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:	*Kuma, LLC*
Name of Submitter/POC:	*Michael Magrath, Managing Director - Digital Identity*
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	iii	148	mechanisms to securely deliver services… and emphasizes the need for digital identity services to support multiple authenticator options to address diverse consumer needs and secure account recovery. We suggest NIST publish a “quantifiable” set of measures and requirements for proofing and authentication levels, including a set of technologies/elements with their corresponding values. With such a framework in place, the technology community can build innovative approaches to satisfy the desired proofing/authentication value outcomes with being limited by a small set of acceptable methods. This is especially critical with regard to NIST’s request for alternatives for solutions such as Face Biometrics. Please find the areas of focus regarding this topic below: - Establish a scoring/measurement system for all proofing and authentication levels. 800-63-4 should include a scale that allows all CSPs to understand the value of proofing and authentication. For example, an IAL2 Proofing event must equal a value of “10 points”. - Rather than a short list of “strong” and “fair” pieces of evidence, please offer a list of evidence categories with point values. From there the technology community can innovate to achieve the desired outcomes in ways that will address all populations better by combining them to better fit the realities of each audience. - In lieu of publishing a list of acceptable evidence “categories” and point values, NIST may also allow for solution providers to present their own assessments of proofing/authentication values when the are certifying their solutions. Further, they may also be allowed to present their case for alternatives and unique combinations of evidence that meet the spirit/desire of 800-63-4 for approval. NIST stands to unlock the true innovative capabilities of the solutions market by clearly stating quantifiable details for all proofing and authentication levels. With the freedom to creatively develop solutions that achieve the desired outcomes for each proofing/authentication level, the choices available to CSPs across public and private sectors will flourish. These options will drastically improve the overall ability to make the advancements in equity and accessibility described in the draft.	
2	63-Base	Note to Reviewers	iii	175	publish a quantifiable scoring system within the identity proofing process incorporating values to allow for value-based replacements for elements such as Selfie Match. 1. We believe that the innovative strengths of the solutions marketplace would be unleashed with more freedom to combine technologies/practices to deliver the intended outcomes of all proofing and authentication levels. A well-constructed valuation methodology would empower the development of a robust marketplace of solution options to meet the identity assurance goals of the rule. 2. In order to offer alternatives to the use of biometrics at the highest levels of proofing and authentication, the market needs a means of quantifying the value they currently bring to a model. With a methodology clearly communicated within guidance, solutions can be assembled to offset the value only biometrics could deliver under prior rule releases. 3. Improving equity and accessibility requires solutions to be extended to meet the capabilities available to lesser served populations. With a methodology that offers room for solutions providers to assert new evidence/approaches (and to propose what values they should hold) we can collectively broaden support to wider demographics across more channels. 4. Specific risk-based value categories can be created to allow for multi-vendor support such as: a) Device fingerprint risk; b) Device Reputation risk; c) Real-time user behavior risk; d) identity attribute risks; e) identity resolution risks; f) Photo ID risks; g) KBV risks.	
3	63-Base	General Comment			In support of NIST’s desire to increase one-time and ongoing device risk assessment and trust, 800-63-4 should specifically call for demonstrated techniques/technologies that are being leveraged with all devices that are involved in a proofing or authentication workflow. Device risk should include device reputation. Assess Real-Time Device Risk on all inbound channels regardless of modality For Identity Proofing, CSPs should be able to assess the riskiness of all devices invoked by individuals during entire process. Individuals may interact with the CSP through a series of channels/devices during the proofing process including personal computers, tablets, mobile devices and even phone calls with a call center representative. 800-63-4 should include requirements for CSPs to demonstrate their ability to assess risk with regard to all of these devices at proofing time… and on a regular basis thereafter as the individual returns to authenticate themselves and via normal business transactions to ensure the identity continues to operate within reasonable risk thresholds. For Authentication, CSPs should be required to have one-time and ongoing risk assessment capabilities in place specific to the devices that hold authenticators. When an authenticator is aligned with a proofed identity, the CSP must be able to demonstrate their ability to re-assess risk whenever the authenticator is presented at a minimum. For adding new Authenticators or changing identity attributes, CSPs should be able to demonstrate their ability to assess the risk of any device used during the request and provision of new authenticators acter the proofing event has been completed. The new authenticator should adhere to the requirements above in that they are able to assess the device and device reputation risk every time the individual presents it for authentication. Ongoing use of Authoritative Attribute Providers should also be specifical required for CSPs to have in place regarding their proofed identities as a means mitigating risk long-term. CSPs should be able to demonstrate a dynamic ability to leverage their relationship with the authoritative sources they leveraged during identity proofing to be alerted to changes	

4	63-Base	Note to Reviewers	iii	187	NIST asks, "Are there existing fraud checks (e.g., date of death) or fraud prevention techniques (e.g., device fingerprinting) that should be incorporated as baseline normative requirements? If so, at what assurance levels could these be applied?" SP800-63 has always been more of a binary identity check. We believe that fraud checks should not be normative requirements, and should instead be considered as risk mitigations. This is because industry provides risk insights differently across vendors, making specificity difficult to document within guidance (except at the highest level – see (3) above). Also, as technology changes, prior fraud checks may be replaced with new ones making conformance difficult on CSP's going forward. That being said, guidance that references known and accepted high level fraud checks (see (3) above) can be referenced within guidance to provide underlying support for CSP assessment processes who chose to use them as risk mitigations	
5	63-Base	Note to Reviewers	iii	206	NIST asks, "How might risk analytics and fraud mitigation techniques be integrated into the selection of different identity assurance levels? How can we qualify or quantify their ability to mitigate overall identity risk?" The required use of risk-based controls (but not normative/specific requirements) to allow for KBV's at IAL1 and the non-selfie matched Photo ID at IAL2. This would allow CSPs to document and employ risk mitigations that match their preferences across a range. We encourage NIST to create room within the 800-63-4 for CSPs and solution providers to assess all risks with the goal of minimizing the need for individuals to be proofed with a facial comparison. IAL1 evidence, combined with a lack of risk-based telemetry, should allow for transactions that previously required IAL2 proofing to be performed with expanded options. Not only would this adjustment allow for individuals to opt-out of biometric technologies, it would also support broader capabilities aimed at addressing equity and accessibility	
6	63-Base	Note to Reviewers	iv	230	NIST asks, "Is there an element of this guidance that you think is missing or could be expanded?" 1. As digital channel access controls have improved, impersonation attack risks have shifted to call centers. 63-4 should therefore provide guidance for Agencies and CSP's to protect telephony or the audio channel with the definition of "omnichannel authentication". 2. STIR/SHAKEN is a caller ID authentication methodology designed for this purpose and will protect against Spoofed Calls (fraud) and Robocalls (waste & abuse). This service is provided by telephone carriers and is analogous to digital channel encryption. 3. This recommendation is also supportive of equity as not all users are able to use the digital or in-person channels. 4. Increasing equity and accessibility means meeting users with capabilities they have available to them. STIR/SHAKEN, and complementary solutions, may reduce the risk profile for under-served populations.	
7	63-Base	2.3.3. Equity	8	554	channel access controls have improved, impersonation attack risks have shifted to call centers. NIST should broaden the landscape of technologies included in omni-channel identity by introducing more telephony-based capabilities within the scope of the rule for both proofing and authentication. 63-4 should therefore provide guidance for Agencies and CSP's to protect telephony or the audio channel with the definition of "omnichannel authentication". We recommend the inclusion of Secure Telephone Identity Revisited (STIR), sometimes referred to as STIR/SHAKEN, to protect the audio channel and therefore securing relying party trust. There is also the potential to use STIR for IAL's. The STIR capability is supported by the FCC here: https://www.fcc.gov/call-authentication Rationale: 2. STIR/SHAKEN offers the opportunity to add safety to phone-based interactions analogous to the rigor encryption provides to digital channels. The ability to leverage a digital signature within the SIP header of a call offers innovative vendors new pathways to explore in creating proofing/auth capabilities. STIR/SHAKEN expands the art of the possible for all solution providers. 3. This comment lends itself to addressing NIST's desire for alternatives to offset the use of biometrics. Telephony oriented solutions (likely combined with others) may address the desire for non-biometric alternatives. 4. This recommendation is also supportive of equity as not all users are able to use the digital or in-person channels. 5. Increasing equity and accessibility means meeting users with capabilities they have available to them. STIR/SHAKEN, and complementary solutions, may reduce the risk profile for under-served populations. 6. If Trusted Referees can support users in a Remote Supervised fashion within a call center, proofing would require security protections analogous to encryption within the digital channel.	
8	63-Base	2.3.3. Equity	8	554	Providing equitable accessibility to programs for all populations requires 800-63-4 to have the ability to welcome the use of "Pay-as-you-go" mobile phones. NIST is looking for pathways to better extend access to important programs/systems for populations that have been historically underserved by identity proofing/auth solutions. Certain demographics leverage pay-as-you-go mobile phones for a variety of legitimate reasons. We believe those devices should be more welcome within omni-channel identity services and therefore encourage NIST to make accommodations for them in the next draft via specific reference. This simple update would provide support to CSPs in the use of such devices which is supportive of equity and inclusion.	

9	63A	Note to Reviewers	iii	185	Rationale: NIST asked, "What methods exist for integrating digital evidence (e.g., Mobile Driver's Licenses, Verifiable Credentials) into identity proofing at various identity assurance levels?" Response: mDLs may be used as a source of signed data attributes from an authoritative source (state DMVs). They may also be leveraged an authenticator (either at the time of proofing or by linking sometime later). However, they should adhere to some of the other suggestion presented within this comments document. Here are some specific areas for NIST to consider regarding the use of mDLs as they become more prevalent: -mDLs should all be able to present a public key certificate that can be authenticate back to a trusted issuing authority. States may publish their own public key certificates, but most will likely partner with AAMVA (American Association of Motor Vehicle Administrators) as participants with their new mDL Digital Trust Service. The mDL DTS will securely collect and publish the public key certificates of participating issuing authorities thought a single Verified Issuer Certificate Authority List (VICAL) for all relying parties to access. NIST should consider requiring all mDLs used in proofing/authentication under 800-63-4 should make their public keys available to the community via AAMVA's mDL DTS Service, or equally trustworthy means. -mDLs should all be conforming to the ISO 18013-5 Standard for interoperability as a base requirement. This standard has been established collaboratively with an international working group and has included the leadership of AAMVA and many US state DMVs. Adherence to the standard will drive the interoperability and ubiquity required for mDLs to enjoy the same universal acceptance that physical driver licenses have historically. -Every device leveraged during a proofing/authentication process include one-time and ongoing risk assessment, including devices that hold or present mDLs. When an mDL is leveraged during the proofing event of a CSP, the device should be assessed for reputation and device fingerprint specific risks. Further, anytime an mDL is leveraged as an authenticator there should be continuing risk assessments made to ensure the device holding the mDL continues to be safe to trust.	
10	63A	4.3	9	495	Multiple types and combinations of identity evidence are referenced. NIST should publish and maintain a list of acceptable identity evidence. This should not be a document, but a live website that can be continuously updated for agencies to reference. For example, concealed carry gun permits may be classified as STRONG identity evidence if issued by one state or county and FAIR evidence if issued by another state or county, depending how it is issued and what the permit looks like including the presence of security features or not present.	
11	63A	4.4.1	15	684	Control of a digital account. It would be helpful for NIST to provide an example of how this would be done during a remote identity proofing session.	
12	63A	5.1.8	23	930	63A states that CSPs shall have all biometric algorithms tested by an independent entity. Question: Is this a one-time test or should the algorithms be re-tested periodically, e.g.. annually?	
13	63A	5.1.9.1	24	993	Question regarding Trusted Referees With the expansion of the role Trusted Referees will play in 800-63-4, can you please add specifics regarding their ability to make "risk-based decisions". Is it the intent of NIST to allow individuals to make risk-based decisions by relying on published CSP policies? Or, are risk-based decisions purely made by systems/software? What ability can/should the referees have to override or make individual decisions. This is especially important in the areas of advancing equity and accessibility as the requirement for unique actions will be dramatically increased. In order to cater to the diverse needs of specific (perhaps traditionally under-served) populations, Trusted Referees should be well empowered to make decisions. Please offer guidance within the next draft regarding this aspect of the rule.	
14	63A	5.3	26	1035	We encourage NIST to include method(s) through which more service can be offered at the IAL1 level in the spirit of simplifying processes and increasing equitable accessibility. Specifically, we recommend that the rule contain guidance regarding risk thresholds that indicate whether an individual must be proofed at IAL1 or IAL2 levels for IAL2-like transactions. If risk assessment yields a "low" risk of concern regarding the trustworthiness of the individual, IAL1 should prove sufficient to support actions previously reserved for IAL2. Alternatively, "high" risk assessment may require individuals to be proofed at IAL2 before safely transacting. We request that NIST include measurement criteria within the rule and/or offer certification bodies the ability to evaluate/certify risk assessment approaches under the standard. Given sensitivities regarding the use of biometric comparisons, NIST could simply adjust the definition of Strong evidence to exclude the requirement for identity binding to a photo ID when risk-based controls are present thereby allowing for a more equitable IAL 2 with fewer failures. Increase support for the use of knowledge-based questions at IAL 1 when risk-based controls are present including required velocity controls to prevent scaled attacks. Adjust impact assessment and assurance level selection to incorporate use cases that are applicable: i.e. IAL 1 = CSP interactions supporting government benefits or call center-based interactions; IAL 2 = CSP interactions involving the release of digital data such as tax or health information	NIST clearly is looking to allow for more business to be conducted without the need of the biometric elements prevalent ir
15	63A	5.4.2.1	28	1106	800-63-3 requires one piece of STRONG evidence and two pieces of FAIR evidence for IAL2. While we support this, what is NIST's reasoning for lowering the FAIR evidence requirement from two pieces to one at IAL2?	

16	63A	10.4	54	1818	If Remote Supervised is acceptable across assurance levels using Trusted Referees and potentially involving Vouching Parties, then non-digital guidance should be provided within 63A and 63B. Rationale: 1. Call center-based proofing using Trusted Referee in a Remote Supervised format is technically feasible using hybrid digital/audio technologies. 2. This channel is required to support large populations in an equitable manner as desired by CSPs for the benefit of the customer facing federal agencies including SSA, IRS, VA, CMS and users 3. Equity and inclusion is promoted in a cost efficient manner by supporting the telephony channel. 4. The use of call center-based proofing will allow for the use of an agent/Trusted Referee at non-IAL3 assurance levels.	
17	63B	4.2.2	9	532	**If Trusted Referees can support users in a Remote Supervised fashion within a call center, proofing would require security protections analogous to encryption within the digital channel. 63B-4 makes multiple references to encryption that shall be implemented to protect the digital channel. Therefore, we recommend the inclusion of Secure Telephone Identity Revisited (STIR), sometimes referred to as STIR/SHAKEN, to protect the audio channel and therefore securing relying party trust. There is also the potential to use STIR for IAL's. The STIR capability is supported by the FCC here: https://www.fcc.gov/call-authentication** **Rationale:** **1. As digital channel access controls have improved, impersonation attack risks have shifted to call centers. 63-4 should therefore provide guidance for Agencies and CSP's to protect telephony or the audio channel with the definition of "omnichannel authentication".** **2. STIR/SHAKEN is a caller ID authentication methodology designed for this purpose and will protect against Spoofed Calls (fraud) and Robocalls (waste & abuse). This service is provided by telephone carriers and is analogous to digital channel encryption.** **3. This recommendation is also supportive of equity as not all users are able to use the digital or in-person channels.** **4. Increasing equity and accessibility means meeting users with capabilities they have available to them. STIR/SHAKEN, and complementary solutions, may reduce the risk profile for under-served populations.**	
18	63B	5.1.8.1	29	1156	To avoid confusion with conformance of the Guidelines we recommend that NIST eliminate the practice of including back links/references to preceding requirements. In this case referencing Sec. 5.2.12. It would be much clearer to just restate the full requirements for each authenticator. This will increase the number of pages, but that should not be a factor. Clarity is more important.	
19	63B	5.1.8.1	29	1157	"requirements" is misspelled.	
20	63B	5.2.2	31	1235	Rationale: Clarity Comment: 100 consecutive failed authentication attempts on a single subscriber account seems to be way too permissive and poses a risk to the subscriber. Why is this number not a lot less? Closer to 10 seems more appropriate.	