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

Please submit responses to dig-comments@nist.gov by March 24, 2023

Organization:	*Zygma Inc.*
Name of Submitter/POC:	*Richard G. WILSHER*
Email Address of Submitter/POC:	[REMOVED]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
	63-Base	Whole doc / set	0	0	This document (indeed, the complete box-set) is presented in very contradictory ways, most obviously in the Abstract ("These guidelines provide technical requirements ..." [!!]) and in §1 ("This publication [provides] technical guidelines ...", "This document provides requirements ..."). Not only is the terminology inconsistent, the idea of requirements is that they define something that one has to do, whereas guidance is purely informational. So where does NIST stand? It is noted that the main body of the work contains a mix of informative material and presumably normative material which uses the specific capitalized key word 'SHALL', 'SHOULD' and 'MAY', the intent of which, I think one can reasonably assume, is to take on the meanings imparted to these words by RFC 2119, a document very widely adopted amongst SDOs. This dichotomy SHOULD be resolved.	Amend the title to be "Digital Identity Requirements" and make the necessary changes to the while document (set) to reflect this change to stae clearly that the document defines [normative] requirements [using key words as defined in RFC 2119] whilst providing supporting, explanatory and informative guidance. Implicit in this suggested change is that all references throughout the document to 'guidance' need to be reviewed to determine whether ther truly informative as opposed to being normative requirements.
	63-Base	Whole doc / set	0	0	The structure of the document does not lend itself to easy determination of: a) which clauses are actually expressing normative requirements; and b) what are discrete normative requirements. This is evidenced by no consistency in style regarding whether informative discussion precedes normative requirements and by single paragraphs which bear both normative and informative text. This weakens the utility of the document [set] in either its use as an educational/informative source or as a set of formal requirements.	1 - Express each normative requirement as a distinct clause; 2 - Give each such clause a unique reference; 3 - Give the user a very clear means to determine the status of a passage of text - i.e. exclusively normative or informative. It is noted that adopting a presentational distinction would be an easier solution to achieving much greater presentational clarity than trying to extract and regroup all passages of one type or another.
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					

	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					
	63-Base					

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Including rationale for comment)	Suggested Change
ZYG-A#001	63A	Whole doc / set	0	0	This document (indeed, the complete box-set) is presented in very contradictory ways, most obviously in the Abstract ("These guidelines provide technical requirements ..." [!!]) and in §1 ("This publication [provides] technical guidelines ...", "This document provides requirements ..."). It has potential to confuse implementors and users (in the broadest sense). Not only is the terminology inconsistent, the idea of requirements is that they define something that one has to do, whereas guidance is purely informational, to be taken or ignored at will and without consequence. So where does NIST stand? It is noted that the main body of the work contains a mix of informative material and presumably normative material which uses the specific capitalized key words 'SHALL', 'SHOULD' and 'MAY' in a very specific style of presentation, the intent of which, it seems one can reasonably assume, is to take on the meanings imparted to these words by RFC 2119, a practice very widely adopted amongst SDOs (see also ISO Directives Part 2 App.H). This dichotomy SHOULD be resolved.	Amend the title to be "Digital Identity Requirements" and make the necessary changes to the whole document (set) to reflect this change to state clearly that the document defines [normative] requirements [using key words as defined in RFC 2119] whilst providing supporting, explanatory and informative guidance. Implicit in this suggested change is that all references throughout the document to 'guidance' need to be reviewed to determine whether they are truly informative as opposed to being actual normative requirements.
ZYG-A#002	63A	Whole doc / set	0	0	The structure of the document does not lend itself to easy determination of: a) which clauses are actually expressing normative requirements (within informative text); and b) what are discrete normative requirements. This is evidenced by no consistency in style regarding whether informative discussion precedes normative requirements and by single paragraphs which bear both normative and informative text (e.g. para commencing line 611). This weakens the utility of the document [set] in either its use as an educational/informative source or as a set of formal requirements.	1 - Express each normative requirement as a distinct clause; 2 - Give each such clause a unique reference; 3 - Give the user a very clear means to determine the status of a passage of text - i.e. exclusively normative or informative. It is noted that adopting a presentational distinction (e.g. different indentation, different font, ...) would be an easier solution to achieving much greater presentational clarity than trying to extract and regroup all passages of one type or another.
ZYG-A#003	63A	Whole doc	0	0	The terminology used to refer to various types of proofing is overly simplistic, confusing and inconsistent. Though it is appreciated that there is good reason to allow developers and service providers scope for innovation, there is a set of proofing types which can and should be defined at the level of abstraction a standard should address.	A proposed taxonomy and associated definitions are provided in tabs 'Proofing Type Taxonomy' and 'Proofing Definitions'. These should be inserted as a new §2.2 'Identity Proofing Types'. Adopt the proposed taxonomy and use the defined terms or their abbreviations very deliberately and specifically for each normative clause. This will serve to remove from the start a considerable scope for confusion in implementation and in assessment/audit/evaluation. EACH reference to a proofing type needs to be reviewed and in almost all cases replaced with the appropriate term from the taxonomy. I have not sought to call out all of them - there are far too MANY. NOTE 1 - as a draft submission the referenced taxonomy has explanatory notes intended to explain/justify the chosen terms. It is not intended that these explanatory notes be retained for publication, unless NIST see merit in doing so. NOTE 2 - while the terms used make sense to the proposer there may me better terms worthy of consideration. The primary point is that a clear taxonomy with readily understood and non-conflicting/confusing terms be established and consistently used. NOTE 3 - given better-defined types of proofing, the authors may feel that they can relax, or perhaps feel the need to enhance, the evidentiary requirements, on eras or at the attribute level, according to both type and IAL
ZYG-A#004	63A	Whole doc / set	0	0	With relevance to comment ZYG-A#002, it is difficult to make a discrete reference to any part of these documents when they either: 1 - use bulleted lists, not those indexed (e.g.); or 2 - within any given clause, the numbering of indexed lists within different paragraphs is reset for each list, rather than continuing the numbering within the specific clause (e.g. §5.1.8)	Do NOT use bulleted lists; Always use indexed lists. Always continue numbering of indexed list elements within a distinct parent clause, do NOT restart each list where multiple paragraphs within the same parent clause have such lists. Furthermore, consider the choice of indexing sequences: taking 5.1.2.1 as an example, which has two levels of indexation, consider lower-case alphabetic indexing for the first level, numbers for the second. Thus, rather than §5.1.2.1 1) a), one would refer to 5.1.2.1 a) 1). The benefit of this is that it avoids confusion / error when referring to (e.g.) 3.2.1 and 3.2.1). If that was confusing then I rest my case.
ZYG-A#005	63A	Whole doc / set	0	0	From experience of detail review of 63A comes the point that a question that will arise is "So what is actually different between each xAL?". As presented, this is not at all readily determined from reading the text. E.g. §5.3.1 (IAL1), §5.4.1 (IAL2), §5.5.1 (IAL3) have identical text. Why need this be repeated, rather than stated once in a section which addresses common proofing requirements? Yes, Table 1 gives a summary, but it is only that and, e.g., does not address the example just given. The detail is in the text and it is that to which anyone with a serious interest is going to have to refer. See tab 'IAL compn'.	Help implementers, operators, agencies, consumers (Subjects and RPs), certification bodies, assessors/auditors, etc. get an easy read into what are the incremental changes between xALs by stating these clearly and distinctly. Equally, where there is no change but some imperative reason to retain a discrete clause (perhaps for reasons of discrete headings, e.g. 5.4.4 vs. 5.5.4 - see ZYG-A#063)
ZYG-A#006	63A	Whole doc / set	0	0	Notwithstanding suggestions to replace 'subject' with 'subscriber', in order to ensure internal consistency and also in keeping with the usage of the drafts as presented, where a single entity appears to be uniquely intended (as opposed to the word being interpreted with the broad definition which is offered) it is noted that whereas the NIST set of documents refers to a 'Subscriber' seemingly as a sole person, other standards (e.g. ISO?, EN, Kantara) differentiate between a Subscriber and a Subject, as follows: Subscriber: a party that has entered into an agreement to use a «Proofing / Credential / other trusted» Service; Subject: an Applicant which has had its Identity proven [and potentially bound to a credential]. The notion here is that a Subscriber could be an organization which subscribes to a service provider for the provision of proofing / authentication / verifier services for the organizations specific community of (potential) subjects. The NIST definitions reverse the relationship between the two terms, which creates conflict when 'subject' alone is used.	Amend the definitions as now given and replace all instances of 'subscriber' with 'subject' (taking care not to eliminate the frequent instances of 'subject' in its natural sense. This will resolve to a consistent usage. As a recommendation in this specific instance but recommended across the whole suite of documents is that defined terms should be set in a capitalized form. This makes clear the intention that the word or term is being applied with the specific context of its definition. This also delineates between words (such as subject/Subject) which may be used in their natural language sense(s).
ZYG-A#007	63A	Acknowledgments	14	343 - 346	There has been notable interaction with Kantara pre-publication of -63 rev.4 DRAFT and since, and it is noted that concepts developed by Kantara in creating its own criteria against (especially with regard to federation) which to have assessments performed have now been adopted in rev.4. Recognition of this would be appropriate.	Add Kantara Initiative to line 346
ZYG-A#008				426	This (and all other such instances) is not an accurate statement - the section is not entirely normative	Amend to "This section includes normative clauses"
ZYG-A#009	63A			427	typo	this section provides an overview ...
ZYG-A#010	63A			434	value of the data to whom?	better to state "value which a successful attacker might gain" ?
ZYG-A#011	63A			438	what does it mean to 'enable optionality', and is that the same as 'providing options'? Enabling and providing are not the same.	Please explain this phrase or amend the text to be more explanatory
ZYG-A#012	63A			443	'multiple channels for engagement' seems rather flowery.	It would be more direct to say "multiple proofing types (see §2.2)"
ZYG-A#013	63A			451	grammar	"certainty, that the applicant"
ZYG-A#014	63A			494	word choice	Better to say "identity proofing process", not transaction
ZYG-A#015	63A			497	word choice	Better to say "determine whether it is ...", not transaction

ZYG-A#016	63A			503	the CSP may not have the capability to accept any piece of evidence but may state specific forms which are acceptable to it. This may depend upon the xAL, jurisdiction, ...	Better to "presentation of acceptable identity evidence " And, incidentally, these two numbered points would be better set out on their own lines.
ZYG-A#017	63A			539	typo	"accessible to the intended person"
ZYG-A#018	63A			570	I find "high likelihood" to be very difficult to determine even without the 'high'. It makes me more uncomfortable than the preceding 'reasonable belief'. Whereas the term likelihood is not well-defined I feel I could more readily justify a rational argument for having a reasonable belief.	Use the same phraseology here
ZYG-A#019	63A			574	"a facial portrait or other biometric characteristic" seems to be slightly weird wording: could it be a painting, or must it be a photographic/digital image? And why make a case of the facial representation at all? Is there a deliberate distancing of facial images from other biometrics (as seems to be at places implied in the present published revision)?	simply require "a biometric characteristic" or explain whatever subtle difference there is in the mind of the author(s) between a facial image and any other bio characteristic.
ZYG-A#020	63A			603	text structure	state "by confirming" and remove 'confirming' from each of the three following points (and see also ZYG-A#004)
ZYG-A#021	63A	4.3.4.3		620 -628	The text mixes manners of validation with proofing types.	After embedding a proofing taxonomy this can hopefully be made much clearer
ZYG-A#022	63A	4.3.4.3		622, 623	Here we have 'trained personnel' The definition of IAL3 uses ' trained CSP representative ' In 4.4.1 we have 'CSP operator'. If these are essentially the same role then a single label would be much clearer - if they are not the same role then something needs to be done to describe the differences between them, consistently use differential terms, and when one might apply vs. any other(s).	For the sake of consistency and therefore reducing potential confusion amongst implementers and possibly auditors/assessors, a single phrase would be helpful. The term 'Supervisor' (as used in 63 rev.3) would seem sufficient, if defined in a manner which imparts the need that they be trained, competent and efficient.
ZYG-A#023	63A	4.3.4.4		633 - 646	It is unclear whether this is informative or trying to set limitations, i.e. it is pseudo-normative. Better to be clear, if this is essentially trying to place limitations on how a CSP may consider an entity to be authoritative.	Modify line 634/635 to state: "A CSP SHALL only consider a source to be authoritative if it:" Modify line 642 to commence "Has collected ..." (for grammatical correctness)
ZYG-A#024	63A	4.3.4.4		647 - 654	The same argument as ZYG-A#023	Modify line 634/635 to state: "A CSP SHALL only consider a source to be credible if it:"
ZYG-A#025	63A	4.4.1		659	This whole section is confusing. It seems to be pseudo-normative since it appears to be setting conditions on how proofing should/may be performed and it seems to be making such determinations based on proofing type (which itself sorely needs clarification and resolution), yet there are no normative key words. If these ideas are important should they not be expressed normatively? If the following normative sections do actually enforce these points then need they be set out here? Oh, and bullet points ...	The only meaningful suggestion is "decide which way to play this". State normatively in appropriate places and remove from here seems best.
ZYG-A#026	63A	4.4.1		682, 683	As a specific case of the point made in ZYG-A#025, this is the sole instance of the phrase "mathematical algorithm", so where is this normatively asserted?	Resolution should be accommodated by fixing the bigger picture, per ZYG-A#025
ZYG-A#027	63A	5.1.1.1		724 - 731	This clause confuses the CSP as an entity (points 1 and 3) and its service (point 2).	The requirement actually needs to address both circumstances, i.e. cessation of the CSP's service per se, and cessation of the service because of the CSP's demise or whatever.
ZYG-A#028	63A	5.1.1.1		730, 731	This clause has nothing to do with ceasing operations, it stands at any time the CSP is in operation. It is certainly made more pertinent if the CSP is ceasing or has ceased operations (circumstances may not allow for a graceful degradation of the service).	Place this requirement elsewhere, where it will relate to ongoing operation. Point 1 appears to deal with the end of life for the CSP (or at least its service).
ZYG-A#029	63A	5.1.2.1		757	unnecessary repetition or separation?	Remove - this is covered by §5.1.1.1 2)
ZYG-A#030	63A	5.1.2.1		762	an obligation to consult is very hard to enforce or audit in any meaningful way, Consulting may result in no action or a multitude of actions, but there is no normative basis to determine a pass or fail.	Replace SHALL with SHOULD or state concrete and measurable requirements.
ZYG-A#031	63A			869, 870	this is first use of ' validated address' - what makes any of these addresses 'validated' as opposed to 'run of the mill'? Can a CSP validate an address themselves or is it implicitly confirmed by another source? Perhaps this US gov site gives an answer? Thank you for completing your request for a Respondent Portal account! To complete the registration process, you must validate your email address. An email has been sent to [redacted] Please check your email and follow the instructions to validate your email address. You will then be able to sign in to the Respondent Portal.	Explain 'validated express' in a concise and subsequently validatable manner
ZYG-A#032	63A			880	From these times, one has to presume that an enrollment code is not considered as something which binds an Applicant to a Supervised (In-person) proofing session? If that were intended then these times are not practical if the means of communicating the code is electronic (c) or d)).	Clarify this point.
ZYG-A#033	63A			895	exemplars have already been given - need they be repeated? Though, this does suggest that a definition of ' validated address ' is required.	Resolve with ZYG-A#031
ZYG-A#034	63A			943	shouldn't this be qualified - it may not be in the power of the CSP to publish the results achieved by third parties?	Amend to read: 'If the CSP performs its own performance and operational tests, it SHALL make them all publicly available" Ditto 11.
ZYG-A#035	63A			943	Might this be construed as potentially impeding a competitive advantage? If minima were established then assessment could ensure that they were met without compromising any features of a service's advantage.	'all performance' should expressly exclude the internal functioning of algorithms, capture mechanisms, etc. Better to state the minimal characteristics which need to be published, e.g. FMRs, etc.
ZYG-A#036	63A			953	is this unsupervised or supervised (remote) or supervised (in-person), or ... ? Just an instance of uncertainty as to which proofing type(s) actually relate to this reqt.	ZYG-A#003 should help resolve this.
ZYG-A#037	63A			960	enhancement to phrasing	"promote equality of access"
ZYG-A#038	63A			993, 1003, 1013	It has already been stated that this section includes normative clauses and normative key words are used in these sections. Is the word 'Requirements' actually necessary (and in other such instances) in a document having the defined scope? Maybe this is emblematic of the confusion between requirements which are published as guidance, and the parts which are informative and hence guidance?	This is not a consistently-applied titling practice, so remove the word 'Requirement'. See also ZYG-A#002
ZYG-A#039	63A			994	What is it that makes a Trusted Referee different from the personnel referred-to in (see ZYG-A#022)? These persons are actually not acting as referees, they do not know the Applicant - they ARE acting in a Supervisory function, so let's call them that.	Deal with the requirements for Supervisors in a single place. Avoid 'Trusted Referee'.
ZYG-A#040	63A			994 - 996	The requirement to 'provide an option' demands that the capability be there, and that it is the service user who exercises the option to use that facility or not. Yet line 996 says "WHERE this is offered", so apparently the provision is not mandatory. One has to ask why this is seemingly being forced upon CSPs?	Modify 994 to state "CSPs SHOULD provide Supervisors for Supervised (Remote) proofing at IAL1 and IAL2". The rest then flows.
ZYG-A#042	63A			999 - 1000	Shouldn't this ability to make 'risk-based' decisions require that the net risk is the same ... and are these persons really going to be able to make such decisions. I understand why this is here, but it seems to be a potential weakness, a diminution of the level of risk associated with the proofing process, unless very clear requirements are given.	It would be far better to: a) phrase this so as to allow Supervisors to make decisions based upon a clear framework of optional paths open to them; and b) require the CSP to develop such a framework (which would allows a more uniform and sophisticated risk-based approach to be determined and more uniformly applied).

ZYG-A#042	63A			999 - 1000	Notwithstanding the comment above, this is all very well but adopts a slightly too happy a path ...	Supervisors should be trained equally to detect attempts to fraudulently pass through the proofing process
ZYG-A#043	63A			1024 - 1030	It seems a bit late in the doc to be stating this (even if one had no problem with it) because there have already been references to types of proofing. Further, the bulleted points are not using previously-used terms, so even if their descriptive qualities were good, they cannot be readily matched to the labels used thus far. And of course, a better taxonomy is proposed (see ZYG-A#003).	Remove the entire section 5.2 - implementing the suggestions from ZYG-A#003 will render this nugatory, the essence of it will have been already addressed and appropriate terms used.
ZYG-A#044	63A			1032	this appears to use 'IAL3 Supervised Remote' as a title of a proofing type. The need to prefix with the IAL reference shouldn't be necessary - the section addressing IAL3 proofing requirements ought to make the necessary distinction between such a type at this level versus at any other level (for the sme type).	Since ZYG-A#043 suggests removal of this entire section no text-specific suggested need be made, BUT pls note that describing proofing types needs no 'IAL - exclusive' labeling - let the definition of specific requirements per type and per IAL do that.
ZYG-A#045	63A			1035, 1090, 1142	I.e. all three sections addressing requirements at IAL1, 2 and 3 respectively. This may be an overly simplistic question, but in terms of permissible evidentiary sources, why not simply cite the I-9 list of acceptable documents (ignoring the employment aspects) and relate to the PRIMARY and SECONDARY documents therein? If it's good enough for the FBI, ... ?	Cite the I-9 list of acceptable documents (ignoring the employment aspects and presumably relating PRIMARY/STRONG and SECONDARY/FAIR) as being acceptable by default and require CSPs to make a risk-based decision to use/accept any other form of identity evidence by documenting the equivalent or greater strength of any other sources.
ZYG-A#046	63A			1035, 1090, 1142	I.e. all three sections addressing requirements at IAL1, 2 and 3 respectively. Let's just assume any refs to proofing types are addressed by ZYG-A#003?	See ZYG-A#003.
ZYG-A#047	63A			1039	typo	"false negatives and applicant departures "
ZYG-A#048	63A			1044	redundant text	remove "CSPs providing" - that should be quite explicit
ZYG-A#049	63A			1046 - 1050	This clause has little normative quality. A 'means' could be anything, and no extent of rigor is implied nor can be expected. The list of acceptable means is not helpful since nothing invokes consideration of its contents and is almost deprecated by the phrase 'not limited to'. This comment relates to the same clause at each IAL.	If you think having such means is important, relate the requirement to a risk assessment, and since you invoke 800-53 elsewhere why not relate to that and to system categorization? Furthermore, since this section is one of those simply re-stated without change for each IAL, put it somewhere else which addresses risk assessment/mitigation.
ZYG-A#050	63A			1057 - 1060	This also has limited normative value - as a 'MAY', it will be largely ignored and cannot be assessed. This comment relates to the same clause at each IAL.	It (and its peers) would be better moved to a place where it would be simply informative.
ZYG-A#051	63A			1061	What are 'Core Attributes' - I understand that they might be something that an observer would recognize when they see them but different observers may not agree ...	... so this terms needs to be defined / described
ZYG-A#052	63A			1068 - 1069	This clause will not be feasible for Unsupervised proofing (of any kind) - hopefully by definition	Qualify it as "When performing Supervised proofing of any type the CSP SHALL ..."
ZYG-A#053	63A			1068 - 1069	are these 'trained personnel' not in fact ...	Supervisors?
ZYG-A#054	63A			1076	The phrase "For added assurance," is pure decoration - the fact that it is a normative clause is all that matters.	Remove said phrase, including any other same or similar instances
ZYG-A#055	63A			1084 - 1085	I don't see what this achieves (I guess I'm missing a piece of the plot): wouldn't either of these mechanisms require an IAL1 (or higher) proofing in the first place?	Justify this provision
ZYG-A#056	63A			1086	typo	"see Sec 5.1.6"
ZYG-A#057	63A			1106	1 x STRONG + 1 x FAIR appears to have dropped a second FAIR requirement from rev.3. This illustrates the lack of any published risk assessment which might justify this change, which could arguably be a weakening of the required rigor.	It would be very constructive and illuminating if NIST would put forward some concrete justification for any of its normative requirements for strength of evidence, both for the present draft and for the current revision. It is very difficult to make any judgements on these requirements, or indeed for comparable alternatives (where agencies are permitted to go down that path) since there is no stated risk quantification against which any determination of comparison or comparability can be made.
ZYG-A#058	63A			1117 - 1118	What happened to validation of FAIR evidence? Is it no longer required or is it meant to be embraced by this phrase??	If FAIR evidence is indeed intended to be included, be specific: "The CSP SHALL validate the core attributes from all pieces of evidence at all strengths collected by". If it is not then state explicitly what strengths are to be addressed.
ZYG-A#059	63A			1147	Notwithstanding prior intent not to raise matters of proofing type terminology, the notion of 'in-person' including 'remote' is very confusing.	See ZYG-A#003.
ZYG-A#060	63A			1157, 1159	If elements 1) and 2) are alternatives is it not reasonable for one to assume that they counter the same risk (whatever that may be)? Therefore, they must be equivalent, hence 2 x SUPERIOR = SUPERIOR + STRONG and so by deduction SUPERIOR = STRONG. Therefore, by this deduction, isn't the third element actually the more rigorous by wording alone, being equivalent to 2 x SUPERIOR + FAIR?	Apply strength requirements which create a genuine distinction which relies on greater rigor.
ZYG-A#061	63A			1164	Section titling (of this and subordinate heading phrasing) differs from its IAL1 and 2 peers, for no apparent reason (other than editing oversight?)	Apply same heading to each clause addressing the same scope/subject material?
ZYG-A#062	63A			1180, 1181	Basically item 2) is saying "same as above", right? It is unclear why crypto features are specifically pointed-out , since they would (at least theoretically) be considered to be core attributes ... but this term is not defined, so therefore this is a subtle pointer to crypto features being a core attribute?	See ZYG-A#051
ZYG-A#063	63A			1184	A great case of repetition when maybe there's a simpler solution?	State only "The requirements stated in §5.4.4.1 apply."
ZYG-A#064	63A			1200 - 1202	"An in-person interaction between the applicant and a CSP operator" - so Supervised (In-person) proofing? "A remote interaction with the applicant, supervised by an operator" - so Supervised (Remote) [and does it matter whether the CSP's or the User's hardware/firmware is employed?] Additionally, why is the phrasing emphasized in red different in each bulleted item? Is there intended to be some subtle difference or is it just inattention to using consistent terms in a consistent manner? It seems that in each case a Supervisor would have to be employed and the use of agreed taxonomic proofing titles would be hugely beneficial	Re-state in accordance with changes to adopt a proofing type taxonomy, define and adhere to the term 'Supervisor' and remove bullets.
ZYG-A#065	63A			1214 - 1216	Exemplar in normative statement	Remove - possibly include as a note.
ZYG-A#066	63A			1217, 1218	points 1) and 2) appear to address the same requirement, just with different phrasing (e.g. does it matter if it is 'the CSP' or 'live operator'? Consistent with other comments, 'Supervisor' would appear to be the appropriate term.	Resolve to a single clause
ZYG-A#067	63A			1237	This may not be the place to express such a requirement but there should also be a unique id for the service - where is that required, and is that unique for the broad service or does it have xAL/policy qualifiers? This becomes relevant for AAL and FAL but the need for uniqueness of the identity-proofing service, or at least that which binds the id to its credentials, is necessary	Create at an appropriate point (possibly NOT in this document) a requirement to the effect of: "The CSP SHALL assign a unique identifier to each discrete proofing service which it operates, including any specific policy identifiers where these are pertinent to the use of the identity."
ZYG-A#068	63A			1257	This is quite vague and hence open to interpretation and thus leading to inconsistent implementations and pain for assessors. E.g. is it sufficient to record 'DL' in each case ("Yes, we used a DL, we validated the DL") or must it go to the level of discrete info fields from each piece of identity evidence?	At the least, minima should be specified to the extent possible - issuing authy, iss athy's unique evidence ident, account ref., ... (depending on source)
ZYG-A#069	63A			1268, 1269	If this refers to the account maintained by the CSP does this not imply that the CSP maintaining this info also provides the authentication? What if not - it could be another authorized CSP seeking this access obo the subject.	Resolve

ZYG-A#070	63A			1274, 1275	Redundant - already stated in §6.1	Remove
ZYG-A#071	63A			1234	Table 1 - first row - 'Presence': this is confusing, not least because of the inconsistent terminology of the preceding text, as noted in prior comments concerning the need for clarity on proofing types.	Explicitly state the permitted proofing types (headings in bold): Requirement: Proofing type IAL1: Unsupervised OR Supervised (Remote) OR Supervised (Co-located) IAL2: Same as IAL1 IAL3: Supervised (Remote) OR Supervised (Co-located)
ZYG-A#072	63A			1234	Table 1 - a consideration in establishing a proofing capability apart from the proofing type could be the technology involved - its specific performance, how it is configured, perhaps how it is physically protected, etc. This is not adequately brought out in the text, and should be both addressed and therefore included in this table.	Explicitly state the applicable technology by inserting a new row into the table (as row 2) (headings in bold): Requirement: Supervised Remote IAL1: No stipulation IAL2: Same as IAL1 IAL3: Controlled environment This topic needs to be addressed in detail in each IAL section in §5.
ZYG-A#073	63A			1234	Some entries in this standard are repeated for any given requirement but one has to read the full text to determine whether they are actually the same. A more obvious appreciation of the same requirement could be determined if a simple statement to that effect were given.	Where the requirement for any given IAL is the same as the preceding IAL, simply state so, i.e. "Same as IALx". This actually makes it much easier to review and appreciate this quality, rather than comparing two paragraphs of text. As noted, this practice should also be applied in the body of the text.
ZYG-A#074	63A	Whole doc / set	0	0	FAQs. PLEASE DO NOT publish the new rev.4 and then provide a list of FAQs. Clearly, if the document has not been long-published then the likelihood is that no-one has actually asked these questions once, never mind 'frequently'. The honest truth about FAQs is that they are an admission that their subject points were inadequately or insufficiently addressed and explained in the source material.	Best if these 'proto-FAQs' are addressed and resolved during the editing, leading to a much more 'fit for purpose' product.

PROOFING TYPE TAXONOMY

Proofing Type	
UNSUPERVISED	
SUPERVISED	**REMOTE PROOFING**
	CO-LOCATED PROOFING

PROOFING TYPE DEFINITIONS

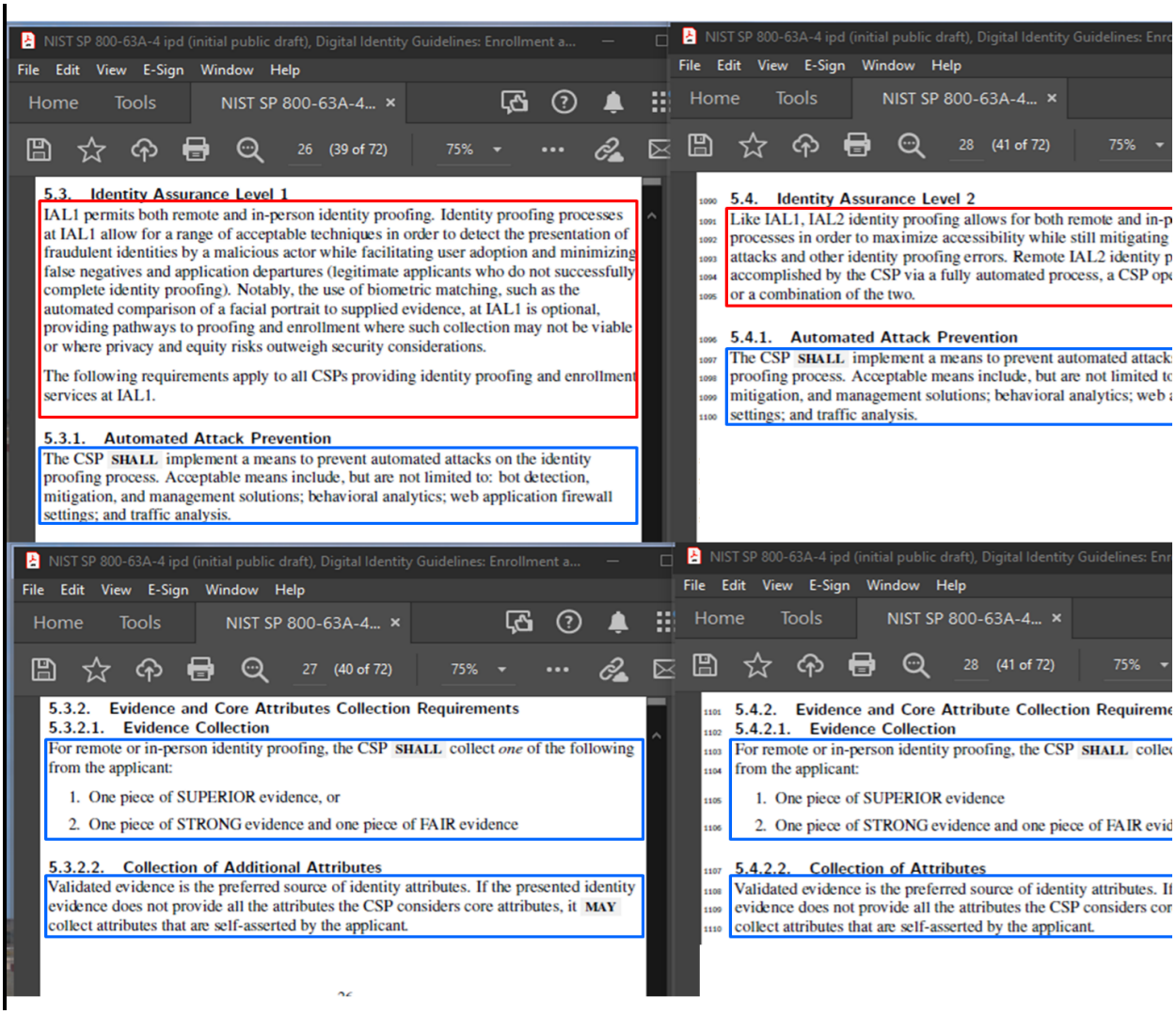
Term	***Definition***
Unsupervised Proofing	Proofing performed exclusively
Supervised Proofing	Proofing which demands huma
Supervised (Remote) Proofing	Proofing which uses telecomm
Supervised (Co-located) Proofing	Proofing at which a human Sup and participation in the process
Hybrid Proofing	A combination of any of the pre
NOTES	*1 - 'Proofing' is used as a conve*
	2 - 'Proofing type' is used as a

Definition
Proofing performed exclusively automatically, without any human supervisory interaction.
Proofing which uses telecommunications to permit/support human Supervisory oversight of and participation in the proofing process.
Proofing at which a human Supervisor has direct physical oversight of and participation in the process.

automatically, without any human
n Supervisory interaction.
unications to permit/support human
ervisor has direct physical oversight of
s.
eviously-defined Proofing Types which is

enient term to mean 'identity proofing',
convenient term to refer to one or more

The following images show in three columns 63A rev.4 reqts for IAL1, 2 & 3 left to right respectiv
adjacent IAL, red boxes show where the requirement differs from that in at least one adjacent IA
clear what changes and what does not change by stating words to the effect of "The requiremen
a given section is explicitly titled being applicable to IALn at some superior heading level then the



5.3. Identity Assurance Level 1

IAL1 permits both remote and in-person identity proofing. Identity proofing processes at IAL1 allow for a range of acceptable techniques in order to detect the presentation of fraudulent identities by a malicious actor while facilitating user adoption and minimizing false negatives and application departures (legitimate applicants who do not successfully complete identity proofing). Notably, the use of biometric matching, such as the automated comparison of a facial portrait to supplied evidence, at IAL1 is optional, providing pathways to proofing and enrollment where such collection may not be viable or where privacy and equity risks outweigh security considerations.

The following requirements apply to all CSPs providing identity proofing and enrollment services at IAL1.

5.3.1. Automated Attack Prevention

The CSP **SHALL** implement a means to prevent automated attacks on the identity proofing process. Acceptable means include, but are not limited to: bot detection, mitigation, and management solutions; behavioral analytics; web application firewall settings; and traffic analysis.

5.4. Identity Assurance Level 2

Like IAL1, IAL2 identity proofing allows for both remote and in-p
processes in order to maximize accessibility while still mitigating
attacks and other identity proofing errors. Remote IAL2 identity p
accomplished by the CSP via a fully automated process, a CSP op
or a combination of the two.

5.4.1. Automated Attack Prevention

The CSP **SHALL** implement a means to prevent automated attack
proofing process. Acceptable means include, but are not limited t
mitigation, and management solutions; behavioral analytics; web
settings; and traffic analysis.

5.3.2. Evidence and Core Attributes Collection Requirements

5.3.2.1. Evidence Collection

For remote or in-person identity proofing, the CSP **SHALL** collect *one* of the following from the applicant:

1. One piece of SUPERIOR evidence, or
2. One piece of STRONG evidence and one piece of FAIR evidence

5.3.2.2. Collection of Additional Attributes

Validated evidence is the preferred source of identity attributes. If the presented identity evidence does not provide all the attributes the CSP considers core attributes, it **MAY** collect attributes that are self-asserted by the applicant.

5.4.2. Evidence and Core Attribute Collection Requireme

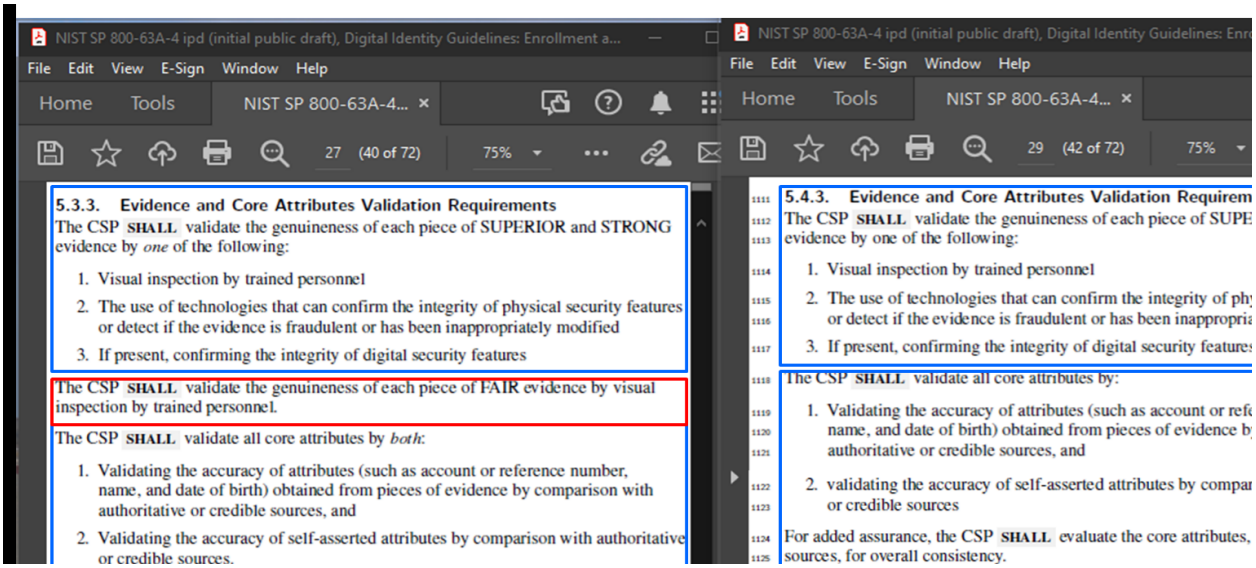
5.4.2.1. Evidence Collection

For remote or in-person identity proofing, the CSP **SHALL** collec
from the applicant:

1. One piece of SUPERIOR evidence
2. One piece of STRONG evidence and one piece of FAIR evid

5.4.2.2. Collection of Attributes

Validated evidence is the preferred source of identity attributes. I
evidence does not provide all the attributes the CSP considers cor
collect attributes that are self-asserted by the applicant.



5.3.3. Evidence and Core Attributes Validation Requirements

The CSP **SHALL** validate the genuineness of each piece of SUPERIOR and STRONG evidence by *one* of the following:

1. Visual inspection by trained personnel
2. The use of technologies that can confirm the integrity of physical security features or detect if the evidence is fraudulent or has been inappropriately modified
3. If present, confirming the integrity of digital security features

The CSP **SHALL** validate the genuineness of each piece of FAIR evidence by visual inspection by trained personnel.

The CSP **SHALL** validate all core attributes by *both*:

1. Validating the accuracy of attributes (such as account or reference number, name, and date of birth) obtained from pieces of evidence by comparison with authoritative or credible sources, and
2. Validating the accuracy of self-asserted attributes by comparison with authoritative or credible sources.

5.4.3. Evidence and Core Attributes Validation Requirem

The CSP **SHALL** validate the genuineness of each piece of SUPE
evidence by one of the following:

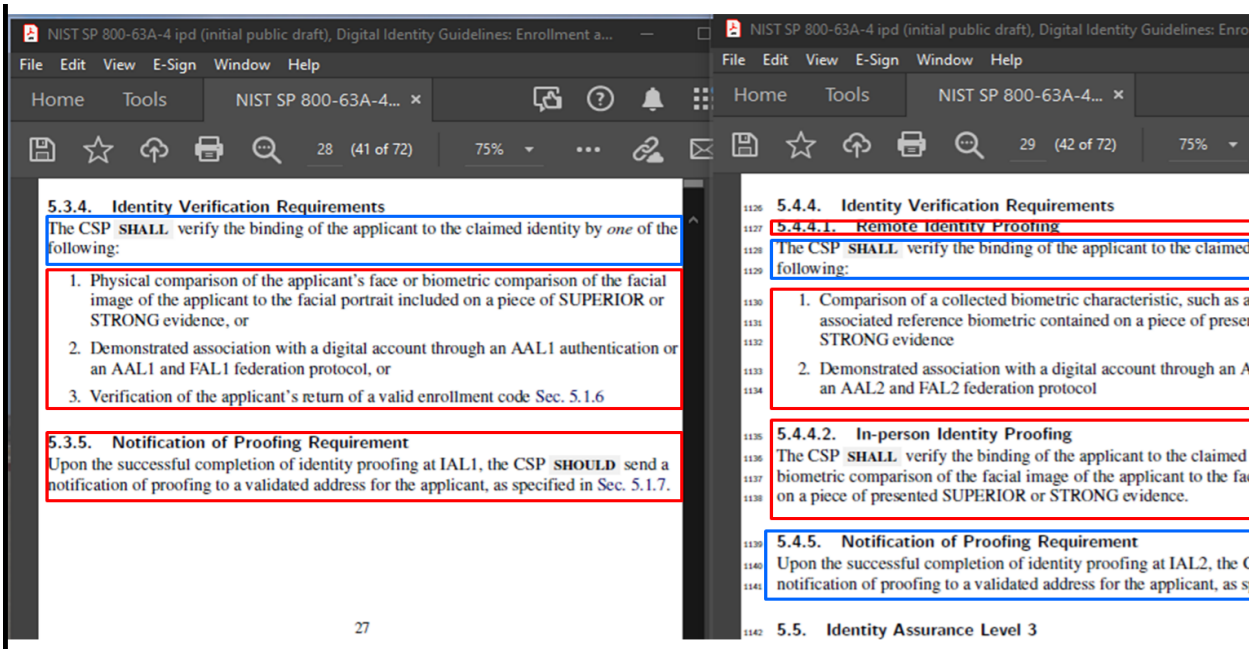
1. Visual inspection by trained personnel
2. The use of technologies that can confirm the integrity of phy
or detect if the evidence is fraudulent or has been inappropria
3. If present, confirming the integrity of digital security feature

The CSP **SHALL** validate all core attributes by:

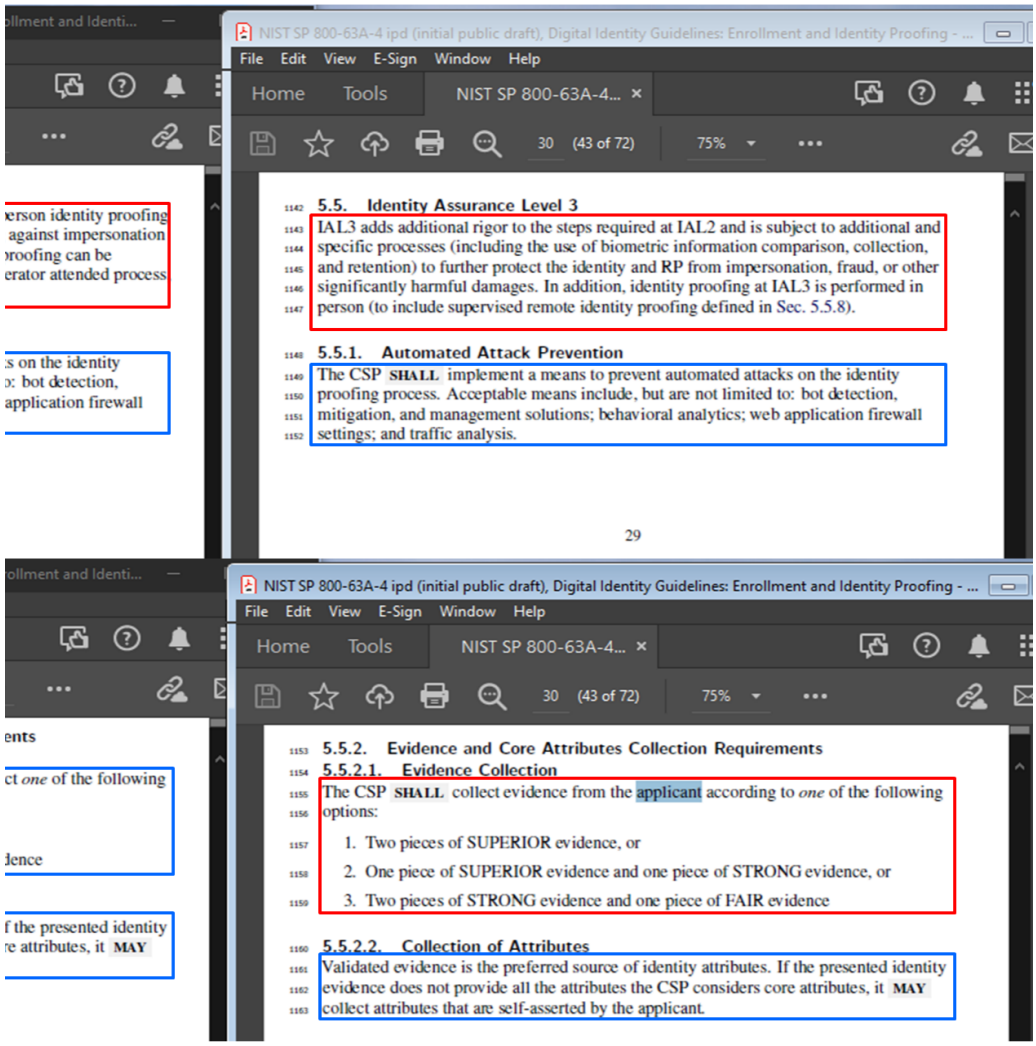
1. Validating the accuracy of attributes (such as account or refe
name, and date of birth) obtained from pieces of evidence b
authoritative or credible sources, and
2. validating the accuracy of self-asserted attributes by compar
or credible sources

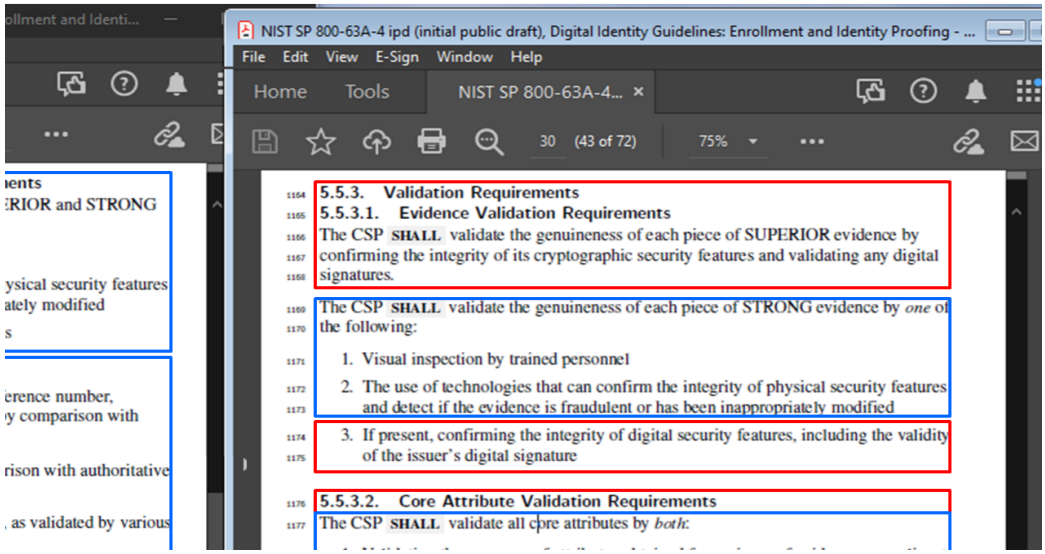
For added assurance, the CSP **SHALL** evaluate the core attributes,
sources, for overall consistency.

For added assurance, the CSP **SHALL** evaluate the core attributes, as validated by various sources, for overall consistency.



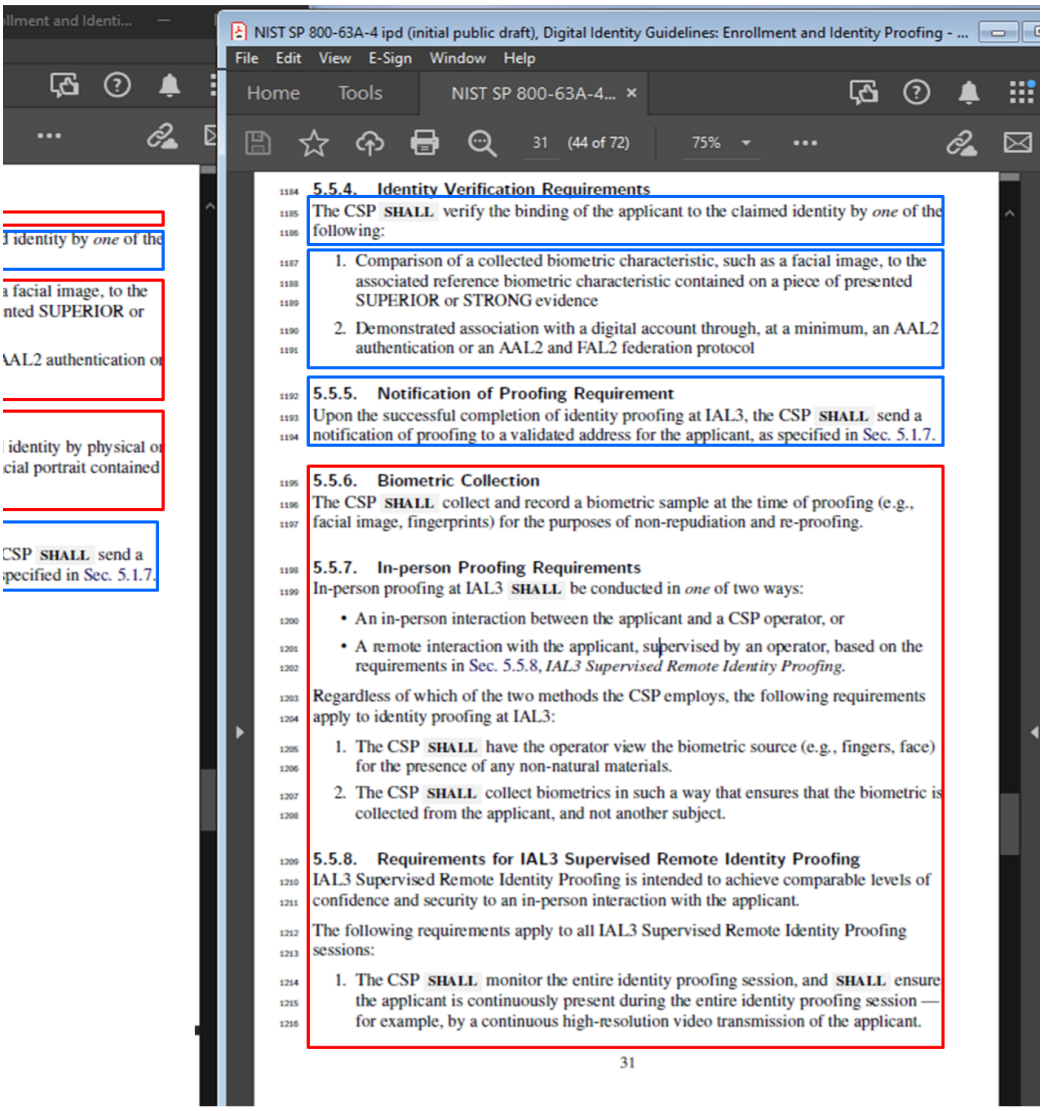
ely. Blue boxes indicate where text is the same as at least one
L. The purpose of this is that there is plenty of scope to make
ts for IALn apply at this IAL unchanged". Also, it is noted that, if
ere is no need to repeat the applicable IAL when it is the same.





1. Validating the accuracy of attributes obtained from pieces of evidence or applicant self-assertion by comparison with authoritative or credible sources
2. Validating the cryptographic features of any presented digital evidence, as described above

For added assurance, the CSP **SHALL** evaluate the core attributes, as validated by various sources, for overall consistency.



5.5.4. Identity Verification Requirements

The CSP **SHALL** verify the binding of the applicant to the claimed identity by *one* of the following:

1. Comparison of a collected biometric characteristic, such as a facial image, to the associated reference biometric characteristic contained on a piece of presented SUPERIOR or STRONG evidence
2. Demonstrated association with a digital account through, at a minimum, an AAL2 authentication or an AAL2 and FAL2 federation protocol

5.5.5. Notification of Proofing Requirement

Upon the successful completion of identity proofing at IAL3, the CSP **SHALL** send a notification of proofing to a validated address for the applicant, as specified in Sec. 5.1.7.

5.5.6. Biometric Collection

The CSP **SHALL** collect and record a biometric sample at the time of proofing (e.g., facial image, fingerprints) for the purposes of non-repudiation and re-proofing.

5.5.7. In-person Proofing Requirements

In-person proofing at IAL3 **SHALL** be conducted in *one* of two ways:

- An in-person interaction between the applicant and a CSP operator, or
- A remote interaction with the applicant, supervised by an operator, based on the requirements in Sec. 5.5.8, *IAL3 Supervised Remote Identity Proofing*.

Regardless of which of the two methods the CSP employs, the following requirements apply to identity proofing at IAL3:

1. The CSP **SHALL** have the operator view the biometric source (e.g., fingers, face) for the presence of any non-natural materials.
2. The CSP **SHALL** collect biometrics in such a way that ensures that the biometric is collected from the applicant, and not another subject.

5.5.8. Requirements for IAL3 Supervised Remote Identity Proofing

IAL3 Supervised Remote Identity Proofing is intended to achieve comparable levels of confidence and security to an in-person interaction with the applicant.

The following requirements apply to all IAL3 Supervised Remote Identity Proofing sessions:

1. The CSP **SHALL** monitor the entire identity proofing session, and **SHALL** ensure the applicant is continuously present during the entire identity proofing session — for example, by a continuous high-resolution video transmission of the applicant.