***Email Address of Submitter/POC:*** [redacted]

| Comment # | Publication (Base, 63A, 63B, 63C) | Section | Page # | Line # | Comment (Include rationale for comment) | Suggested Change |
|---|---|---|---|---|---|---|
| ZYG#A.001 | 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. |
| ZYG#A.002 | 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 management service" should be used throughout. |
| ZYG#A.003 | 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 fulfill 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 bureaux and other complex technical capabilities, such as document verification. This should be acknowledged in these documents. | Following the referenced paragraph, add:<br>"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. |
| ZYG#A.004 | 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 funtionality 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.<br>Each such individual would therefore be a Subject. | Replace "subscriber" with 'Subject', throughout |
| ZYG#A.005 | 63A | | | 492 - 494 | While the principle is understood and supported, 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 and so the normative expression is effectively extremely weak. | Replace SHALL with SHOULD. |
| ZYG#A.006 | 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 behoves 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).<br>The absence of any sound basis for NIST's postulated requirements is a weakness of this publication and imposes a difficulty in making consistent assesments. |
| ZYG#A.007 | 63A | | | 530 - 533 | This selection is illustrative 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 (e.g.) "third indented bullet of the fifth bullet" or some such clumsy form of words. Ease and clarity of reference is important in a normative doc, whether the specific text is itself normative or not. |
| ZYG#A.008 | 63A | | | 572 | "Applicant Reference" refers to an object or value, not a person, which is what is defined. | Use the term "[Applicant] Referee" instead |
| ZYG#A.009 | 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. Limit this publication to describing the technical requirements for proofing (and credential management in the broader sense within the suite as a whole) and 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, which would itself be detrimental to the goals of providing assured services). It surely is not NIST's role to define the marketplace. |
| ZYG#A.010 | 63A | | | 611, 613 | Is the "&" inclusive or exclusive?? | "and/or" is surely required? But hopefully superseded, given the preceding suggested change. |
| ZYG#A.011 | 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 unuccessful. Indeed there are agencies deploying services which do not intrinsically follow this requirement | Remove this text - the exemplar serves well enough, if it must be used at all (exemplars in normative clauses should be avoided) |
| ZYG#A.012 | 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 |
| ZYG#A.013 | 63A | | | 628, 630 | editorial - "to which" is grammatically incorrect | "at which" |
| ZYG#A.014 | 63A | | | 629 | the colon is a confusing use of punctuation and impedes readability, hence comprehension. | replace the colon with "i.e." |
| ZYG#A.015 | 63A | | | 662 | This section is normative but the appendix is not - it would be worth making that clear in this referrence to the appendix | "informative, non-exhaustive, list ..." |
| ZYG#A.016 | 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. Worse still, many forms of FAIR evidence which are accepted in principal will not even be recognised by the service provider (be that automated or by a human operator) - e.g. how many lenders are there across the country? How can such a requirement be meaningfully fulfilled? Therefore this is frequently technically unachievable, ergo, 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. Admittedly, this would still leave generally acceptable forms of FAIR evidence as being less than absolutely certain, at best. |
| ZYG#A.017 | 63A | | | 668 | The example is very narrow and doesn't help much with fulfilling the requirement | Remove the example |
| ZYG#A.018 | 63A | | | 674 | editorial - mis-indexed | this should be item # 2 - the page break is perhaps interfering |
| ZYG#A.019 | 63A | | | 674 | "SHALL" and "likely" are not good normative companions ! Unassessable and likely to lead to philosphical debate | Either rephrase so as to require that this be so or state a condition which can be reasonably justified, or remove it altogether |

| | | | | | | |
|---|---|---|---|---|---|---|
| ZYG#A.020 | 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? |
| ZYG#A.021 | 63A | | | 683 | editorial - "verified" is incorrect | replace with "validated" |
| ZYG#A.022 | 63A | | | 685 & 707 | All comments applicable to 2.4.1.1 (and, re.line 707, 2.4.1.2) apply here unless modified/overridden by specific comments below. | Replicate as necessary |
| ZYG#A.023 | 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?<br>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. |
| ZYG#A.024 | 63A | | | 690 - 691 | By the same arguments presented in ZYG#A.023, 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. |
| ZYG#A.025 | 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 fulfill two needs. |
| ZYG#A.026 | 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 terminology?). | replace " validated through verification of a digital signature applied" with "authenticated" |
| ZYG#A.027 | 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" |
| ZYG#A.028 | 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. |
| ZYG#A.029 | 63A | | | 755 | Is this not a validation method which could be listed with the four points above? | Add to the preceding list |
| ZYG#A.030 | 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. |
| ZYG#A.031 | 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. |
| ZYG#A.032 | 63A | | | 795, 799, 809 | Further inconsistent use of naming terminology. | Use a single distinct term in each instance of a reference to a distinct proofing type. |
| | 63A | | | 831 | The stated requirement is to "conduct its operations according to a practice statement", 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. | 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. |
| ZYG#A.033 | 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.<br>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'). | It would be prefereable to require that the CSP publishes a Policy/Service Description for general (consumer) consumption, stating the mutual expectations and obligations of the partipating parties, and to define minimum contents for such a document; and<br>(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. |
| ZYG#A.034 | 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). | For the sake of conveying the gravity of the requirements, state all normative (i.e. SHALL) requirements THEN state in order all SHOULD, MAY and CAN stipulations.<br>This principle may be applied in other instances. |
| ZYG#A.035 | 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:<br>1) rephrase to requre whatever means are identified consequent to a isk assessment ... or<br>2) remove this altogether - wouldn't the broader requirements for risk assessment as required in following items 4 and 5 address this need? |
| ZYG#A.036 | 63A | | | 1509 - 1510 | Consistency of terms ought to be paramount in a standards body - 2.1.3 defines Remote Unattended. Which should it be. Ditto (Remote or Onsite) Attended. | Review throughout for consistent use of a single defined term for each type. |
| ZYG#A.037 | 63A | | | 1509 - 1510 | Notwithstanding ZYG#A.036, these two clauses should be removed, since it is not NIST's place to dictate how the market shapes itself. | Remove - consider offering the thought in an informative annex intended to assist agencies in the selectin of CSPs and in the provision (on the agencies' behalf) of a desirable range of services overall. 'Parallel' clauses at other IALs should be treated likewise. |
| ZYG#A.038 | 63A | | | 2728 | editorial | ensure that table headers are repeated on each new page, for readers' convenience. |
| ZYG#A.039 | 63A | | | 2728 | re. Table 4: the term 'intended origin' is neither defined nor clear. Is this the new term for 'issuing source'? The latter term would be much clearer. In fact '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 |
| | 63A | | | 2729 | Shouldn't this table include a "US Passport" (i.e. a 'non-ePassport') | state "US e-Passport" unless it is known that all non-e passports have by now expired IF UNEXPIRED passports are required. Consider also, ANY passport can qualify under this table, e.g. an e-Passport which cannot be authenticated is just another passport. And why not Foreign passports, at the least if they can be authenticated. 'US persons' might not have a US passport. |
| ZYG#A.040 | 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" |
| ZYG#A.041 | 63A | | | 2820 | why is "high confidence" required by this definition - isn't confidence a function of the rigour applied at a specific IAL? | remove the subjective qualification |

| | | | | | | |
|---|---|---|---|---|---|---|
| ZYG#A.043 | 63A | | | 2822 | "An issuing source may also be an authoritative source" creates a circular defintion, which is not definitive | remove this sentence |