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

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

Organization: Beruku Identity

Name of Submitter/POC: Julian White

Email Address of Submitter/POC: [REMOVED]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	t Line t	Comment (Include rationale for comment)	Suggested Change
	63-Base	Identity proofing and enrolment	iii	18	One of your stated aims is to improve demographic coverage epically for IAL2 without using face recognition. This implies that CSP's will be relying on data and data services for verification instead. Whilst this is possible verification	Where data & KBV are used to replace face recognition there must be a requirement on the CSP to introduce sufficient fraud checks and prevention measures to mitigate the risks introduced to maintain equivalence, otherwise it will create a
					using such methods is inherently more risky than face verification, epically if CSP's are relying on data services such as a credit bureau, therefore those risks need to be mitigated with other controls such as fraud checks, but these haven't been	2 tier IAL2
	63-Base	4.3.1	18	77	The example using a driving licence is likely to be confusing as it mixes authentication and verification. In the example, it could be argued that if a driving licence was an authentication method then in theory person A should be able to give it to person B to present to the security guard, and as long as the driving licence is authentic and relates to a person	Replace the example with something that is less likely to be misinterpreted, e.g. an at-home-printed ticket to enter an event so its clear that the guard is authenticating an authenticator not performing a verification.
					allowed to pass the checkpoint then the bearer should be able to proceed regardless of whether they match the image of the licence holder because the licence is the authenticator. However in practice the guard would also check that the bearer matches the face on the driving licence, which is more like verification, but it could also be that the licence is acting as the 'template' that is going to be used to authenticate a manual facial recognition. It is quite common for	
					people to easily confuse these two things so it would be better to either make it explicit what the guard is doing with both the licence itself and matching against the person, or provide a different example that makes a clear distinction between authentication and verification. It's also not entirely true, some countries do issue driving licences on a smart	
					card and can be used in a digital environment. A more real world example would be a ticket for an event or boarding pass for a plane, the ticket with a QR or bar code is authenticated by the security guard, usually by scanning it with a	
	63-Base	5.2.2.1	31	119	B This section is telling the reader HOW to reach an IAL, but not WHAT value it gives you. It should talk more about what risks and attacks etc each IAL is designed to protect the service against, rather than the mechanics of what happens for each IAL, that is for part A to explain.	The description for each IAL should talk about the risk and attacks that the IAL is designed to protect against, e.g. at IALI it should reduce the risks of a service accepting synthetic identities and prevent the creations of accounts by impostors who do not have a relationship with the subject. It's probably not going to do much to protect it from someone with a
						close relationship, e.g. a spouse or other family member that lives with them, as they are likely to have access to the necessary information to pass the checks.
	63-Base	5.2.3.1	33	1283 / 1290	This section seems to allow an organisation to decide to 'tailor' some parts of the identity checking process if they believe it would have a negative impact but doesn't appear to require them to introduce any mitigations where they fall short in meeting the standard needed, just that they need to be accessed. However mitigation are covered in 5.3.2 but it	This section should also say that organisation must introduce sufficient mitigations where they are 'tailoring' the service.
					would be better to say it explicitly here for clarity.	
	63-Base 63-Base	5.2.3.2	34 37	_	5 "who they claim to be" is the "subscriber", so use that for consistency  1 This section seems to allow an organisation to decide to 'tailor' some parts of the identity checking process if they	replace "who they claim to be" with "subscriber"  The IALs should explicitly state which variations are allowed and what mitigations must be in place to ensure
	63-Base	533	38		believe it would have a negative impact but doesn't appear to require them to introduce any mitigations where they fall short in meeting the standard needed. This is unhelpful as its then not possible to know when an IAL2 from CSP A is equivalent to an IAL2 from CSP A is in the capital	equivalence.
					an optional activity, which comes at a cost and therefore will not be performed unless mandated to do so. Its not clear whether the requirement is to add more identity evidence or improve the verification controls, doing the wrong one may have no impact in the fraud risk. There's two main risks that are being addressed by the proofing process, preventing the use of synthetic identities and preventing someone impersonating a real identity. If the fraud risk in question is about synthetics then that is in the identity resolution stage and needs more controls or checks against identity evidence, whether that is provided by the claimant or data from an authoritative source; if the fraud risk is impersonation then you need to increase the verification controls. This section isn't clear on this.	gathering further identity evidence, or increasing the verification controls.
	63-Base	A.1	46		This definition appears to be circular since it refers to Authenticate, which refers to Authentication, which then refers back to this definition. It is also unclear as it says "authenticate the claimants identity" which seems to imply doing an identity proofing process, which isn't what was meant, it should be proving that the claimant is someone who is	Change "used to authenticate the claimant's identity" to "prove the claimant is a subscriber"
	63-Base	A.1	52		According to 4.1, to attach and assert an IAL the user can't be an applicant, they should be a subscriber	Change "applicant" to "subscriber"
	63-Base	A.1	52	191	4 A mobile Driving Licence (mDL) would also be valid digital evidence	add mDL as a digital evidence example

6	3-Base	A.1		56			'subsystem" and "interfering" seems to imply that it would cover technical attacks such as an injection attack, or other ybe security type attacks, which is incorrect. Presentation attacks would always be against the sensor, not an attack that interferes with its subsystem(s).	Replace "Presentation to the biometric data capture subsystem with the goal of interfering with the operation of the biometric system" with "Presentation to the biometric sensor with the goal of convincing the biometric system that the captured sample was from a genuine person"
6	53A		2.1	4			'unexpired" isn't always true, later in this document it states some expired evidence is allowable. The evidence needs to be valid, which may include recently expired evidence.	Change "unexpired" to "valid"
6	33A		2.1	4	ļ	419	All seems to imply that its not materially different to IAL 2 other than it mandates that it must be done by a human. This seems to be more like a solution rather than stating the requirements needed to met IA3, and in practice humans rend to be less consistent and reliable than a lot of the technology platforms that are now available on the market. It would be better to change this to say what measures and processes need to be performed, even if might be that they	Change to "IAL3 requires the collection of the strongest types of evidence and a very rigorous process for validating the evidence and verifying the identity."
6	53A	4.1.1		8	figu	ure 1	can only be done in person at the current time due to technical imitations. This will also future proof the specification.  30x 3 seems to have a typo, "evidence validation" should be "identity verified"	change "evidence validation" to "identity verified" in box 3
6	53A		4.3	9		498	'unexpired" isn't always true, later in this document it states some expired evidence is allowable. The evidence needs to	Change "unexpired" to "valid"
6	53A		4.3	9	ì	á	pe valid, which may include recently expired evidence.  This implies that "copies, photograph and scans" are allowed to be used at any IAL. This should not be the case, as soon as evidence is "copied, photographed or scanned" too much information is lost and they are then easily doctored using commercially available software. So whilst this might be ok for IAL1, it might not be for IAL2 and 3. Each IAL should say whether copies/scans et car acceptable.	Remove the acceptance of copies, photographs and scans from this section and add them as applicable to each IAL
6	53A	4.3.1		10	517	7-	This section isn't needed as the requirements are covered in 4.3.3.1, 4.3.3.2 & 4.3.3.3 for each strength, in fact it seems to contradict them in places. It would be clearer if it were removed and just stated in the following sections	Remove 4.3.1 and add "The presented evidence identifies the issuer" to 4.3.3.1, 4.3.3.2 & 4.3.3.3
6	53A	4.3.1		10	)	524	This isn't really needed. All that matters at this stage is that the evidence is authentic and make no assumptions that the bearer and the owner are the same person.	Remove point 5
6	53A	4.3.2		10	526 541	6-	This section isn't needed as the requirements are covered in 4.3.3.1, 4.3.3.2 & 4.3.3.3 for each strength, in fact it seems to contradict them in places. It would be clearer if it were removed and just stated in the following sections	Remove 4.3.2 and add "If applicable, the presented digital evidence can be verified through authentication at an AAL or FAL commensurate with the assessed IAL." to 4.3.3.1, 4.3.3.2 & 4.3.3.3
6	53A	4.3.1		10	)	538	This isn't really needed. All that matters at this stage is that the evidence is authentic and make no assumptions that the pearer and the owner are the same person.	
6	53A	4.3.3.1		11	Ī	553	This isn't really needed. All that matters at this stage is that the evidence is authentic and make no assumptions that the bearer and the owner are the same person.	Remove point 2
6	3A	4.3.3.2		11		578	suggest that recently expired evidence is probably also valid for strong, its probably more applicable here than in IAL1. Its retainly possible to use a recently expired passport to prove your identity to get a new one, which this requirement seems to orevent.	add "The evidence has not expired or it expired within the previous six (6) months, or it was issued within the previous six (6) months if it does not contain an expiration date."
6	53A	4.3.3.3		12	!	588	This isn't really needed. All that matters at this stage is that the evidence is authentic and make no assumptions that the pearer and the owner are the same person.	Remove point 3
6	53A	4.3.4.1		12	2	604	This section isn't needed here, the requirements should be covered in each IAL in 5.3.3, 5.4.3 & 5.5.3 because they vary by AI	Remove 4.3.4.1 and add details to 5.3.3, 5.4.3 & 5.5.3
6	33A	4.3.4.3		13			This doesn't define what being "trained" means, i.e. by whom, to what standard and how often do they need to be refreshed. This also might change depending on the IAL, especially for IAL3.  For example in GPG 45 for low strength evidence we've said that:  The person will need to use official templates to check any of the following features on the evidence look the way they should:  background printing fonts and alignment	Clarify what the training requirements are for each IAL
							holograms and positioning the way it's been laminated designs printed with optical variable ink (and check they look the way they should at certain angles) the format of any 'compound identifiers' or a machine-readable zone (MRZ) the position of any photographs on the evidence (they should not have been replaced or edited) be trained in how to detect false documents by a specialist trainer, such as the Home Office, National Document Fraud Jnit, Centre for the Protection of National Infrastructure (CPNI) or any other company that follows the Home Office's sest practice guidance	
	53A		4.4		_		'and establish" seems superfluous, remove.	Remove "and establish"
6	3A		5	16	i	689 1	Nearly all of this section is not about IAL's at all, but general requirements to be a CSP that apply regardless of the IAL. It would be clearer if there were two sections, one that is just about the IAL and the processes needed, and another which was all the other general CSP requirements.	Rename section 5 to "General requirements for a CSP", move 5.3, 5.4 & 5.5 to a new section on IALs.
6	33A	5.1.1.2		17		í	This should be mandatory, otherwise a) no one will do it because it costs money, 2) there is a growing risk from online raud and CSP's must protect themselves from it otherwise there will be no trust in the digital identities they issue. The types of fraud checks used can be proportionate to the risk depending on the IAL, the evidence being used and the verification process. Suggest that specific fraud checks should be included in the IALs.	Make fraud checks mandatory and include them in the IALs.
6	53A	5.1.2.2		18	8	1	ts not clear what you mean by "knowledge of the SSN shall not be considered evidence", because certainly an SSN can be used for identity resolution, as mentioned in the previous sentence, which therefore makes it evidence and contradicts the previous sentence. However knowledge of the SSN can not be used as a verification method (i.e. as a KBV) because ts not secret and known by too many people.	Make it clear what the statement means
6	33A	5.1.8		22		914	As applied to the identity proofing process, CSPs may use biometrics to uniquely resolve an individual identity within a given population or context" is misleading, it implies that CSPs can do 1:N matching against biometric data. This should not be the case as this introduces significant false match issues and requires more complex matching and handling processes, in all cases a biometric comparison should be 1:1 against a target template.	Remove "uniquely resolve an individual identity within a given population or context,"
6	53A	5.1.8		23		954	The specification defines "liveness detection" as a subset of PAD, therefore this requirement should refer to PAD in general, not just a subset.	Replace "liveness detection" with "PAD"
6	33A	5.1.9.1		24		993	There's insufficient detail about how and whom may act as a referee, its been left open for the CSP to write their own policy on it but that will lead to significant inconsistencies; one CSP may simply allow a "note from your parent" and the specification says that will be ok as long as the CSP has written that into their policy. The specification needs to define both how referee gives the reference to the CSP and what restrictions there are on being a referee. We've written a guide for this in the UK, we've called them a vouch, but the concept is the same: https://www.gov.uk/government/publications/how-to-accept-a-vouch-as-evidence-of-someones-identity/how-to-accept-	Clearly define the requirements to be a referee and how the reference is given to the CSP
	53A	5.3.1		26	<u>.</u>	á	a-vouch-as-evidence-of-someones-identity  This section is the same in every IAL, therefore it should be in a general "CSP requirements" section and not here	Move to section 5.1
b	JOA	J.3.1		26	1	1040	inis section is the same in every IAL, therefore it should be in a general CSP requirements section and not here	ואוטיפ נט זפנעוטוו ב.1

6.8.4 1.3.2.1 26 105 Filts residence selection is quite restriction, one of the stated aims of the update was to introduce more way to get at which get all and provided in the core of the specification has not changed with a which address and the provided and t
digital identity but the core of the specification has not changed. Whist cather sections have added creates and things upon a reference, flowers in the section is allow members of the specification in allow members of the section in 14 and members of the section of the se
usus as referees, indexes in matter if this section does not reflect it. Previously in the specification it also mentioned using further feat sources and fraud relate sources and fraud related sources and fraud r
ouing further data sources and fraud checks to improve demographic coverage. In that regard you have 3 levers you can use for identify esolution. If the service which the service of the
use for identity resolution, 1] the strength of the identity evidence needed, whether that is provided by the claimant or taken from an authoritative source, 2 how well the CD primarise authoritical tension, 2 how well the CD primarise that is inclined to the existence of the strength of the control of th
tale from an authoritative source. 2) how well the CSP confirms the authemicity of the identity elderine, 3) what other froat of data check the CSP received by perform indice to the tempting the existence of the identity for each IAL. We added executly this fileshilly to the Use equivalence of 800-62 (nown as GP4.5).  The company of the company of the identity elders are company of the identity elders and incident the identity elders are company of the identity elders and incident the identity elders are company of the identity elders are elders, which are analogous to the interval of the interval of the identity elders are company of the identity elders are company of the interval of the identity elders are company of the identity elders are elders, which are are company of the identity elders are company of
fraud or data checks the CSP needs to perform in order to meet the risk appetite in confirming the existence of the detecting for each IAL. We added eachty this ficiality to the Use qualment of SL jamon as GR 64 - 1 https://www.gov.uk/government/publications/identity-proofing-and-verifications-of-an-individual/inow-to-proce-and-verify-surrous-societity, in Intervence societisty, in Intervence societisty, in Intervence societisty, in Intervence societisty, and the very confirmance requirements that is intimized when it suits them. This simply can not be the case, core attributes must only be the minimum set of common attributes when it suits them. This simply can not be the case, core attributes must only be the minimum set of common attributes when it suits them. This simply can not be the case, core attributes must only be the minimum set of common attributes when it suits them. This simply can not be the case, core attributes must only be the minimum set of common attributes are an accorn with the CSP and they must called confirmation of the CSP and they must call the case may be self-asserted or or SSN for distinctive must only be the minimum set of common attributes when it is not common attributes are considered in order to constant and account maintenance propriess in the case the name. Does not self-asserted attributes which was a self-asserted asserted ass
fraud or data checks the CSP needs to perform in order to meet the risk appetite in confirming the existence of the detecting for each IAL. We added eachty this ficiality to the Use qualment of SL jamon as GR 64 - 1 https://www.gov.uk/government/publications/identity-proofing-and-verifications-of-an-individual/inow-to-proce-and-verify-surrous-societity, in Intervence societisty, in Intervence societisty, in Intervence societisty, in Intervence societisty, and the very confirmance requirements that is intimized when it suits them. This simply can not be the case, core attributes must only be the minimum set of common attributes when it suits them. This simply can not be the case, core attributes must only be the minimum set of common attributes when it suits them. This simply can not be the case, core attributes must only be the minimum set of common attributes when it suits them. This simply can not be the case, core attributes must only be the minimum set of common attributes are an accorn with the CSP and they must called confirmation of the CSP and they must call the case may be self-asserted or or SSN for distinctive must only be the minimum set of common attributes when it is not common attributes are considered in order to constant and account maintenance propriess in the case the name. Does not self-asserted attributes which was a self-asserted asserted ass
dentity for each IAL. We added exacty bits fieldbilly to the UK equivalent of 800-53 (kmox as GG 45-https://www.gov.uk/government/publication/fielders/proofing-and-werliffs-into-of-an-individual/plivo-to-prove-and-verify-someons-identity), in that we use confidence levels, which are analgoous to IALs and created profiles!  (EXA
https://www.gov.uk/goverment/publications/identity-poorling-and-verification-of-an-individual/flow-to-prove-ano-en-indentity, in that we use confidence levels, which are and so to IAs and created profiles' integration of the various was that has the created profiles' integrated by the various was that was considered in the various was that as the various was the v
enthy-comeones-identity), in that we use confidence levels, which are analogous to IALs and created frortiles' litters/ livew are, out government/publications/ frortiles' proofings and vestor of 3-ani-individual/fortility-proofings and vestor of 3-ani-individual/fortility-proofings and vestor of 3-ani-individual/fortility-proofings and vestor of 3-ani-individual/fortility-proofings and vestor of the specification of a second training and the second of the state of the specification of a second training and the second of the state of the specification of the state of the specification of the state of the specification of the state of the state of the specification of the specification of the state of the specification of the s
Integrit/News grow/Jegoremment/publications/identity-proofines and verification of an individual/identity-profile) that set out the various way of that a CSP an mere a sport confidence industry and a sport of common and the various way of that a CSP an mere a sport confidence in the various way of that a CSP an mere a sport confidence in the various way of the various way of the case, one attembates must only be the minimum as et or common attributes may be self asserted or attributes may be self asserted when it was the minimum as et or common attributes may be self asserted when it was the minimum as et or common attributes may be self asserted when it was the minimum as et or common attributes may be self asserted when it was the minimum as et or common attributes may be self asserted when it was the minimum as et or common attributes may be self asserted when it was the minimum as et or common attributes may be self asserted or attributes may be self asserted when it was the minimum as et or common attribute may be self asserted when it was the minimum as et or common attributes may be self asserted when it was the minimum as etc. and it was the minimum as etc. and it was the self-decided or birth, with the being mandatory to the pine mandatory to the safetities of the supplier to mandatory to the pine mandatory to the supplications of
Integrit/News grow/Jegoremment/publications/identity-proofines and verification of an individual/identity-profile) that set out the various way of that a CSP an mere a sport confidence industry and a sport of common and the various way of that a CSP an mere a sport confidence in the various way of that a CSP an mere a sport confidence in the various way of the various way of the case, one attembates must only be the minimum as et or common attributes may be self asserted or attributes may be self asserted when it was the minimum as et or common attributes may be self asserted when it was the minimum as et or common attributes may be self asserted when it was the minimum as et or common attributes may be self asserted when it was the minimum as et or common attributes may be self asserted when it was the minimum as et or common attributes may be self asserted when it was the minimum as et or common attributes may be self asserted or attributes may be self asserted when it was the minimum as et or common attribute may be self asserted when it was the minimum as et or common attributes may be self asserted when it was the minimum as etc. and it was the minimum as etc. and it was the self-decided or birth, with the being mandatory to the pine mandatory to the safetities of the supplier to mandatory to the pine mandatory to the supplications of
SA   S.3.2.2   26   1057 his seems at odds with the rest of the specification, it seems to include, it is easy that all attributes that are core, or used for identity resolution must attribute when it suits them. This simply can not be the case, core attributes with the specification of the case, core attributes when they may be mandatory to be provided, are not core and a recount with the CP3 and they must be validated, other attributes, whish they may be mandatory to be provided, are not core and a recount with the CP3 and they must be validated, or and attributes may be self asserted or early the specification, and a phone number for contant and crown maintenance purposes; in this case the name, DoB must be validated, as a so must the address or SSH because its used for resolution, but they enhanced in the contant and the contant
53.2.2 26 107 This seems at odds with the rest of the specification, it seems to injuly that an CFC an just accept any self asserted core of startification when it suits them. This simply can not be the case, core attributes must only be the minimum, set of common attributes medded in order to create an account with the CFP and they must be validated; other attributes, whilst when they may be mandatory to provide at least one of "address" or "SSN for identity resolution, and a phone manner for cortact and account minimum powers, in this case the training of the traini
attribute when it suits them. This simply can not be the case, core attributes must only be the minimum set of common attributes needed in order to create an account with the CSP and the suits be validated, when they may be mandatory to be provided, are not core and in some cases may be self-asserted. For example core attributes when they may be mandatory to be provided, are not core and in some cases may be self-asserted. For example core attributes when they may be mandatory to be provided, are not core and in some cases may be self-asserted. For example core attributes when they may be mandatory to be provided, are so must the stude the in agreed to the case of the same. Doll must be called to find the provided at least one of "of identity resolution, and a phone number for contact and account maintenance purposes, in this case the name. Doll must be called the provided and
attributes needed in order to create an account with the CSP and they must be validated, other attributes, whilst when they may be mandatory to be provided, an ent core and in sost earn and care of a britty. with It being mandatory to provide at least one of "address" or "SSN" for identity resolution, and a phone number for contact and account maintenance purposes; in this case the name, DoB must be validated, as so must the address or SSN because its used for resolution, but the phone number is not.  5.3.4 27 1031 There's no performance requirements for the biometric system delivery in the state of the contact of
they may be mandatory to be provided, are not core and in some cases may be self-asserted. For example core attributes might just be "name" and "idea of birth", with the legin analytic the same of "addes" or "SN" for identity resolution, and a phone number for contact and account maintenance purposes; in this case the name, DoB must be validated, as so must the address or SN because its used for resolution, but the phone number is not.  1834
might just be "name" and "date of birth", with It being mandatory to provide at least one of "address" or "SN" for identity resolution, and a phone number for contact and account manner purposes; in this case the name, DooB must be validated, as so must the address or "SN" because its used for resolution, but the global manner or purpose; in this case the name, DooB must be validated, as so must the address or "SN" because its used for resolution, but the global manner or purpose; in this case the name, DooB must be validated, as so must the address or "SN" because its used for resolution, but the global manner or purpose; in this case the name, DooB must be validated, as so must the address or "SN" because its used for resolution, but the global manner or purpose; in the past was so were the global manner or purpose; in the past was so with the section of an other the section of the past was so introduce more ways to get a digital identity but the core of the specification in labs not changed. Whilst interest on the past was not introduce more ways to get a digital identity but the core of the specification in labs most changed. Whilst interest on the past was not introduce more ways to get a digital identity but the core of the specification in labs mentioned using further data sources and fraud checks to improve the section share added caveats and things such as reference, it doesn't matter if this section does not reduce the resolution, and select its provided by the claimant or taken from an authoritative source, 2) how well the CSP confirms the authority of the identity evidence, 3) what other fraud or data checks the CSP preads to perform in order to more the risk appetite in confirming the existence of the identity for each IAL. We added exactly this flexibility to the UK equivalent of 800-83 (Incom as 6FG 45 - https://www.gov.uk/government/publications/identity-profiles and every flexibility to profile and every flexibility to the vidence of the identity for each IAL. We added exactly this flexibility
might just be "name" and "date of birth", with It being mandatory to provide at least one of "address" or "SN" for identity resolution, and a phone number for contact and account manner purposes; in this case the name, DooB must be validated, as so must the address or "SN" because its used for resolution, but the global manner or purpose; in this case the name, DooB must be validated, as so must the address or "SN" because its used for resolution, but the global manner or purpose; in this case the name, DooB must be validated, as so must the address or "SN" because its used for resolution, but the global manner or purpose; in this case the name, DooB must be validated, as so must the address or "SN" because its used for resolution, but the global manner or purpose; in the past was so were the global manner or purpose; in the past was so with the section of an other the section of the past was so introduce more ways to get a digital identity but the core of the specification in labs not changed. Whilst interest on the past was not introduce more ways to get a digital identity but the core of the specification in labs most changed. Whilst interest on the past was not introduce more ways to get a digital identity but the core of the specification in labs mentioned using further data sources and fraud checks to improve the section share added caveats and things such as reference, it doesn't matter if this section does not reduce the resolution, and select its provided by the claimant or taken from an authoritative source, 2) how well the CSP confirms the authority of the identity evidence, 3) what other fraud or data checks the CSP preads to perform in order to more the risk appetite in confirming the existence of the identity for each IAL. We added exactly this flexibility to the UK equivalent of 800-83 (Incom as 6FG 45 - https://www.gov.uk/government/publications/identity-profiles and every flexibility to profile and every flexibility to the vidence of the identity for each IAL. We added exactly this flexibility
resolution, and a phone number for contact and acceptance is used.    1081   There's no performance requirements for the biometric system define here, without that there is no way.   1082   There's no performance requirements for the biometric system define here, without that there is no way.   1083   There's no performance at IALI does not have to be as strict for those at IALI or IALI
wildsted, as so must the address or SSN because its used for resolution, but that there is no way to ensure equivalence between CSPs. The performance requirement for the biometric system defined here, without that there is no way to ensure equivalence between CSPs. The performance at IA1 does not have to be a strict for those at IA12 or IA13.  63A 5.4.1 28 1096 This section is the same in every IA1, therefore it should be in a general "CSP requirements" section and not here ways to get a digital identity but the core of the specification is an every IA1, therefore it should be in a general "CSP requirements" section and not here ways to get a digital identity but the core of the specification is not changed. Whilst other sections have added caveats and things such as reference, it doesn't matter if this section does not have to the specification is a lost of the specification is confirmed the specification is confirmed the specification is lost of the specification is to limit the lost of the specification is to limit the lost of the spec
S3A   S.3.4   27   1081   There's no performance requirements for the biometric system defined here, without that there is no way to ensure equivalence between CSPs. The performance at Ital Lor VIA.3.
equivalence between CSPs. The performance at IAL1 does not have to be as strict for those at IAL2 or IAL3  63A 5.4.1 28 1096 This section is the same in every IAL, therefore it Spould be in a general "CSP requirements" section and not here  63A 5.4.1 28 1096 This section is the same in every IAL, therefore it Should be in a general "CSP requirements" section and not here  63A 5.4.2 128 1006 This sections esteroit in squite restrictive, one of the specification of the
G3A   S.3.5   27   1087   This section is the same in every IAL, therefore it is hould be in a general "CSP requirements" section and not here   Move to section S.1
G3A   S.3.5   27   1087   This section is the same in every IAL, therefore it is hould be in a general "CSP requirements" section and not here   Move to section S.1
53A   5.4.1   28   1096   This section is the same in every IAL, therefore it should be in a general "CSP requirements" section and not here ways to get a final foliation of the stated aims of the update was to introduce more ways to get a digital identity but the core of the specification has not changed. Whilst other sections have added caveats and things such as referees, it doesn't matter if this section does not reflect it. Previously in the specification it also mentioned using further data sources and fraud checks to improve demographic coverage. In that regard you have a levers you can use for identity resolution, 1) the strength of the identity evidence needed, whether that is provided by the claimant or taken from an authoritative source, 2) how well the CSP confirms the authenticity of the identity devidence, 3) what other fraud or data checks the CSP needs to perform in order to meet the risk appetite in confirming the existence of the identity of each IAL. We added exactly this littly to the U. (equivalence) of 30-63 (a. 1), the strength of the identity profiles and everification-of-an-individual/how-to-prove-and-verification-of-an-individual/how-to-prove-and-verifications-of-an-individual/how-to-prove-and-verifications-of-an-individual/how-to-prove-and-verifications-of-an-individual/how-to-prove-and-verifications-of-an-individual/how-to-prove-and-verifications-of-an-individual/how-to-prove-and-verifications-of-an-individual/how-to-prove-and-verifications-of-an-individual/how-to-prove-and-verifications-of-an-individual/how-to-prove-and-verifications-of-an-individual/how-to-prove-and-verifications-of-an-individual/how-to-prove-and-verifications-of-an-individual/how-to-prove-and-verification-of-an-individual/how-to-prove-and-verification-of-an-individual/how-to-prove-and-verification-of-an-individual/how-to-prove-and-verification-of-an-individual/how-to-prove-and-verification-of-an-individual/how-to-prove-and-verification-of-an-individual/how-to-prove-and-verification-of-an-individual/how-to-prove-
5.4.2.1 28 1105 This evidence selection is quite restrictive, one of the stated aims of the update was to introduce more ways to get a digital identity but the core of the specification has not changed. Whilst other sections have added caveats and things such as referees, it doesn't matter if this section does not reflect it. The reviously in the specification it also mentioned using further data sources and fraud checks to improve demongraphic coverage. In that regard you have 3 levers you can use for identity resolution.) It he strength of the identity evidence, 3 what other fraud or data checks the CP needs to perform in order to meet the risk appetite in confirming the existence of the identity for each IAL. We added exactly this flexibility to the UK equivalent of 800-63 (known as GPG 45 - https://www.gov.uk/gov.memort/publications/identity-proofing-and-verification-of-an-individual/indow-to-prove-and-verify-someones-identity), in that we use confidence levels, which are analogous to IALs and created 'profiles' (https://www.gov.uk/gov.memort/publications/identity-proofing-and-verification-of-an-individual/indentity-profiles) and -individual/indentity-profiles and-verification-of-an-individual/indentity-profiles and-verification-of-an-individual/indentity-profiles and-verification-of-an-individual/indentity-profiles and-verification-of-an-individual/indentity-profiles and-verification-of-an-individual/indentity-profiles and-verification-of-an-individual/indentity-profiles and-verification-of-an-individual/indentity-profiles and-verification-of-an-individual/indentity-profiles and-verification-of-an-individual/indentity-profiles that are core, or used for identity resolution must attribute when it suits them. This simply can not be the case, core attributes must only be the minimum set of common attributes may be mandatory to be provided, are not core and in some cases may be self-asserted. For example core attributes may be self asserted attributes may be self asserted without the wind of the provide at lea
digital identity but the core of the specification has not changed. Whilst other sections have added caveats and things such as referees, it doesn't matter if this section does not reflect it. Previously in the specification it also mentioned using further data sources and fraud checks to improve demographic coverage. In that regard you have 3 leversy you can use for identity resolution, 1) the strength of the identity of the identity evidence, 3) what other fraud or data checks the CSP needs to perform in order to meet the risk appetite in confirming the existence of the identity for each IAL. We added exactly the stebiliship to the Live equivalent of 800-63 (linown as 6 RG 45 - https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual/how-to-prove-and-verify-someones-identity), in that we use levelshilly to the Live equivalent of 800-63 (linown as 6 RG 45 - https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual/how-to-prove-and-verify-someones-identity), in that we use this are social confidence levels which are analogous to IALs and created 'profiles' (https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual/identity-profiles) that set out the various waxs that a CSP can meet a secretic confidence levels based on varying different checks and stributes when it suits them. This simply can note be the case, core attributes must only be the minimum set of common attributes needed in order to create an admit with the CSP and they must be validated; other attributes, whilst when they may be mandatory to be provided, are not core and in some cases may be self-asserted. For example core attributes may be self-asserted with they may be mandatory to be provided, are not core and in some cases may be self-asserted. For example core attributes may be self-asserted asserted in dentity in the self-asserted asserted in dentity in the self-asserted asserted asserted asserted asserted asserted in dentity in the
such as referees, it doesn't matter if this section does not reflect it. Previously in the specification it also mentioned using further data sources and fraud checks to improve demographic coverage. In that regard you have 3 levers you can use for identity resolution, 1) the strength of the identity evidence needed, whether that is provided by the claimant or taken from an authoritative source, 2) how well the CSP confirms the authenticity of the identity evidence, 3) what other fraud or data checks the CSP needs to perform in order to meet the risk appetite in confirming the existence of the identity for each IAL. We added exactly this flexibility to the UK equivalent of 800-63 (known as GPG 45-https://www.gov.uk/government/publications/identity-profing-and-verification-of-an-individual/how-to-prove-and-verify-someones-identity), in that we use confidence levels sand or availage different checks and statistic when it suits the warrist was was that a CSP can meet a specific confidence levels based on varining different checks and attribute when it suits them. This simplication-of-an-individual/identity-profiles) that set out the various wasys that a CSP can meet a specific confidence levels based on varining different checks and attribute when it suits them. This simplifience levels based on varining different checks and attributes and the various wasys that a CSP can meet a specific confidence levels based on varining different checks and attributes may be self-asserted.  534 5.4.2.2 28 110 This seems at odds with the rest of the specification, it seems to display the minimum set of common attributes meeded in order to create an account with the CSP and they must be validated; other attributes, whilst when they may be mandatory to be provided an one cases may be self-asserted. For example cone attributes may be self asserted or examined the providence of the second of the providence providence provided must include better solution, with the decision of the second of the second of the second of the second of t
such as referees, it doesn't matter if this section does not reflect it. Previously in the specification it also mentioned using further data sources and fraud checks to improve demographic coverage. In that regard you have 3 levers you can use for identity resolution, 1) the strength of the identity evidence needed, whether that is provided by the claimant or taken from an authoritative source, 2) how well the CSP confirms the authenticity of the identity evidence, 3) what other fraud or data checks the CSP needs to perform in order to meet the risk appetite in confirming the existence of the identity for each IAL. We added exactly this flexibility to the UK equivalent of 800-63 (known as GPG 45-https://www.gov.uk/government/publications/identity-profing-and-verification-of-an-individual/how-to-prove-and-verify-someones-identity), in that we use confidence levels sand or availage different checks and statistic when it suits the warrist was was that a CSP can meet a specific confidence levels based on varining different checks and attribute when it suits them. This simplication-of-an-individual/identity-profiles) that set out the various wasys that a CSP can meet a specific confidence levels based on varining different checks and attribute when it suits them. This simplifience levels based on varining different checks and attributes and the various wasys that a CSP can meet a specific confidence levels based on varining different checks and attributes may be self-asserted.  534 5.4.2.2 28 110 This seems at odds with the rest of the specification, it seems to display the minimum set of common attributes meeded in order to create an account with the CSP and they must be validated; other attributes, whilst when they may be mandatory to be provided an one cases may be self-asserted. For example cone attributes may be self asserted or examined the providence of the second of the providence providence provided must include better solution, with the decision of the second of the second of the second of the second of t
using further data sources and fraud checks to improve demographic coverage. In that regard you have 3 levers you can use for identity resolution, 3) the strength of the identity evidence needed, whether that is provided by the claimant or taken from an authoritative source, 2) how well the CSP confirms the authenticity of the identity evidence, 3) what other fraud or data checks the CSP needs to perform in order to meet the risk appetite in confirming the existence of the identity for each IAL. We added exactly this flexibility to the UK equivalent of 800-63 (known as GPG 45 - https://www.gov.uk/government/publiciations/identity-profine; and-verification-of-an-individual/how-to-prove-and-verify-someones-identity), in that we confidence levels, which are analogous to IALs and created 'profiles' (https://www.gov.uk/government/publiciations/identity-profine; and-verification-of-an-individual/identity-profiles) that set out the various wass that a CSP can meet a specific confidence levels, based on varyine different checks and.  63A 5.4.2.2 28 1107 This seems at odds with the rest of the specification, it seems to imply that an CSP can just accept any self asserted core attribute when it suits them. This simply can not be the case, core attributes must only be the minimum set of common attributes needed in order to create an account with the CSP and they must be validated, other attributes, whilst when they may be mandatory to be provided, are not core and in some cases may be self-asserted. For example core attributes may be self asserted without self-account maintenance purposes; in this case the name, DoB must be validated, as so must the address or She cause its used for resolution, but the phone number is not.  63A 5.4.3 28 1111 Validation requirements at IAL2 should be stronger than IAL1, the stronger evidence provided must include better security features which must be testing the CSPs, and the quality of the checks they are performing should be better sequirements at IAL2 should be stronger evidence provid
use for identity resolution, 1) the strength of the identity evidence, 3) what other fraud or data checks the CSP needs to perform in order to meet the risk appetite in confirming the existence of the identity for each IAL. We added exactly this flexibility to the UK equivalent of 800-63 (known as GPG 45 - https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual/how-to-prove-and-verify-somenes-identity), in that we use confidence levels, which are analogous to IALs and created 'profiles' (https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual/how-to-prove-and-verify-somenes-identity), in that we use confidence levels, which are analogous to IALs and created 'profiles' (https://www.gov.uk/government/publications/identity-proofing-and-n-individual/identity-profiles) that set out the various wavs that a CSP can meet a specific confidence levels based on varving different checks and  107 This seems at odds with the rest of the specification, it seems to imply that an CSP can just accept any self asserted core attributes when it usits them. This usits the many long that the CSP and they must be validated; other attributes, whilst when they may be mandatory to be provided, are not core and in some cases may be self-asserted. For example core attributes may be self asserted  63A 5.4.3 28 1111 Validation requirements at IAL2 should be stronger than IAL1, the stronger evidence provided must include better security features which must be test by the CSPs, and the quality of the checks they are performing should be better.  63A 5.4.1 29 1130 There's no performance requirements for the biometric system defined here, without that there is no way to ensure equirements that is inline with your risk appetite for IAL1 equivalence between CSPs. The peak of the checks they are performing should be better.  63A 5.4.5 29 1130 This section is the same in every IAL, therefore it should be i
taken from an authoritative source, 2) how well the CSP confirms the authenticity of the identity evidence, 3) what other fraud or data checks the CSP needs to perform in order to meet the risk appetite in confirming the existence of the identity for each IAL. We added exactly this flexibility to the UK equivalent of 800-63 (known as GPG 45-https://www.go.uk/government/publications/identity-profing- and-verification-of-an-individual/how-to-prove-and-verify-someones-identity), in that we use confidence levels, which are analogous to IAIs and created 'profiles' (https://www.go.uk/government/publications/identity-profing-and-verification-of-an-individual/identity-profiles) that set out the various wax that a CSP can meet a soecific confidence levels based on varying different checks and  63A 5.4.2.2 28 1107 This seems at odds with the rest of the specification, it seems to imply that an CSP can just accept any self asserted core attributes when it suits them. This simply can not be the case, core attributes must only be the minimum set of common attributes when it suits them. This simply can not be the case, core attributes must only be the minimum set of common attributes when it suits them. This simply can not be the case, core attributes must only be the minimum set of common attributes when it suits them. This simply can not be the case, core attributes must only be the minimum set of common attributes and a phone number of the case and a sound in the CSP and they must be validated; other attributes, whilst when they may be mandatory to be provided, are not core and in some cases may be self-asserted. For example core attributes might just be 'name' and 'date of birth', with it being mandatory to provide at least one of 'address' or 'SSN' for identity resolution, and a phone number or contact and account maintenance purposes; in this case the name, DoB must be validated, as so must the address or SSN because its used for resolution, but the phone number is not.  63A 5.4.3 28 1111 Validation requirements at IAI
taken from an authoritative source, 2) how well the CSP confirms the authenticity of the identity evidence, 3) what other fraud or data checks the CSP needs to perform in order to meet the risk appetite in confirming the existence of the identity for each IAL. We added exactly this flexibility to the UK equivalent of 800-63 (known as GPG 45-https://www.gov.uk/government/publications/identity-profing- and-verification-of-an-individual/loidentity-profiles) that set out the various wax that a CSP can meet a specific confidence levels shich are analogous to IAIs and created 'profiles' (https://www.gov.uk/government/publications/identity-profing-and-verification-of-an-individual/loidentity-profiles) that set out the various wax that a CSP can meet a specific confidence levels based on varying different checks and stribute when it suits them. This simply can not be the case, core attributes must only be the minimum set of common attribute when it suits them. This simply can not be the case, core attributes must only be the minimum set of common attributes when it suits them. This simply can not be the case, core attributes must only be the minimum set of common attributes when it suits them. This simply can not be the case, core attributes must only be the minimum set of common attributes when it suits them. This simply can not be the case, core attributes must not be evidence provided in order to create an account with the CSP and they must be validated; other attributes, whilst when they may be mandatory to be provided, are not core and in some cases may be self-asserted. For example core attributes might just be 'name' and 'date of birth', with it being mandatory to provide at least one of 'address' or 'SSN' for identity resolution must attribute and a phone number for contact and account maintenance purposes; in this case the name, DoB must be validated, as so must the address or SSN because its used for resolution, but the phone number is not.
fraud or data checks the CSP needs to perform in order to meet the risk appetite in confirming the existence of the identity for each IAL. We added exactly this flexibility to the UK equivalent of 800-63 (known as GPG 45 - https://www.gov.uk/govormment/publications/identity-profing-and-verification-of-an-individual/how-to-prove-and-verify-someones-identity), in that we use confidence levels, which are analogous to IALs and created 'profiles' (https://www.gov.uk/govormment/publications/identity-profing-and-verification-of-an-individual/identity-profiles) that set out the various wavs that a CSP can meet a specific confidence levels, based on varvine different checks and set the various wavs that a CSP can meet a specific confidence levels hased on varvine different checks and stribute when it suits them. This simply can not be the case, core attributes must only be the minimum set of common attributes needed in order to create an account with the CSP and they must be validated; other attributes, whilst when they may be mandatory to be mandatory to provide at least one of 'address' or 'SSN' for identity resolution, and a phone number for contact and account maintenance purposes; in this case the name, DoB must be validated, as so must the address or SSN because its used for resolution, but the phone number is not.  63A 5.4.3 28 1111 Validation requirements at IAL2 should be stronger than IAL1, the stronger evidence provided must include better. Security features which must be tested by the CSPs, and the quality of the checks they are performing should be better. Security features which must be tested by the CSPs, and the quality of the checks they are performing should be better. Security features which must be tested by the CSPs, and the quality of the checks they are performing should be better. Security features which must be tested by the CSPs, and the quality of the checks they are performing should be better. Security features which must be steaded by the CSPs, and the quality of the checks they are perform
identity for each IAL. We added exactly this flexibility to the UK equivalent of 800-63 (known as GPC 45 https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual/how-to-prove-and-verify-someones-identity), in that we use confidence levels, which are analogous to IALs and created 'profiles' (https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual/identity-profiles) that set out the various wavs that a CSP can meet a specific confidence levels, which are analogous to IALs and created 'profiles' (https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual/identity-profiles) that set out the various wavs that a CSP can meet a specific confidence levels based on varying different cheeks and  5.4.2.2 28 1107 This seems at odds with the rest of the specification, it seems to imply that an CSP can just accept any self asserted core attribute when it suits them. This simply can not be the case, core attributes must only be the minimum set of common attributes have needed in order create an account with the CSP and they must be validated; other attributes, whilst when they may be mandatory to be provided, are not core and in some cases may be self-asserted. For example core attributes might just be 'name' and 'date of birth', with it being mandatory to provide at least one of 'address' or 'SSN' for identity resolution, and a phone number for contact and account maintenance purposes; in this case the name, DoB must be validated, as so must the address or SSN because its used for resolution, but the phone number is not.  63A 5.4.3 28 1111 Validation requirements along the self-acceptance requirements for the biometric system defined here, without that there is no way to ensure evidence provided must include better.  63A 5.4.4.1 29 1130 Three's no performance requirements for the biometric system defined here, without that there is no way to ensure evidence provided must include better.  63A 5.4.5 29 1139 This sec
https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual/how-to-prove-and-verify-someones-identity), in that we use confidence levels, which are analogous to IALs and created profiles!  (https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual/identity-profiles) that set out the various ways that a CSP can meet a specific confidence levels based on varying different checks and  5.4.2.2 28 1107 This seems at odds with the rest of the specification, it seems to limply that an CSP can just accept any self asserted core attributes when it suits then est of the specification to be the case, core attributes must only be the minimum set of common attributes needed in order to create an account with the CSP and they must be validated; other attributes, whilst when they may be mandatory to be provided, are not core and in some cases may be self-asserted. For example core attributes may be self asserted within the core and in some cases may be self-asserted. For example core attributes may be self asserted within the service of "SSN" for identity resolution, and a phone number for contact and account maintenance purposes; in this case the name, DoB must be validated, as so must the address or SSN because its used for resolution, but the phone number is not.  63A 5.4.3 28 1111 Validation requirements at IAL2 should be stronger than IAL1, the stronger evidence provided must include better security features which must be tested by the CSPs, and the quality of the checks they are performing should be better.  63A 5.4.1 29 1130 There's no performance requirements for the biometric system defined here, without that there is no way to ensure equivalence between CSPs. The performance at IAL2 does not have to be as strict for those at IAL3, but higher than IAL1.  63A 5.4.5 29 1139 This section is the same in every IAL, therefore it should be in a general "CSP requirements" section and not here equivalence between CSPs. The performance at IAL2 does not hav
verify-someones-identity), in that we use confidence levels, which are analogous to IALS and created 'profiles' (https://www.gov.uk/government/publications/identity-profiles) that set out the various wavs that a CSP can meet a specific confidence levels based on varving different checks and 1107 This seems at odds with the rest of the specification, it seems to imply that an CSP can just accept any self asserted core attributes ment it suits them. This simply can not be the case, ore attributes must only be the minimum set of common attributes needed in order to create an account with the CSP and they must be validated; other attributes, whilst when they may be mandatory to be provided, are not core and in some cases may be self-asserted. For example core attributes might just be 'name' and 'date of birth', with being mandatory to provide at least one of 'address' or 'SSN' for identity resolution, and a phone number for contact and account maintenance purposes; in this case the name, DoB must be validated, as so must the address or SSN because its used for resolution, but the phone number is not.    63A
verify-someones-identity), in that we use confidence levels, which are analogous to IALS and created 'profiles' (https://www.gov.uk/government/publications/identity-profiles) that set out the various wavs that a CSP can meet a specific confidence levels based on varving different checks and 1107 This seems at odds with the rest of the specification, it seems to imply that an CSP can just accept any self asserted core attributes ment it suits them. This simply can not be the case, ore attributes must only be the minimum set of common attributes needed in order to create an account with the CSP and they must be validated; other attributes, whilst when they may be mandatory to be provided, are not core and in some cases may be self-asserted. For example core attributes might just be 'name' and 'date of birth', with being mandatory to provide at least one of 'address' or 'SSN' for identity resolution, and a phone number for contact and account maintenance purposes; in this case the name, DoB must be validated, as so must the address or SSN because its used for resolution, but the phone number is not.    63A
Comparison of the control of the c
set out the various ways that a CSP can meet a specific confidence levels based on varying different checks and  5.4.2.2 28 1107 This seems at odds with the rest of the specification, it seems to imply that an CSP can just accept any self asserted core attributes when it suits them, this simply can not be the case, core attributes must only be the minimum set of common attributes needed in order to create an account with the CSP and they must be validated; other attributes, whilst when they may be mandatory to be provided, are not core and in some cases may be self-asserted. For example core attributes may be self asserted within the common attributes may be mandatory to be provided, are not core and in some cases may be self-asserted. For example core attributes may be self asserted within the core attributes may be mandatory to be provided, are not core and in some cases may be self-asserted. For example core attributes may be self asserted within the core attributes may be self asserted or attributes may be self asserted with the core attributes may be self asserted or attributes m
5.4.2.2   28   1107   This seems at odds with the rest of the specification, it seems to imply that an CSP can just accept any self asserted core attributes must only be the minimum set of common attributes needed in order to create an account with the CSP and they must be validated; other attributes, whilst when they may be mandatory to be provided, are not core and in some cases may be self-asserted. For example core attributes might just be 'name' and 'date of birth', with it being mandatory to provide at least one of 'address' or 'SSN' for identity resolution, and a phone number for contact and account maintenance purposes; in this case the name, DoB must be validated, as so must the address or SSN because its used for resolution, but the phone number is not.    63A
attribute when it suits them. This simply can not be the case, core attributes must only be the minimum set of common attributes needed in order to create an account with the CSP and they must be validated; other attributes, whilst when they may be self-asserted. For example core attributes might just be 'name' and 'date of birth', with it being mandatory to provide at least one of 'address' or 'SSN' for identity resolution, and a phone number for contact and account maintenance purposes; in this case the name, DoB must be validated, as so must the accessor SSN because its used for resolution, but the phone number is not.  63A 5.4.3 28 1111 Validation requirements at IAL2 should be stronger than IAL1, the stronger evidence provided must include better security features which must be tested by the CSPs, and the quality of the checks they are performing should be better.  63A 5.4.4.1 29 1130 There's no performance requirements for the biometric system defined here, without that there is no way to ensure equivalence between CSPs. The performance at IAL2 does not have to be as strict for those at IAL3, but higher than IAL1.  63A 5.4.5 29 1139 This section is the same in every IAL, therefore it should be in a general "CSP requirements" section and not here does not not here of the state of the provided, belancing it with validation of the validation of validation of validation of validation of validation of validati
attributes needed in order to create an account with the CSP and they must be validated; other attributes, whilst when they may be mandatory to be provided, are not core and in some cases may be self-asserted. For example core attributes might just be 'amen' and 'date of birth', with it being mandatory to provide at least one of 'address' or 'SSN' for identity resolution, and a phone number for contact and account maintenance purposes; in this case the name, DoB must be validated, as so must the address or SSN because its used for resolution, but the phone number is not.    63A   5.4.3   28   1111 Validation requirements at IAL2 should be stronger than IAL1, the stronger evidence provided must include better security features which must be tested by the CSPs, and the quality of the checks they are performing should be better.    63A   5.4.1   29   1130   There's no performance at IAL2 does not have to be as strict for those at IAL3, but higher than IAL1.    63A   5.4.5   29   1139   This section is the same in every IAL, therefore it should be in a general "CSP requirements" section and not here does not not here of the strict or they date was to introduce more ways to get a did greater flexibility to the evidence that can be provided, balancing it with validation or the validation process for IAL2 than IAL1.    63A   5.5.1   30   1157   This evidence selection is quite restrictive, one of the stated aims of the update was to introduce more ways to get a dod greater flexibility to the evidence that can be provided, balancing it with validation process.
attributes needed in order to create an account with the CSP and they must be validated; other attributes, whilst when they may be mandatory to be provided, are not core and in some cases may be self-asserted. For example core attributes might just be 'mane' and 'date of birth', with it being mandatory to provide at least one of 'address' or 'SSN' for identity resolution, and a phone number for contact and account maintenance purposes; in this case the name, DoB must be validated, as so must the address or SSN because its used for resolution, but the phone number is not.  1111 Validation requirements at IAL2 should be stronger than IAL1, the stronger evidence provided must include better security features which must be tested by the CSPs, and the quality of the checks they are performing should be better.  1130 There's no performance requirements for the biometric system defined here, without that there is no way to ensure equivalence between CSPs. The performance at IAL2 does not have to be as strict for those at IAL3, but higher than IAL1.  1131 This section is the same in every IAL, therefore it should be in a general "CSP requirements" section and not here (Move to section 5.1)  1132 This section is quite restrictive, one of the stated aims of the update was to introduce more ways to get a Add greater flexibility to the evidence that can be provided, balancing it with validation.
they may be mandatory to be provided, are not core and in some cases may be self-asserted. For example core attributes might just be 'name' and 'date of birth', with it being mandatory to provide at least one of 'address' or 'SSN' for identity resolution, and a phone number for contact and account maintenance purposes; in this case the name, DoB must be walldated, as so must the address or SSN because its used for resolution, but the phone number is not.    63A   5.4.3   28   1111 Validation requirements from the properties of t
might just be 'name' and 'date of birth', with it being mandatory to provide at least one of 'address' or 'SSN' for identity resolution, and a phone number for contact and account maintenance purposes; in this case the name, DoB must be validated, as 5 must the address or SSN because its used for resolution, but the phone number is not.  63A 5.4.3 28 1111 Validation requirements at IAL2 should be stronger than IAL1, the stronger evidence provided must include better security features which must be tested by the CSPs, and the quality of the checks they are performing should be better.  63A 5.4.1 29 1130 There's no performance remember for the biometric system defined here, without that there is no way to ensure equivalence between CSPs. The performance at IAL2 does not have to be as strict for those at IAL3, but higher than IAL1.  63A 5.4.5 29 1139 This section is the same in every IAL, therefore it should be in a general "CSP requirements" section and not here  63A 5.5.1 29 1148 This section is quite restrictive, one of the stated aims of the update was to introduce more ways to get a Add greater flexibility to the evidence that can be provided, balancing it with validation
resolution, and a phone number for contact and account maintenance purposes; in this case the name, DoB must be will display as so must the address or SSS because its used for resolution, but the phone number is not.  1111 Validation requirements at IAL2 should be stronger than IAL1, the stronger evidence provided must include better security features which must be tested by the CSPs, and the quality of the checks they are performing should be better.  1120 Significant of the biometric system defined here, without that there is no way to ensure equivalence between CSPs. The performance at IAL2 does not have to be as strict for those at IAL3, but higher than IAL1.  1121 Significant or some significant is the same in every IAL, therefore it should be in a general "CSP requirements" section and not here  1122 Significant or some significant is the same in every IAL, therefore it should be in a general "CSP requirements" section and not here  1123 Significant is the same in every IAL, therefore it should be in a general "CSP requirements" section and not here  1124 Significant is the same in every IAL, therefore it should be in a general "CSP requirements" section and not here  1125 Significant is the same in every IAL, therefore it should be in a general "CSP requirements" section and not here  1126 Significant is the same in every IAL, therefore it should be in a general "CSP requirements" section and not here  1227 Significant is the same in every IAL, therefore it should be in a general "CSP requirements" section and not here  1228 Significant is the same in every IAL should be in a general "CSP requirements" section and not here  1229 Significant is the same in every IAL should be in a general "CSP requirements" section and not here  1229 Significant is the same in every IAL should be in a general "CSP requirements" section and not here  1220 Significant is the same in every IAL should be in a general "CSP requirements" section and not here  1220 Significant is the same in every IAL should be in a general "CSP
validated, as so must the address or SSN because its used for resolution, but the phone number is not.   5.4.3   28   1111 Validation requirements at IAL2 should be stronger than IAL1, the stronger evidence provided must include better security features which must be tested by the CSPs, and the quality of the checks they are performing should be better.   63A   5.4.4.1   29   1130 There's no performance requirements for the biometric system defined here, without that there is no way to ensure equivalence between CSPs. The performance at IAL2 does not have to be as strict for those at IAL3, but higher than IAL1.   63A   5.4.5   29   1139 This section is the same in every IAL, therefore it should be in a general "CSP requirements" section and not here   Move to section 5.1     63A   5.5.1   29   1148 This section is the same in every IAL, therefore it should be in a general "CSP requirements" section and not here   Move to section 5.1     63A   5.5.2.1   30   1157 This evidence selection is quite restrictive, one of the stated aims of the update was to introduce more ways to get a   Add greater flexibility to the evidence that can be provided, balancing it with validation
validated, as so must the address or SSN because its used for resolution, but the phone number is not.   5.4.3   28   1111 Validation requirements at IAL2 should be stronger than IAL1, the stronger evidence provided must include better security features which must be tested by the CSPs, and the quality of the checks they are performing should be better.   63A   5.4.4.1   29   1130 There's no performance requirements for the biometric system defined here, without that there is no way to ensure equivalence between CSPs. The performance at IAL2 does not have to be as strict for those at IAL3, but higher than IAL1.   63A   5.4.5   29   1139 This section is the same in every IAL, therefore it should be in a general "CSP requirements" section and not here   Move to section 5.1     63A   5.5.1   29   1148 This section is the same in every IAL, therefore it should be in a general "CSP requirements" section and not here   Move to section 5.1     63A   5.5.2.1   30   1157 This evidence selection is quite restrictive, one of the stated aims of the update was to introduce more ways to get a   Add greater flexibility to the evidence that can be provided, balancing it with validation
5.4.3   28
security features which must be tested by the CSPs, and the quality of the checks they are performing should be better.  5.4.4.1 29 1130 Finer's no performance requirements for the biometric system defined here, without that there is no way to ensure equivalence between CSPs. The performance at IAL2 does not have to be as strict for those at IAL3, but higher than IAL1.  63A 5.4.5 29 1139 This section is the same in every IAL, therefore it should be in a general "CSP requirements" section and not here  63A 5.5.1 29 1148 This section is the same in every IAL, therefore it should be in a general "CSP requirements" section and not here  63A 5.5.2.1 30 1157 This evidence selection is quite restrictive, one of the stated aims of the update was to introduce more ways to get a Add greater flexibility to the evidence that can be provided, balancing it with validation
63A 5.4.1 29 1130 There's no performance requirements for the biometric system defined here, without that there is no way to ensure equirements that is inline with your risk appetite for IAL1 63A 5.4.5 29 1139 This section is the same in every IAL, therefore it should be in a general "CSP requirements" section and not here 63A 5.5.1 29 1148 This section is the same in every IAL, therefore it should be in a general "CSP requirements" section and not here 63A 5.5.1 30 1157 This evidence selection is quite restrictive, one of the stated aims of the update was to introduce more ways to get a 64d greater flexibility to the evidence that can be provided, balancing it with validation
equivalence between CSPs. The performance at IAL2 does not have to be as strict for those at IAL3, but higher than IAL1.  63A 5.4.5 29 1139 This section is the same in every IAL, therefore it should be in a general "CSP requirements" section and not here  63A 5.5.1 29 1148 This section is the same in every IAL, therefore it should be in a general "CSP requirements" section and not here  63A 5.5.1 30 1157 This evidence selection is quite restrictive, one of the stated aims of the update was to introduce more ways to get a  63A 5.5.1 30 1157 This evidence selection is quite restrictive, one of the stated aims of the update was to introduce more ways to get a  63A 5.5.2 30 1157 This evidence selection is quite restrictive, one of the stated aims of the update was to introduce more ways to get a
63A 5.4.5 29 1139 This section is the same in every IAL, therefore it should be in a general "CSP requirements" section and not here Move to section 5.1 63A 5.5.1 29 1148 This section is the same in every IAL, therefore it should be in a general "CSP requirements" section and not here Move to section 5.1 63A 5.5.2.1 30 1157 This evidence selection is quite restrictive, one of the stated aims of the update was to introduce more ways to get a Add greater flexibility to the evidence that can be provided, balancing it with validation
63A 5.5.1 29 1148 This section is the same in every IAL, therefore it should be in a general "CSP requirements" section and not here Move to section 5.1 63A 5.5.2.1 30 1157 This evidence selection is quite restrictive, one of the stated aims of the update was to introduce more ways to get a Add greater flexibility to the evidence that can be provided, balancing it with validation
63A 5.5.1 29 1148 This section is the same in every IAL, therefore it should be in a general "CSP requirements" section and not here Move to section 5.1 63A 5.5.2.1 30 1157 This evidence selection is quite restrictive, one of the stated aims of the update was to introduce more ways to get a Add greater flexibility to the evidence that can be provided, balancing it with validation
63A 5.5.2.1 30 1157 This evidence selection is quite restrictive, one of the stated aims of the update was to introduce more ways to get a Add greater flexibility to the evidence that can be provided, balancing it with validation
digital identity but the care of the specification has not changed. Whilet other continue have added correct and things. What output is described
digital identity but the core of the specification has not changed. Whilst other sections have added caveats and things what extent is dependent on your risk appetite.
such as referees, it doesn't matter if this section does not reflect it. Previously in the specification it also mentioned
using further data sources and fraud checks to improve demographic coverage. In that regard you have 3 levers you can
use for identity resolution, 1) the strength of the identity evidence needed, whether that is provided by the claimant or
taken from an authoritative source, 2) how well the CSP confirms the authenticity of the identity evidence, 3) what other
fraud or data checks the CSP needs to perform in order to meet the risk appetite in confirming the existence of the
identity for each IAL. We added exactly this flexibility to the UK equivalent of 800-63 (known as GPG 45 -
https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual/how-to-prove-and-
verify-someones-identity), in that we use confidence levels, which are analogous to IALs and created 'profiles'
Verni y-someones-relentity), in that we use commence revers, with a releasing out to this and oreacted priorites  (https://www.gov.uk/goverment/publications/identity-proofing-and-verification-of-an-individual/identity-profiles) that
set out the various ways that a CSP can meet a specific confidence levels based on varying different checks and
63A 5.5.2.2 30 1160 This seems at odds with the rest of the specification, it seems to imply that an CSP can just accept any self asserted core Change this to say that all attributes that are core, or used for identity resolution must
63A 5.5.2.2 30 1160 This seems at odds with the rest of the specification, it seems to imply that an CSP can just accept any self asserted core Change this to say that all attributes that are core, or used for identity resolution must
5.5.2.2 30 1160 This seems at odds with the rest of the specification, it seems to imply that an CSP can just accept any self asserted core Change this to say that all attributes that are core, or used for identity resolution must attribute when it suits them. This simply can not be the case, core attributes must only be the minimum set of common attributes may be self asserted
63A 5.5.2.2 30 1160 This seems at odds with the rest of the specification, it seems to imply that an CSP can just accept any self asserted core change this to say that all attributes that are core, or used for identity resolution must attribute when it suits them. This simply can not be the case, core attributes must only be the minimum set of common attributes needed in order to create an account with the CSP and they must be validated; other attributes, whilst when
63A 5.5.2.2 30 1160 This seems at odds with the rest of the specification, it seems to imply that an CSP can just accept any self asserted core attributes when it suits them. This simply can not be the case, core attributes must only be the minimum set of common attributes may be self asserted attributes may be self asserted they may be mandatory to be provided, are not core and in some cases may be self-asserted. For example core attributes
63A 5.5.2.2 30 1160 This seems at odds with the rest of the specification, it seems to imply that an CSP can just accept any self asserted core change this to say that all attributes that are core, or used for identity resolution must attribute when it suits them. This simply can not be the case, core attributes must only be the minimum set of common attributes needed in order to create an account with the CSP and they must be validated; other attributes, whilst when
5.5.2.2 30 1160 This seems at odds with the rest of the specification, it seems to imply that an CSP can just accept any self asserted core attributes when it suits them. This simply can not be the case, core attributes must only be the minimum set of common attributes needed in order to create an account with the CSP and they must be validated; other attributes, whilst when they may be mandatory to be provided, are not core and in some cases may be self-asserted. For example core attributes must be 'name' and 'date of birth', with it being mandatory to provide at least one of 'address' or 'SSN' for identity
63A  5.5.2.2  30  1160 This seems at odds with the rest of the specification, it seems to imply that an CSP can just accept any self asserted core attributes when it suits them. This simply can not be the case, core attributes must only be the minimum set of common attributes needed in order to create an account with the CSP and they must be validated; other attributes, whilst when they may be mandatory to be provided, are not core and in some cases may be self-asserted. For example core attributes might just be 'name' and 'date of birth', with it being mandatory to provide at least one of 'address' or 'SSN' for identity resolution, and a phone number for contact and account maintenance purposes; in this case the name, DoB must be
5.5.2.2 30 1160 This seems at odds with the rest of the specification, it seems to imply that an CSP can just accept any self asserted core attributes must only be the minimum set of common attributes ment only be the minimum set of common attributes may be self asserted attributes may be self asserted attributes may be mandatory to be provided, are not core and in some cases may be self-asserted. For example core attributes might just be 'name' and 'date of birth', with it being mandatory to provide at least one of 'address' or 'SSN' for identity resolution, and a phone number for contact and account maintenance purposes; in this case the name, DoB must be validated, as so must the address or SSN because its used for resolution, but the phone number is not.
55.2.2   30   1160 This seems at odds with the rest of the specification, it seems to imply that an CSP can just accept any self asserted core can attribute shear at the seed of common attribute when it suits them. This simply can not be the case, core attributes must only be the minimum set of common attributes needed in order to create an account with the CSP and they must be validated; other attributes, whilst when they may be mandatory to be provided, are not core and in some cases may be self-asserted. For example core attributes might just be 'name' and 'to be 'provided, are not core and in some cases may be self-asserted. For example core attributes might just be 'name' and 'to be 'provided, are not core and in some cases may be self-asserted. For example core attributes might just be 'name' and 'to be 'name' and 'to be 'now' and the provided in the self-asserted. For example core attributes might just be 'name' and 'to be 'n
5.5.2.2   30   1160 This seems at odds with the rest of the specification, it seems to imply that an CSP can just accept any self asserted core change this to say that all attributes that are core, or used for identity resolution must attribute when it suits them. This simply can not be the case, core attributes, whilst when they may be mandatory to be provided, are not core and in some cases may be self-asserted. For example core attributes might just be 'name' and 'date of birth', with it being mandatory to provide at least one of 'address' or 'SSN' for identity resolution, and a phone number for contact and account maintenance purposes; in this case the name, DoB must be validated, as so must the address or SSN because its used for resolution, but the phone number is not.    63A   5.5.3.1   30   1164 Validation requirements at IAL3 should be stronger evidence provided must include better security features which must be tested by the CSPs, and the quality of the checks they are performing should be better.
5.5.2.2   30   1160 This seems at odds with the rest of the specification, it seems to imply that an CSP can just accept any self asserted core change this to say that all attributes that are core, or used for identity resolution must attribute when it suits them. This simply can not be the case, core attributes, whilst when they may be mandatory to be provided, are not core and in some cases may be self-asserted. For example core attributes might just be iname' and 'date of birth', with it being mandatory to provide at least one of 'address' or 'SSN' for identity resolution, and a phone number for contact and account maintenance purposes; in this case the name, DoB must be validated, as so must the address or SSN because its used for resolution, but the phone number is not.    63A
5.5.2.2   30   1160 This seems at odds with the rest of the specification, it seems to imply that an CSP can just accept any self asserted core attributes must only be the minimum set of common attributes meeded in order to create an account with the CSP and they must be validated; other attributes, whilst when they may be mandatory to be provided, are not core and in some cases may be self-asserted. For example core attributes might just be 'name' and 'date of birth', with it being mandatory to provide at least one of 'address' or 'SSN' for identity resolution, and a phone number for contact and account maintenance purposes; in this case the name, DoB must be validated, as so must the address or SSN because its used for resolution, but the phone number is not.    63A   5.5.3.1   30   1164 Validation requirements at IAL3 should be stronger evidence provided must include better security features which must be tested by the CSPs, and the quality of the checks they are performing should be better.    63A   5.5.4   31   1187 There's no performance requirements for the biometric system defined here, without that there is no way to ensure   Add biometric performance requirements that is inline with your risk appetite for IAL1
5.5.2.2   30   1160 This seems at odds with the rest of the specification, it seems to imply that an CSP can just accept any self asserted core attributes must only be the minimum set of common attributes needed in order to create an account with the CSP and they must be validated; other attributes, whilst when they may be mandatory to be provided, are not core and in some cases may be self-asserted. For example core attributes might just be 'name' and 'date of birth', with it being mandatory to provide at least one of 'address' or 'SSN' for identity resolution, and a phone number for contact and account maintenance purposes; in this case the name, DoB must be validated, as so must the address or SSN because its used for resolution, but the phone number is not.    63A
55.2.2   30   1160 This seems at odds with the rest of the specification, it seems to imply that an CSP can just accept any self asserted core change this to say that all attributes that are core, or used for identity resolution must attribute when it suits them. This simply can not be the case, core attributes, whilst when they may be mandatory to be provided, are not core and in some cases may be self-asserted. For example core attributes might just be 'name' and 'date of birth', with it being mandatory to provide at least one of 'address' or 'SSN' for identity resolution, and a phone number for contact and account maintenance purposes; in this case the name, DoB must be validated, as so must the address or SSN because its used for resolution, but the phone number is not.    63A
5.5.2.2   30   1160 This seems at odds with the rest of the specification, it seems to imply that an CSP can just accept any self asserted core attributes must only be the minimum set of common attributes needed in order to create an account with the CSP and they must be validated; other attributes, whilst when they may be mandatory to be provided, are not core and in some cases may be self-asserted. For example core attributes might just be 'name' and 'date of birth', with it being mandatory to provide at least one of 'address' or 'SSN' for identity resolution, and a phone number for contact and account maintenance purposes; in this case the name, DoB must be validated, as so must the address or SSN because its used for resolution, but the phone number is not.    63A
5.5.2.2   30   1160 This seems at odds with the rest of the specification, it seems to imply that an CSP can just accept any self asserted core attributes may be self asserted. For example core attributes must be self asserted in order to create an account with the CSP and they must be validated; other attributes, whilst when they may be mandatory to be provided, are not core and in some cases may be self-asserted. For example core attributes might just be 'name' and 'total be in a simple of indivision, and a phone number for contact and account maintenance purposes; in this case the name, DoB must be validated, as so must the address or 'SSN because its used for resolution, but the phone number is not.    63A   5.5.3.1   30   1164 Validation requirements at IAL3 should be stronger than IAL2, the stronger evidence provided must include better security features which must be tested by the CSPs, and the quality of the checks they are performing should be better.   5.5.4   31   1182 There's no performance requirements for the biometric system defined here, without that there is no way to ensure equivalence between CSPs. The performance at IAL2 does not have to be as strict for those at IAL3, but higher than IAL1.   63A   8.1.1   40   1355   Its not clear what you mean by "knowledge of the SSN shall not be considered evidence", because certainly an SSN can   Make it clear what the statement means   1850   185
5.5.2.2   30   1160 This seems at odds with the rest of the specification, it seems to imply that an CSP can just accept any self asserted core attributes may be self asserted. For example core attributes must only be the minimum set of common attributes needed in order to create an account with the CSP and they must be validated; other attributes, whilst when they may be mandatory to be provided, are not core and in some cases may be self-asserted. For example core attributes might just be 'name' and 'date of birth', with it being mandatory to provide at least one of 'address' or 'SSN' for identity resolution, and a phone number for contact and account maintenance purposes; in this case the name, DoB must be validated, as so must the address or 'SSN because its used for resolution, but the phone number is not.    63A
5.5.2.2   30   1160 This seems at odds with the rest of the specification, it seems to imply that an CSP can just accept any self asserted core cattributes must be self asserted or attributes meded in order to create an account with the CSP and they must be validated; other attributes, whilst when they may be mandatory to be provided, are not core and in some cases may be self-asserted. For example core attributes might just be 'name' and 'cell of birth', with the leng mandatory to provide at least one of 'address' or 'SSN' for identity resolution, and a phone number for contact and account maintenance purposes; in this case the name, DoB must be will dated, as so must the address or SSN because its used for resolution, but the phone number is not.    63A

63A		10.2	52	1756	There's insufficient detail about how and whom may act as a referee, its been left open for the CSP to write their own	Clearly define the requirements to be a referee and how the reference is given to the CSP
					policy on it but that will lead to significant inconsistencies; one CSP may simply allow a "note from your parent" and the	
					specification says that will be ok as long as the CSP has written that into their policy. The specification needs to define	
					both how referee gives the reference to the CSP and what restrictions there are on being a referee.	
					We've written a guide for this in the UK, we've called them a vouch, but the concept is the same:	
					https://www.gov.uk/government/publications/how-to-accept-a-vouch-as-evidence-of-someones-identity/how-to-accept-	
					a-vouch-as-evidence-of-someones-identity	
63A		10.3	53	1790	This should not be encouraged, there are plenty of products on the market that do not demonstrate any significant bias,	replace "Providing risk-based alternative processes that compensate for residual bias" to "Replace image capture
					instead of compensating for a biased system the system should just be replaced with one that does not have such a bias	technology with one that does not demonstrate bias"
63A		10.3	53	1804	This should not be encouraged, there are plenty of products on the market that do not demonstrate any significant bias,	replace "Providing risk-based alternative processes that compensate for residual bias" to "Replace biometric algorithm
					instead of compensating for a biased system the system should just be replaced with one that does not have such a bias	with one that does not demonstrate bias"
63A	References		56	1875	There is an updated version of this specification here: https://www.gov.uk/government/publications/identity-proofing-	
					and-verification-of-an-individual	
63A	General				One of the stated objectives of the update is to broaden the demographic coverage and provide different routes to allow	
					people to get a digital identity. However we're not sure that this is reflected sufficiently in the guide as is, the core IAL	
					definitions haven't really changed and whilst some other clarifications have been added or updated around referees etc	
					we're not sure that the changes made so far will dramatically improve the coverage.	
63A	General				The guidance doesn't reflect some of the current services and technology that is available, in particular using fraud	
					services to manage risk and thereby allow users to use less than ideal sources of evidence or KBV etc as fraud checks	
					seem to be optional (which means they won't happen in real life) and if a CSP implements them it doesn't give them any	
					benefit in terms of reaching the IAL.	
63A	General				There aren't any controls about how KBV should work, which is probably needed since lots of services ask poor questions	
					that leave them open to impostors and account takeover	
63B	5.1.3		18	837	Is there a 3rd option where there is no secret exchange between the two devices, for example user accesses a service	Add OOB example without secret exchange between the devices
					from a computer, they enter their userID and PWD, then a challenge is sent to their registered app on their phone and	
					they authenticate using a biometric to the app, and then they can continue with their web session?	
63B	5.1.3.2		22	899	Is there a 3rd option where there is no secret exchange between the two devices, for example user accesses a service	Add OOB example without secret exchange between the devices
					from a computer, they enter their userID and PWD, then a challenge is sent to their registered app on their phone and	
					they authenticate using a biometric to the app, and then they can continue with their web session?	
63B	5.2.3		33		This sets an FMR rate but this must be paired with an FNMR.	Add appropriate FNMR
63B	5.2.3		33			Make SHALL
63B	5.2.3	Т	33	1284		Performance for different attack species or NIST SOFA levels should be defined.
					should be very effective at stopping attacks using photographs, but probably less effective at stopping full face latex	
					masks. NIST have another publication on this: https://pages.nist.gov/SOFA/SOFA.html which might be useful to use as a	