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

Please submit responses to dig-comments@nist.gov by October 7, 2024.

Organization:	*Kantara Initiative*
Name of Submitter/POC:	*Carol Buttle*
Email Address of Submitter/POC:	[redacted]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
KI-1	63-Base	N/A	N/A	N/A	It would be helpful to have more clarification from NIST about the order of precedence for requirements listed throughout the draft.	
KI-2	63-Base			490	Does NIST have suggestions that go beyond FedRAMP and ISO 27001?	
KI-3	63-Base			554	Does Equity include an intentional effort to support digital identification for underserved communities and how is that aligned with raising the evidence standards?	
KI-4	63-Base			921	This section should contextualize or qualify the applicability of the risk management to CSP vendors who may not or cannot know the users, transactions and data their system will support until they engage with a client. They would typically start at 3.3 by identifying an assurance level for market reasons.	
KI-5	63A			284 - 286	Why is Remote Unattended proofing not addressed? Ditto 4.2 (but understood why it is explicitly omitted from 4.3)	Include such a section with appropriate requirements in each of 4.1 and 4.2; Consider also inclusion in 4.3, if only to make a definite assertion that such proofing SHALL NOT be performed at IAL3.
KI-6	63A			363	These services do not provide identities, which the term 'identity service' might suggest, they prove (or not) claims to existing ones.	To be more accurate and to align more closely to phrasing such as "identity proofing [types]" the term "identity proofing service" should be used throughout.
KI-7	63A			385 - 389	This suite of documents implicitly anticipates a single entity **(the** CSP) as being the provider of services addressed by SP 800-63. Market experience however shows the emergence of a majority of Kantara-approved services as being 'Component Services', i.e. ones which do not fulfil the entire scope of -63 mandated functionality and generally do not manage first-hand the relationship to the proofing Applicant, Rather they tend to provide some form of specialist functionality, e.g. that offered by credit bureaus and other complex technical capabilities, such as document verification. This should be acknowledged in these documents.	Following the referenced paragraph, add: "Though this document refers to the CSP in a singular manner it is recognised that market forces and capabilities may see specialised CSPs providing a part of the required functionality for a full CSP service. References to 'the CSP' should therefore be seen as being potentially a CSP providing only a suite of functionality which would serve as a component of a fully complete offering which, *in toto,* meets all of the applicable requirements from this publication.
KI-8	63A			402	A subscriber may be an entity paying for or organising the proofing of a given population of individuals. The term may also suggest that the entity is known to the CSP, but where CSPs are 'nested', i.e. one (CSP-B) performs a part of the required functionality which is consumed by another entity (CSP-A) which handles the interface with the Applicant (the party seeking to be proofed), then the Applicant need have no direct knowledge of CSP-B and hence have no 'subscription' *per se* with CSP-B. Each such individual would therefore be a Subject.	Replace "subscriber" with 'Subject', throughout
KI-9	63A			491	CSPs or other commercial organizations may only offer one option and should not be required to provide options (although certainly an agency could solicit for a package deal)	~~CSPs and organizations~~ Federal agencies SHALL provide options when implementing their identity proofing services and processes to promote access for applicants with different means, capabilities, and technology access.
KI-10	63A			492 - 494	Any such options would be very difficult to assess - a single alternative, e.g. larger display font, would qualify as an 'option'. This requirement is effectively unenforceable in any qualitative manner.	Replace SHALL with SHOULD.
KI-11	63A			499 - 502	Whilst the intention of the required risk evaluation is understood, such a process is going to be subjective: i) there is no benchmark basis on which to make a comparison (i.e. no understanding of what the 'stated level of certainty' actually is; ii) each CSP will form its own view of risk, which may be more or less rigorous than any other CSP's; iii) an assessor will have no basis for determining whether the risk assessment is reasonable other than a subjective determination that it was based on a methodical / logical approach which would allow repeatability and the same results for a given set of inputs, and that it was reviewed and the outcomes accepted by an appropriately-authorized service-related level of management.	NIST has gone to great lengths over a notable period of time to arrive at the requirements in this draft. There must be some risk-based basis for establishing and publishing these 'stated level of certainty ' requirements which NIST has used in arriving at them and it behooves NIST to publish how these requirements are justified, perhaps as an annex, as a basis on which CSP's can then determine their own comparable assurance. This would provide some kind of comparative basis for CSPs, RPs and assessors (at least). The absence of any sound basis for NIST's postulated requirements is a weakness of this publication.
KI-12	63A	2.1.1	6	529	How is this possible for users who do not already have a record or a presence.	
KI-13	63A			530 - 533	This selection is merely indicative of the fact that the document exhibits inconsistent use of bullets for some lists and indexes for others.	The use of indexed lists in all cases is urged, since the ability to reference a specific point becomes so much easier than stating "third indented bullet of the fifth bullet" or some such clumsy form of words.
KI-14	63A	2.1.1	6	534	For individuals who do not have a presence in records Identity validation is problematic.	
KI-15	63A			556	Is risk based decision the correct phrasing? While all "decisions" are risk based, this phrase was not used in previous versions and could be construed to mean that Proofing Agents are allowed to deviate from their training or procedures. The ability to deviate from procedures would appear to be the intended distinction between Proofing agents and trusted refs and this ambiguity could create confusion.	Proofing Agent - An agent of the CSP who is trained to perform identity proofing, either onsite or remotely, following documented identification procedures, such as visual inspection and data collection.
KI-16	63A			559	It should be noted that the "Trusted Referee" will be a difficult role to implement in the context of a compliance framework like Kantara, with out very specific criteria regarding how they are trained or how they make risk based decisions.	
KI-17	63A			572	It is assumed that notaries would be an applicant reference and representative of the applicant; but if this is not intended, then 63-4 should say so.	
KI-18	63A			572	"Applicant Reference" refers to an object or value, not a person, which is what is defined.	Use the term "Referee" instead

KI-19	63A			611	CSPs or other commercial organizations may only offer one option and should not be required to provide options (although certainly an agency could solicit for a package deal)	Federal agencies ~~CSPs~~ that offer IAL1 & IAL2 services SHALL provide a Remote Unattended identity proofing process and SHALL offer at-least one attended identity proofing process option. (or reference 2.4.2.1)
KI-20	63A			611 - 613	What is the justification for seeking to enforce such requirements? What is the risk mitigation that this achieves? If there is a commercial reason why a CSP should offer a service other than these, be that single or multiple, why should NIST interfere with the operational decisions of federal agencies or the commercial marketplace (which it unavoidably influences, whatever its fundamental remit) in which it has no experience?	Remove this requirement. Let the marketplace decide (noting that, if such a requirement was established many presently-Approved and commercially viable services would fail to meet rev.4)
KI-21	63A			611, 613	Is the "&" inclusive or exclusive??	"and/or" is surely required? But hopefully superseded, given the preceding suggested change.
KI-22	63A			615	Need 'in the event an applicant is unsuccessful with one type' be stated? A CSP could have good reason to allow a transition under some other circumstance and the example given covers such an instance where one type is unsuccessful.	Remove this text - the exemplar serves well enough
KI-23	63A	2.2	9	617	We would advise the extension of core attributes.	There are numerous core attributes that could be included.
KI-24	63A	2.2		622	Use of "SHOULD" here is confusing, as each IAL requires "The CSP SHALL collect all Core Attributes."	
KI-25	63A			624	"if available" or "if used" ? Is there a subtle difference? Middle names are sometimes not used because they are not given and even when given/used, they are not stated (available?), but some forms of document require them to be provided in full when they are given/used.	clarify what is expected
KI-26	63A			628, 630	editorial - "to which" is grammatically incorrect	"at which"
KI-27	63A			629	the colon is a confusing use of punctuation and impedes readability, hence comprehension.	replace the colon with "i.e."
KI-28	63A	2.2		633	Trust agreements are understood to be a component of federation. Requirements for federation should be consolidated in 63C.	
KI-29	63A			662	Very glad to have Appendix A added to the body of 800-63. In the previous version; there were instances where the evidence strength definitions and the evidence example tables did not always align. It is assumed that the table would be "guidance" and evidence show to meet the definitions are valid for the strength. If the intention is otherwise, 63-4 should say so.	
KI-30	63A			662	This section is normative but the appendix is not - it would be worth making that clear in this reference to the appendix	"informative, non-exhaustive, list ..."
KI-31	63A			666 - 668	This requirement assumes or requires a degree of insight into the internal operations of the issuing source which cannot be readily achieved. It may be a fine objective but it does not represent a practical reality. In practice this cannot be reliably proven or established with certitude - e.g. the DoS does not make public its internal processes for issuing passports, and it would be difficult for a CSP in any given country to determine this for what would be an ostensibly valid piece of evidence from another country, nor do the various DL issuers publish their processes. Therefore this is frequently technically unachievable, hence if this is definitively required id-proofing is unachievable for many fundamentally sound forms of id evidences.	A phrasing such as "The CSP has a reasonable and justifiable expectation that the issuing source ..." would require the CSP to justify their expectation: that would hold water with an issuing source such as the DoS, but not with a fast food outlet, e.g.
KI-32	63A			668	The example is very narrow and doesn't help much with fulfilling the requirement	Remove the example
KI-33	63A			674	editorial - mis-indexed	this should be item # 2 - the page break is perhaps interfering
KI-34	63A			674	"SHALL" and "likely" are not good normative companions! Unassessable and likely to lead to philosophical debate	Either require that this be so or remove it altogether
KI-35	63A			679 - 680	A SS card clearly does not meet this requirement. Likewise, how does a TIN (the last time I got an EIN, it was confirmed by email and later by a 'flat' letter - is a TIN allocated by anything more robust?) So this requirement appears to disqualify some potential forms of FAIR evidence.	Remove altogether? Require this or derogate the evidence to being only an acceptable second piece of FAIR evidence? What is the risk mitigation which NIST is trying to achieve with this requirement?
KI-36	63A			683	"verified" is incorrect	replace with "validated"
KI-37	63A			685 & 707	All comments applicable to 2.4.1.1 (and, re. 7070, 2.4.1.2) apply here unless modified/overridden by specific comments below.	Replicate as necessary
KI-38	63A	2.4.1.2	11	688	The first bullet point is confusing. Expand on what is meant here. Further on in bullet 8 you say validation is this supposed to be verification?	
KI-39	63A			688 - 689	How is a CSP to explicitly determine this (or an Assessor, for that matter)? Not only is it unlikely that the (written?) procedures can be reviewed and judged, who defines 'high confidence'?	Remove or re-state in a way which requires CSPs to make a case and for any assessor/evaluator to see a basis for agreement. Admittedly, phrases such as 'generally recognized' or 'reasonable expectation' are not best used in a normative requirement but this could allow the assessing/evaluating body to establish a list of issuing/authoritative/credible sources - perhaps even an RP could do likewise? Note - In its Service Assessment Criteria for -63 rev.3, Kantara deemed it necessary and justifiable to resort to the use of the phrase 'reasonable expectation' to overcome the great difficulty if not impossibility (in most cases) which this requirement presents.
KI-40	63A			689	The phrase "written procedures" is tricky, although it is one of the distinctions between FAIR and STRONG. It is noted that "written procedures" must be assumed. We assume the DMV has procedures for the applicant, but does not release procedures that can be referenced to show they have high confidence that it knows the real-life identity of the subject.	
KI-41	63A			690 - 691	By the same arguments presented elsewhere, how can this be reliably determined? E.g. DoS, DoD, DMVs etc. which issue forms of identity? How is one to establish that the proofing applied by any such body meets IAL2 requirements?	Resolution needs to be aligned with that for the other referenced comment.
KI-42	63A			697 - 698	This wording differs to that used in 2.4.1.1 but omits the inclusion of a facial image, which becomes an absolute requirement - is it NIST's intention that an image cannot satisfy both 4) and 5) ?	Since a facial image would qualify as a required attribute, if it is intended that this may NOT be resolved by using such an attribute that should be stated explicitly, otherwise a facial portrait can legitimately fulfil two needs.
KI-43	63A			717	The requirement to cryptographically validate evidence will make Superior evidence unvalidatable for almost all implementations. (1 STRONG + 1 FAIR will be the near universal implementation for the foreseeable future)	
KI-44	63A			718	NIST has gone to some lengths to use 'validation' and 'verification' for very specific parts of the id proofing process. The use of 'verification' here seems inappropriate (and not following usual PKI practice?).	replace with "authentication"
KI-45	63A			720 - 721	Since specific terms have been created, for the sake of absolute clarity in requirements it would be preferable to be explicit about what "attended" entails or allows.	replace with "in a Remote Attended or an Onsite Attended Proofing process"

KI-46	63A			723	Normative clauses should be limited to being that. Including exemplars leads to potential confusion	Either state emphatically "to a postal address" OR state all acceptable manners of delivery OR leave it unstated.
KI-47	63A	2.4.2.2	13	749	Per our comments related to 2.4.1.1, we propose adding a bullet point in this section that reads: "Geolocation check using a device with appropriate technologies to provide a high level of confidence to associate the location of the individual with an address that is self-asserted or listed on identity evidence."	
KI-48	63A			755	Is this not a validation method which could be listed with the four points above?	Add to the preceding list
KI-49	63A	2.4.2.3		755	The criteria requires the validation of all core attributes described in 2.2. However 2.2 specifically does not require the collection of any attributes, "the following attributes SHOULD be collected by CSPs"	
KI-50	63A	2.4.2.3	13	755	This section poses issues of exclusion for large sections of the community particularly those without permanent addresses or without credit history.	
KI-51	63A			756	If you only SHOULD collect core attributes(2.2), but SHALL validate them, is there a perverse incentive to not collect them at all? This appears to make the collection or validation of attributes completely optional.	
KI-52	63A			756 - 757	editorial - split infinitive	The CSP SHALL validate all core attributes (as described in Sec. 2.2) with an authoritative or credible source (see Sec. 2.4.2.4), whether obtained from identity evidence or self-asserted by the applicant.
KI-53	63A	2.4.2.4	13	759	There seems to be a change in terminology from 800-3 to 800-4 this can lead to confusion. What is authorative and what is credible?	
KI-54	63A	2.4.2.4		761	It is noted that in these definitions AAMVA and maybe the The Social Security Number Verification Service would appear to be the ONLY authoritative source available to CSPs. Repeated mentions of the FCRA suggest that only credit bureaus can at as credible sources. It is unclear the MNO data aggregators would be credible sources, these would be critical for using phones as fair evidence.	
KI-55	63A			761 - 774	as normative criteria these are poorly expressed. 'may also be', 'such as', 'in addition to' and 'Examples of' are not phrases helpful in expressing definitive criteria. This text is more like descriptive terms which would be better used to extend the formal definitions.	Make clear unequivocable statements of requirements.
KI-56	63A			795, 799, 809	Having gone to the trouble of assigning specific terms to specific types of id proofing [see 2.1.3] ...	Could NIST use consistently their own standardised terms
KI-57	63A	2.5.1	15	817	We just wanted to say "thank you" for re-emphasizing that KBV has no place in identity verification.	
KI-58	63A			831	The phrase "practices statement" may have specific connotations exceeding the goal of this criteria	The CSP SHALL conduct its operations according to a documented procedures or practices ~~statement~~ that details all identity proofing processes
KI-59	63A			831	Kantara has adopted the principles of RFC 3647, which makes a distinction between a policy and a practice statement. Whilst accepting that 3647 relates to PKI, the principles it espouses are well-defined and have been observed for decades. It is noted that practice statements frequently disclose operational aspects which the CSP might not wish to have present in a public domain. This may reveal security weaknesses through disclosing practice or exposing features which confer competitive advantage ('specific technologies').	Adopt the practice of separating a Policy/Service Description, and a separate technical document e.g. as a Practice Statement, and require such documents to be produced and maintained by the CSP.
KI-60	63A			831	The stated requirement is to *operate* according to a process, not to *publish* a policy/service description which includes certain contents. This clause is therefore most likely NOT stating what NIST's authors intended, whilst also stating more than is sound advice.	It would be preferable to require that the CSP publishes a Policy/Service Description for general (consumer) consumption, stating the mutual expectations amend obligations of the partipating parties, and to define minimum contents for such a document; and (optionally and quite separately) require what ought to be in a separate technical document as a Practice Statement for internal use, and possible wider disclosure under an NDA, with the requirement that the CSP operates and delivers its service in accordance with this document.
KI-61	63A			885 & 951	The indexed items in these clauses could be better structured (unless there are qualifying cases, but further indexation could accomplish this and make clear the applicability of such).	State all normative (i.e. SHALL) requirements THEN state in order all SHOULD, MAY and CAN stipulations. This principle may be applied in other instances.
KI-62	63A	3.1.2.2	19	951	This is an improvement and good to see.	
KI-63	63A	3.1.2.2	20	963-973	This creates untestable situations and difficult for an assessor to determine compliance. Especially 3.1.2.2	
KI-64	63A	3.1.3.2	22	1028	Limiting PII should be on use case basis depending on need. Using extended PII can have benefits in determining the identity if used correctly. It can still fit the essence of not collecting more than is required.	
KI-65	63A	3.1.5	23	1087	This section should be expanded and consider what a CSP should be expected to collect that can retrospectively be used.	
KI-66	63A			1090 - 1093	The requirement, as stated, is for a single means. Conformity could be achieved with less than what may be adequate, though that assertion begs the question as what may be adequate. Further, it is not clear whether the extensive list of 'acceptable means' is normative or not ... presumably not, because of its non-exhaustive nature.	Two possible solutions: 1) rephrase to require whatever means are identified consequent to a risk assessment … or 2) remove this altogether - wouldn't the broader requirements for risk assessment as required in following items 4 and 5 address this need?
KI-67	63A	3.1.6	24	1105	This section should be expanded. Surely there are expectations on CSPs to proved protection to users.	
KI-68	63A			1118	editorial	insert a comma after 'proofing'
KI-69	63A			1140	editorial	inconsistent style for 'SHALL'
KI-70	63A			1148	Clarify that address and evidence may overlap, but are separate	They ~~are also~~ may also be used as an identity verification option at IALs 1 and 2, as described in Sec. 2.5.1.
KI-71	63A	3.1.11	27-29	1207	This seems to put too much additional consent work on CSPs and is it workable in real life scenarios.	
KI-72	63A			1256	Should a personnel and "manual review" be required or would offering options be sufficient.	CSPs that make use of 1:N biometric matching for either resolution or fraud prevention purposes SHALL NOT decline a user's enrolment without providing other enrolment options. ~~a manual 1257~~ ~~review by a trained proofing agent or trusted referee to confirm the automated 1258~~ ~~matching results and confirm the results are not a false positive identification (for 1259~~ ~~example, twins submitting for different accounts with the same CSP).~~

KI-73	63A			1310	Without a standard format or criteria making data public may result in inconsistent results. Perhaps a specific criteria result format should be specified.	
KI-74	63A			1336	"Certification" of proofers is both a high and ambiguous criteria. Perhaps training and testing should be called for.	Proofing agents and trusted referees SHALL be trained on their ~~reviewed regarding their~~ ability to visually inspect evidence on an ongoing basis, and be assessed ~~and certified with~~ at least annually ~~evaluations~~.
KI-75	63A	3.1.13	31	1340-1352	What guidance should be given for how CSPs consider the 'trustworthiness' of an Applicant Reference.	
KI-76	63A			1437	Trust agreements are understood to be a component of federation and 63C. Criteria regarding their use should be kept in 63C and possible references there (as in line 875)	
KI-77	63A			1509	The types of proofing required would seem to belong to a federal agency or possibly an organization, not a CSP. The requirement for a mandatory unattended option is confusing. Face-to-face would seem like the default; while some form of remote may address equity issues.	
KI-78	63A			1525	The requirement to collect all core attributes conflicts with 2.2 which says CPS SHOULD collect.	
KI-79	63A	4.1.7	38	1568-1593	Shouldn't retention be mandatory for non-repudiation.	
KI-80	63A	4.1.10 & 4.1.11		1621	Could these two sections be switched, just to stay aligned with the other assurance levels.	
KI-81	63A			1655	The types of proofing required would seem to belong to a federal agency or possibly an organization, not a CSP. The requirement for a mandatory unattended option is confusing. Face-to-face would seem like the default; while some form of remote may address equity issues.	2. ~~CSPs~~ Federal Agencies SHALL offer Unattended Remote identity proofing as an option AND .~~ CSPs SHALL offer~~ at least one method of Attended (Remote or Onsite) identity proofing as an option.
KI-82	63A	4.2.4 & 4.3.4		1672	There seems some likelihood that implementations will substitute simple "visual inspection" for "confirming security features," as described in C&D. If "confirming security features" is the goal, the language should make that clear.	
KI-83	63A			1685	The requirement here to cryptographically validate evidence seems as if it will make Superior evidence unvalidatable for most implementations.	
KI-84	63A	4.2.6		1701	The discussion of pathways is informative, but the organization may be awkward. These discussions could be consolidated at 4.2.6, and then the various verification methods presented as simple list.	
KI-85	63A			1715 (and 1741 and 1765)	As written, a visual facial comparison of a single piece of STRONG evidence is sufficient for IAL3 (line 1845); BUT IAL2 requires the STRONG facial compare AND ADDITIONAL verification of a 2nd piece of evidence. Verifying the applicants ownership of the strongest piece of evidence should be sufficient at both IAL2 and IAL3	
KI-86	63A			1720	Appendix A includes verification methods that do not meet these criteria (e.g., "Must be presented with other evidence containing a photo (if there is no image on the card).") If this is an acceptable practice, it must be included in the verification sections; or the verification sections should reference appendix a as acceptable verification methods.	(b) Visually comparing the applicant's facial image to a facial portrait on evidence, or in records associated with the evidence, during either an onsite attended session (in-person with a proofing agent), a remote attended session (live video with a proofing agent), or an asynchronous process (i.e., visual comparison made by a proofing agent at a different time). If there is no image on the card, then visual inspection of the card is sufficient if it is presented with other STRONG evidence containing a photo.
KI-87	63A			1720	Describing comparison of a facial image as "non-biometric" maybe confusing.	
KI-88	63A	4.2.6.3	43	1762-1776	Please clarify what you mean by a "non-facial portrait biometric?"	
KI-89	63A			1799	It is unclear if "One piece of STRONG and one piece of FAIR (or better)," is intended to mean anything different than ""One piece of FAIR and one piece of STRONG as described in 4.2.2. The parenthetical "(or better)" should be removed, unless better evidence is actually not allowed in other instances. FIPS 201 includes a waiver for this criteria, based on a back-ground check. Should that waiver be made standard here?	
KI-90	63A	4.3.2		1802	The requirement to collect ALL core attributes in in conflict with 2.2	
KI-91	63A	4.3.8		1879	It is not clear why a remote agent could not still "have the proofing agent view the source of the collected biometric for the presence of any non-natural materials."?	
KI-92	63A			1925	Use of the phrase "when the setting allows" introduces ambiguity to the applicability. The setting requiring tools should be identified specifically. The typical face-to-face configuration, like a PIV issuance workstation would "allow" tools, but would not typically have any. The tools should be specified - as written.	All attended ~~When the setting allows for it (e.g., onsite attended~~ proofing events ~~), proofing agents and trusted referees~~ SHALL be provided with specialized tools and equipment to support the visual inspection of evidence (e.g., magnifiers, ultraviolet lights, barcode readers).
KI-93	63A	5.2		1958	It is noted that some systems may perform identification and account creation well before the need for a higher level of identification or authentication is required and may not be able to support this.	
KI-94	63A	5.4	51	1971-1990	Isn't there a responsibility on CSPs to inform RPs when there are account changes/status changes. A user could be locked out of an account and need to have that account reinstated quickly.	CSPs SHOULD take action to reinstate compromised accounts as quickly as possible.
KI-95	63A	6	53	1991-2011	Shouldn't this include well known and prevalent attacks such as account takeovers.	
KI-96	63A			2724	editorial	ensure that table headers are repeated on each new page, for readers' convenience.
KI-97	63A			2728	the term 'intended origin' is neither defined nor clear. Is this the new term for 'issuing source'? The latter term would be much clearer. At the least, 'expected source' would be more appropriate since one is looking back to when the document was produced.	use 'issuing source' or if 'intended origin' is somehow different, explain this
KI-98	63A			2730	Shouldn't the ref to a "US Passport" be to a "US e-Passport" ? There will be no PKI Certificate otherwise.	state "US e-Passport"
KI-99	63A	Appendix A	79	2728	Credit and debit cards are listed as acceptable fair evidence, since it's assumed the cardholder's identity was proofed in accordance with KYC/CIP account opening practices and that they can be validated by confirming the physical security features and signature. However, given the existence of prepaid cards, additional users who may not have undergone identity proofing, and initiatives like TD Bank's chosen name feature -- which allows individuals to display a chosen name on their debit or credit card -- these cards should not be considered acceptable evidence. There's no way to tell from the card's face whether the name reflects the person's actual identity or if they were subject to identity proofing.	Allow use of a financial account as fair evidence as querying the account could confirm whether the person is the primary account holder and therefore subject to KYC/CIP account opening practices. But don't allow the use of credit or debit card.

KI-100	63B	2.2		556	This uneven description of passwords vs biometrics as a factor is confusing and suggests an unnecessary distinction between them. Is there any reason to identify a biometric characteristic as not recognized as an authenticator by itself, if it is not identified as approved in the document?. The lengthier biometric discussion could be consolidated in 3.2.3	When a combination of two single-factor authenticators is used, the combination SHALL include a password (Sec. 3.1.1) or a biometric characteristic (Sec. 3.2.3) and one physical authenticator (i.e., "something you have") from the following list: •Look-up secret (Sec. 3.1.2) •Out-of-band device (Sec. 3.1.3) •Single-factor OTP (Sec. 3.1.4) •Single-factor cryptographic authentication (Sec. 3.1.6) ~~A biometric characteristic is not recognized as an authenticator by itself. When biometric 563 authentication meets the requirements in Sec. 3.2.3, a physical authenticator is 564 authenticated along with the biometric.~~ The physical authenticator then serves as "something you have," while the password serves as "something you know" or biometric match serves as "something you are." When a biometric comparison is used as an activation factor for a multi-factor authenticator, the authenticator itself serves as the physical authenticator.
KI-101	63B			605	Unclear.	Single-factor cryptographic authentication (Sec. 3.1.6) used in conjunction with a password (Sec. 3.1.1) or a biometric characteristic (Sec. 3.2.3)
KI-102	63B	2.3.3		626	Should the reauthentication criteria be assigned to the RP? Or is it best left ambiguous?	
KI-103	63B	2.4.3		656	Should this be a condition of the authentication service, since it is 63B, or the service in general?	CSPs SHALL NOT make consent for the additional processing a condition of the ~~identity~~ service.
KI-104	63B	3.1.2.2		833	Use of the term "next" secret implies that only one look-up may be valid at a time. This is not always the implementation. If there is a limit on the number allowed to be valid, then it should be identified	Verifiers of look-up secrets SHALL prompt the claimant for a ~~the next~~ secret ~~from their authenticator or a specific (e.g., numbered) secret~~
KI-105				899	It may be useful to note that this does not apply to confirmation codes used to verify addresses.	Email SHALL NOT be used for out-of-band authentication because it may be vulnerable to: •Accessibility using only a password •Interception in transit or at intermediate mail servers •Rerouting attacks, such as those caused by DNS spoofing (this doe not prohibit the use of confirmation codes to validate email addresses, as described in ...)
KI-106	63B	3.1.3.3		956	Somewhere between 3.1.3.3 and 3.2.9 a stronger SHALL statement is needed. This exception seems to get missed often.	Use of the PSTN for out-of-band verification is restricted as described in this section and SHALL address the requirements of Sec. 3.2.9.
KI-107	63B	3.1.6.1		1106	Passkeys may be used as one factor of a multifactor authentication, as described in 2.2.1 and would be a single factor cryptographic authenticator. As such, then reference to the syncable authenticator appendix B should also be added here.	private or symmetric keys SHALL 1106 be strongly protected against unauthorized disclosure by using access controls that limit 1107 access to the key to only those software components that require access. 1108 Some cryptographic authenticators, referred to as "syncable authenticators," can manage their private keys using a sync fabric (cloud provider). Additional requirements for using syncable authenticators are in Appendix B. External (i.e., non-embedded) cryptographic authenticators SHALL meet the 1109 requirements for connected authenticators in Sec. 3.2.11.
KI-108	63B	3.1.7.1		1146	The criteria is confusing. Is there some other criteria that would demand non-exportability invoking this criteria? (i.e., the "IF" part of this "if-then-shall" statement is unclear)	
KI-109	63B	3.2.2		1211	Throttling limits attempts on an account to 100, but does not identify a next step. It could be concluded that the CSP is now no longer allowed to support a given user. Less severely, perhaps a CSP must reidentify them, or must perform recovery. A next step or options should be called out. It is noted that implementing an attempt count for throttling at the account level is complicated for multifactor implementations, where tracking each factor versus the overall account is intricate.	
KI-110				1812	The criteria may wish to establish a method for determining that a suspended authenticator should be reactivated. A phone call saying, "I found it," may not suffice.	
KI-111	63B	5			Do we need a separate role for this? (Session Manager)	
KI-112		Appendix A	79	2728	Credit and debit cards are listed as acceptable fair evidence, since it's assumed the cardholder's identity was proofed in accordance with KYC/CIP account opening practices and that they can be validated by confirming the physical security features and signature. However, given the existence of prepaid cards, additional users who may not have undergone identity proofing, and initiatives like TD Bank's chosen name feature -- which allows individuals to display a chosen name on their debit or credit card -- these cards should not be considered acceptable evidence. There's no way to tell from the card's face whether the name reflects the person's actual identity or if they were subject to identity proofing.	Allow use of a financial account as fair evidence as querying the account could confirm whether the person is the primary account holder and therefore subject to KYC/CIP account opening practices. But don't allow the use of credit or debit card.