process establishing a session)?	Please provide a definition for "non-repudiation" to add relevant context to 800-63A-4 section 5.5.6 Biometric Collection.
31	63-Base		58		Missing definition for "re-proofing". Is this when IdP (or CSP) can biometrically verify a subject's identity without having to examine (or re-examine) their identity evidence for a replacement or new credential?	Please provide a definition for "re-proofing" to add relevant context to 800-63A-4 section 5.5.6 Biometric Collection.
32	63A	5.5.6	31	1197	Biometrics captured during initial enrollment become stale after several years. There is no mention of biometrics used as an authentication factor (in conjunction with something you have authentication factor; 800-63B-4 page 32 lines 1278-1279) become stale (ages) over time and needs to be re-freshed with IdP (or CSP).	Would NIST consider adding recommendations for CSP (or IdP) to re-enroll a subject's biometrics since the original enrollment (or last re-enrollment) for refreshing the subject's biometrics of record as their biometric characteristics will change as they get older or other life change (elective face surgery, trauma to body part used to collect biometric data, etc.)?
33		5.2.3	32 33	1264 & 1315	Looking for clarity on "biometric protection template" and conformation is ISO 24745 is the correct corresponding standard. NIST's Patrick Grother is quoted in news article (dated 2 March 2023) stating "ISO/IEC 24745 sets a standard for biometric information protection, and ISO/IEC 30136 sets a standard specifically for the protection of templates, without specifying a particular biometric modality."	The author's of SP 800-63-4 should circle back with NIST's group who specializes in biometrics to strengthen this section in SP 800-63B-4 and sections 5.1.8 and 5.5.6 in SP 800-63A-4 as appropriate.
34	63B	5.2.3	32	1279	Section 5.2.3 does not provide guidance for protecting the biometric data at-rest that is used to biometrically verify the subject. There are many biometric vendors offering biometric capture capabilities on consumer grade mobile device and personal computers that operates as a small software application to augment the "something you have" device's native authentication capabilities.	Suggest additional sentence(s) describing biometric data be protected within the cryptographic capability of the subject's "something you have" authenticator. This would reuse language for secure element, TEE, or TPM found in 800-63B-4 draft, page 28, section 5.1.7.1, lines 1109-1119 to cryptographically protect the biometric data.
35	63B	5.2.3	33	1299-1300 1306-1307	I was looking for NIST guidance for a biometric cryptosystem, where biometrics provides authentication credential and the cryptosystem that protects any biometric systems from attack or security threat. SC-12 and SC-13 security controls from SP 800-53r5 are looking for FIPS validated, or NSA approved algorithms. Other classes of cryptography for a digital identity ecosystem have been suggested by standards bodies or industry consortiums. Meanwhile U.S. federal agencies would be challenged by RMF auditors for satisfying these security controls using non-compliant cryptographic algorithms that do conform to classical cryptography covered by NIST's Cryptographic Module Validation Program (CMVP). Perhaps NIST can bring together their cryptography and biometric group to identify emerging biometric cryptosystems and peer-review promising cryptographic algorithms (like Post-Quantum Cryptography [PQC]) for FIPS validation for the future digital identity ecosystem.	I have the following types of cryptography use cases in mind for a biometric cryptosystem for NIST's consideration: 1)The ability to split the enrolled reference biometric into two (or more) parts. One part is securely bound to the "something you have" authenticator device (like a smartphone) in the hands of the subject subscriber and the second part is securely stored on a server linked to the IdP (or CSP) and available to the "verifier" capability. Splitting the enrolled reference biometric prevents large scale theft of biometrics data that could be replayed by the thief should the IdP's server hosting biometric data was breached. The Biometric Open Standard (BOPS) described in IEEE 2410-1917 is an example of this kind of biometric cryptosystem employing visual cryptography. One technique has been credits to Moni Naor and Adi Shamir (the "S" in RSA). 2)Protecting the reference biometric data (collected during enrollment with IdP) and real-time capture of biometric data for conducting 1:1 biometric verification. Homomorphic encryption holds the promise of acting on encrypted data (1:1 verification of reference biometric data and real-time capture of biometric data) with compromising the encryption. This is featured in IEEE 2401-2021 for the Standard for Biometric Privacy (SBP). 3)Distributed ledger (a.k.a. blockchain) mechanism are appearing in commercial identity platforms targeting customer interested in Verifiable Credential and Distributed Identifiers.
36	63B	6.1.2.3	44	1662 & 1669	Why isn't there any guidance for reestablishment of authentication factors at IAL2 or IAL1 (line 1663 is for IAL3 and line 1669 is without IAL)	I'm specifically looking for NIST guidance stating the conditions to use the biometric(s) collected during enrollment used for account recovery at IAL2. Would the guidance be different if the primary biometrics used to match the identity evidence of the authorized evidence holder was augment with one or more other biometrics (see "different biometric modality" on line 1296, page 33, SP 800-63B-4) collected during enrollment? Examples of other biometrics were listed in a previous comment as contactless fingerprint, palmprint (or palm crease), and heartbeat.
37	63C	5.4.4	29	1075	If the RP is a cloud-based X-as-a-service from a for-profit entity, then is SORN still the right guidance?	If SORN is still the correct guidance, then NIST should sections 5.5 and 9.4 of 800-63C-4 so SORN isn't seen as a federal agency-specific privacy compliance activity.
38	63C	5.7	32		One of the most common shared signals in the digital economy we'll encounter is when a subject changes their mobile carrier for their smartphone service. Is the IdP solely responsible for knowing if this mobile carrier change is authorized or not? If the aner is it depends, then how would it affect the assurance level of "something you have" or even the mDL that is residing on the smartphone?	SP 800-63 has accounted for identity evidence at different assurance levels to date, but has not addressed the subject's consumer grade "something you have" device and supporting services vulnerable to attack; such as a SIM swap attack (is this a new entry in Table 3 of SP 800-63B-4?) with change in mobile carrier service. Its possible this topic is addressed in the public draft for SP 800-157r1 or another NIST SP artifact that can be referenced in the final SP 800-63x-4.
39		6.3.1	46	1575- 1579	Why is this section written as if the IdP is mandatorily responsible for all attributes (the one its holds and those held by external attribute providers) for the RP? What if the RP requires a up-to-training (recertify subject's training status annually) attribute to execute privileged commands from its service offering? Its more likely the RP would have the trusted agreement with an external service keeping track of the subject's training status has been renewed annually versus having the IdP involved with this type of attribute (tied to a service versus an identity).	Suggest NIST update their Digital Identity Model (section 4 of SP 800-63-4) to include Attribute Provider (AP) entity and modify this section so an AP can have a relationship with either the IdP or RP.