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 #	Line #	Comment (Include rationale for comment)	Suggested Change
	63-Base	Identity proofing and enrolment	iii	184	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 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	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 2 tier IAL2
	63-Base	4.3.1	18	773	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 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	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.
	63-Base	5.2.2.1	31	1198	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 IAL1 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 would be better to say it explicitly here for clarity.	This section should also say that organisation must introduce sufficient mitigations where they are 'tailoring' the service.
	63-Base	5.2.3.2	34	1295	"who they claim to be" is the "subscriber", so use that for consistency	replace "who they claim to be" with "subscriber"
	63-Base	5.3.2	37	1421	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. This is unhelpful as its then not possible to know when an IAL2 from CSP A is equivalent to an IAL2 from CSP B as they can 'tailor' their view of what IAL2 is. This encourages a race to the bottom as it would allow a CSP to cut corners, and cost, whilst claiming compliance to the same IAL, creating an unlevel playing field for CSPs. CSPs that are 'compliant' to the standard will be forced to also 'tailor' their service in order to match cost of cheaper CSPs that have 'tailored' out the expensive parts or higher friction steps. This will result in sub IAL digital identities and no way for the RP to know the difference, so will have to assume that every CSP provides the same sub-par service. If you want to allow organisations to tailor the IAL then you must set the boundaries of what that means and how short falls can be mitigated to ensure there is broadly equivalent between CSPs providing the same IAL. In that regard you have 4 basic levers you can use, 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, and 4) how well they verify the claimant as being the subject they claim to be. 1, 2, & 3 are part of the identity resolution process i.e. can the CSP be sure that the identity is of a real person, where 4 is the verification that the claimant is that person. If you want to allow the CSP to vary those things in a more dynamic way you need to set out what you think is acceptable in a more flexible way than the simple options currently given in 800-63. You may have noticed that 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' (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 processes.	The IALs should explicitly state which variations are allowed and what mitigations must be in place to ensure equivalence.
	63-Base	5.3.3	38	1454	This doesn't appear to have much value. As written there is no requirement in 800-63 to manage or monitor for fraud, its 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.	It should be mandatory to perform fraud checks, and respond with appropriate mitigating actions; which might include gathering further identity evidence, or increasing the verification controls.
	63-Base	A.1	46	1709	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	1910	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	1914	A mobile Driving Licence (mDL) would also be valid digital evidence	add mDL as a digital evidence example

	63-Base	A.1	56	2048	"subsystem" and "interfering" seems to imply that it would cover technical attacks such as an injection attack, or other cyber 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"
	63A	2.1	4	398	"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"
	63A	2.1	4	419	IAL3 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 tend 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 can only be done in person at the current time due to technical imitations. This will also future proof the specification.	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."
	63A	4.1.1	8	figure 1	Box 3 seems to have a typo, "evidence validation" should be "identity verified"	change "evidence validation" to "identity verified" in box 3
	63A	4.3	9	498	"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"
	63A	4.3	9	505	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 etc are acceptable.	Remove the acceptance of copies, photographs and scans from this section and add them as applicable to each IAL
	63A	4.3.1	10	517-522	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
	63A	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
	63A	4.3.2	10	526-541	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
	63A	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 bearer and the owner are the same person.	Remove point 5
	63A	4.3.3.1	11	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
	63A	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 certainly possible to use a recently expired passport to prove your identity to get a new one, which this requirement seems to prevent.	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."
	63A	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 bearer and the owner are the same person.	Remove point 3
	63A	4.3.4.1	12	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 IAL	Remove 4.3.4.1 and add details to 5.3.3, 5.4.3 & 5.5.3
	63A	4.3.4.3	13	623	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 - 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 Unit, Centre for the Protection of National Infrastructure (CPNI) or any other company that follows the Home Office's best practice guidance	Clarify what the training requirements are for each IAL
	63A	4.4	14	656	"and establish" seems superfluous, remove.	Remove "and establish"
	63A	5	16	689	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.
	63A	5.1.1.2	17	733	This should be mandatory, otherwise a) no one will do it because it costs money, 2) there is a growing risk from online fraud 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.
	63A	5.1.2.2	18	780	Its 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 its not secret and known by too many people.	Make it clear what the statement means
	63A	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,"
	63A	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"
	63A	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-a-vouch-as-evidence-of-someones-identity	Clearly define the requirements to be a referee and how the reference is given to the CSP
	63A	5.3.1	26	1046	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	5.3.2.1	26	1055	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. 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' (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	Add greater flexibility to the evidence that can be provided, balancing it with validation methods and fraud controls. To what extent is dependent on your risk appetite.
	63A	5.3.2.2	26	1057	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 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.	Change this to say that all attributes that are core, or used for identity resolution must be validated, other additional attributes may be self asserted
	63A	5.3.4	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 IAL1 does not have to be as strict for those at IAL2 or IAL3.	Add biometric performance requirements that is inline with your risk appetite for IAL1
	63A	5.3.5	27	1087	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	5.4.1	28	1096	This section is the same in every IAL, therefore it should be in a general "CSP requirements" section and not here	Move to section 5.1
	63A	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. 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' (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	Add greater flexibility to the evidence that can be provided, balancing it with validation methods and fraud controls. To what extent is dependent on your risk appetite.
	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 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.	Change this to say that all attributes that are core, or used for identity resolution must be validated, other additional 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 tested by the CSPs, and the quality of the checks they are performing should be better.	There must be stronger controls on the validation process for IAL2 than IAL1
	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.	Add biometric performance requirements 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	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 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 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' (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	Add greater flexibility to the evidence that can be provided, balancing it with validation methods and fraud controls. To what extent is dependent on your risk appetite.
	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 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 '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.	Change this to say that all attributes that are core, or used for identity resolution must be validated, other additional attributes may be self asserted
	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.	There must be stronger controls on the validation process for IAL3 than IAL2
	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 equivalence between CSPs. The performance at IAL2 does not have to be as strict for those at IAL3, but higher than IAL1.	Add biometric performance requirements that is inline with your risk appetite for IAL1
	63A	5.5.5	31	1192	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	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 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 its not secret and known by too many people.	Make it clear what the statement means

	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 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	Clearly define the requirements to be a referee and how the reference is given to the CSP
	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, instead of compensating for a biased system the system should just be replaced with one that does not have such a bias	replace "Providing risk-based alternative processes that compensate for residual bias" to "Replace image capture 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, instead of compensating for a biased system the system should just be replaced with one that does not have such a bias	replace "Providing risk-based alternative processes that compensate for residual bias" to "Replace biometric algorithm 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 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?	Add OOB example without secret exchange between the devices
	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 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?	Add OOB example without secret exchange between the devices
	63B	5.2.3	33	1281	This sets an FMR rate but this must be paired with an FNMR.	Add appropriate FNMR
	63B	5.2.3	33	1283	This should be a SHALL in order to have confidence in the system.	Make SHALL
	63B	5.2.3	33	1284	This doesn't really define the performance, it hasn't detailed the sophistication of the attack species, for example it 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	Performance for different attack species or NIST SOFA levels should be defined.