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

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

Organization:

Name of Submitter/POC:

Email Address of Submitter/POC:

Submitter	Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)
Appian	1	63-Base	2	4	389-390	"(1) is in control of the technologies being used for authentication, and (2) is the same subject that previously accessed the service." seems to be missing the concept "is who they claim to be" which helps establish "same subject". Provable posession of an authentication technology does not fully address this.
Appian	2	63-Base	2.1	5	435-437	"these technical guidelines do not address the identity of subjects for physical access (e.g., to buildings), though some identities used for online transactions may also be used for physical access." This is really out of step with what is actually done, where the difference between LACS and PACS is diminishing.
Appian	3	63-Base	4.1	13-14	657-681	The steps enumerated in Figure 2 are not the same enumerated steps described in the text.
Appian	4	63-Base	4.3.1	17	740-741	"For the purposes of these guidelines, using two factors is adequate to meet the highest security requirements." In many instances, three factors are required. "two factors is adequate" is insufficient.
Appian	5	63-Base	4.3.1	17	745-746	"The authenticators contain secrets the claimant can use to prove they are a legitimate subscriber." This whole section seems to suggest something you know is now on an authenticator token, not something you know in your own memory. Further, it only discusses secrets. What about biometrics as an authenticator to prove they are a legitimate subscriber?
Appian	6	63-Base	4.4.2	22	890	"Figure 2, the CSP provides a service known as an identity provider, or IdP." We must be very careful that this is NOT the only viable architecture. The IdP does not have to be the CSP. In fact, an IdP can be client of multiple CSPs, aggregating attribute information about an individual, and be a much greater value to the RP. In a Fido driven CSP environment, only the CSP can be the IdP as they are the only one that did the identity proofing and retain those attributes. This is a special case, not the norm.
Appian	7	63-Base	5.2.2.1	31	1203-1205	The definition of IAL3 does not include use of biometrics.
Appian	8	63-Base	5.2.2.2	31-32	1206-1218	"5.2.2.2. Authentication Assurance Level" We REALLY need an AAL0 that makes it clear that human memorized passwords as a single factor are of no authentication value. This is differentiated from an activation PIN which is used in concert with a private key.
Appian	9	63-Base	5.2.3.1	33	1252-1254	"Not all RP applications will require identity proofing. If the RP application does not require any personal information to execute any digital transactions, the system can operate without identity proofing users of the RP application." This indicates a need to define and use an IAL0.
Appian	10	63A	2.2	4	419-421	The gold standard for identity proofing is to include at least one biometric: facial, fingerprint, iris. This definition of IAL3 does not mention biometrics are required.
Appian	11	63A	4.1.1	8	464-473	Figure 1 starts the process with Resolution. Generally, the process begins with Enrollment. Then Identity Resolution as described in section 4.2. It is important to distinguish between the two because the IALx have such different requirements for enrollment. Identity Resolution is a difficult process on its own, confirming that all the collected evidenced from enrollment is actually the same individual. Also note the rest of 63A does not use "Resolution". It uses "Enrollment".
Appian	12	63A	4.1.1	8	481-482	3 a & 3 b require a biometric (facial) and that it is compared to the collected identity evidence using 1:1 matching. The definition of the IALx avoids the use of biometrics, but they really should be called out.
Appian	13	63A	4.3.3.2	11	576-577	"5. The evidence includes physical security features that make it difficult to copy or reproduce." This seems to explicitly exclude the use of digital credentials of any type, as this SHALL be met.
Appian	14	63A	4.3.3.3	12	595-596	"7. The evidence includes physical security features that make it difficult to copy or reproduce." This seems to explicitly exclude the use of digital credentials of any type, as this SHALL be met.
Appian	15	63A	4.2.4.3	12	620	This is actually a subsection of 4.2.4.2.
Appian	16	63A	4.2.4.4	12	629	This is actually a subsection of 4.2.4.2.
Appian	17	63A	5.1.6	21	868-872	"The following requirements apply to all CSPs that employ enrollment codes at any IAL: 1. Enrollment codes SHALL be sent to a validated address (e.g., postal address, telephone number, or email address). 2. The applicant SHALL present a valid enrollment code to complete the identity proofing process." 63A is trying to use enrollment codes as a means of maintaining a multi-part enrollment session to support identity validation. 63A SHOULD provide an alternative, as is specified in FIPS 201-3, to maintain a chain-of-trust using biometrics. This is especially important at IAL3 but may also impact IAL2. Enrollment codes as specified should NOT be acceptable for any IAL as is specified here.

Appian	18	63A	5.1.6	21	873-879	"3. Enrollment codes SHALL be comprised of one of the following: a) A random six digit number generated by an approved random number generator with at least 20 bits of entropy; b) A secure link delivered to a uniquely identified address containing an appropriately constructed session ID (at least 64 bits of entropy); or c) A machine readable optical label (such as a QR code) that contains a random secret with at least 20 bits of entropy." 20 bits of entropy is very weak. It should apply to IAL0, IAL1 only. 128 bits should be required for IAL2 and 256 bits should be required for IAL3
Appian	19	63A	5.1.6	21	880-886	"Validated Postal Address" is undefined. How exactly is a postal address considered validated. This also seems to explicitly exclude P.O. Boxes, including non-USPS service provider addresses and P.O. Boxes.
Appian	20	63A	5.1.9	24	984-987	"Since information provided by the applicant reference may be used and relied upon in the identity proofing of the applicant, the applicant reference is identity proofed to the same or higher IAL as the applicant." "...the applicant reference is identity proofed..." should be a SHALL.
Appian	21	63A	5.1.9	24	973-992	There is no discussion of the rather normal process where an individual has Power of Attorney (POA) to act on behalf of another individual. POA is the legal definition of someone who can be an applicant reference. Anyone who has gone through end-of-life support for a family member is very familiar with this process. And it is absent here, yet in those situations, may be critical to establish legal basis to represent the applicant.
Appian	22	63A	5.1.9.2	25	1004	"CSPs SHOULD allow the use of applicant references." This does not seem accurate in the situation of POA for an applicant.
Appian	23	63A	5.1.9.2	25	1010-1012	"...any requirements for the relationship between the reference and the applicant." is catch-all language placing the burden on the CSP to figure out any and all situations where an applicant reference is used and how that relationship is established.
Appian	24	63A	5.1.10	25	1021-1022	There is no definition of the legal requirements for an applicant reference to be bound to the minor in some way.
Appian	25	63A	5.1.10	25	1022	"...age or 18."
Appian	26	63A	5.2	25-26	1023-1035	There is no formal definition of IAL0, yet it was introduced earlier in section 2.2.
Appian	27	63A	5.3	26	1039	"...false negatives and application departures..." we are also worried about false positives where the attacker establishes an identity under false pretences as someone else.
Appian	28	63A	5.3.3	27	1065-1067	This language essentially mandates automated capabilities to look at microtype, digital watermarks, multi-spectral inks, etc. These automated techniques are rarely used to verify driver's licenses. This section exceeds the mandates of FIPS 201 for collection of a driver's license for identity proofing (which by these definitions is STRONG).
Appian	29	63A	5.4.2.1	28	1105	"...evidence" needs the or as is used in IAL1
Appian	30	63A	5.5.6	31	1197	"...for the purposes of non-repudiation and re-proofing." These are not the only purposes. In particular, biometrics are used for chain-of-trust from identity proofing, to issuance of the credential, and subsequent authentication using the credential. This statement is too limiting in how biometrics will actually be used.
Appian	31	63A	5.5.8	32	1221-1223	"4.The CSP SHALL require that all digital verification of evidence (e.g., via chip or wireless technologies) be performed by integrated scanners and sensors (e.g., embedded fingerprint reader)." This sentences mixes two different things inappropriately. First, digital evidence verification (via chip/wireless) performed using integrated credential readers and software to verify digital signatures on the digital evidence; Second, biometric 1:1 comparison of information stored on the digital evidence to the applicant via integrated scanners and sensors (e.g., fingerprint, facial, iris).
Appian	32	63A	6.1	34	1252-1253	"All authenticators currently bound to the subscriber account, whether registered at enrollment or subsequent to enrollment" Binding (registering) an authenticator as part of enrollment is not described nor a defined process in the definitions of IALx. If it is desired to bind an authenticator as part of enrollment, it should be defined and described per appropriate IALx. This is especially important for Fido tokens, where you MUST bind the Fido token public key to the subscriber account at time of enrollment. In general, Fido tokens are BYOD and this should be allowed.
Appian	33	63A	6.2	35	1268-1269	"...subscriber account through AAL2 or AAL3 authentication processes using authenticators registered to the subscriber account." First, if the CSP is for IAL1, requiring AAL2 or AAL3 is overkill. This should be graduated security requirements commensurate with the IAL of the subscriber account. AAL1 should be allowed for IAL1 subscriber accounts. Second, HOW the CSP binds the authenticator to the subscriber account is undefined.

Appian	34	63A	6.2	35	1270-1271	"The CSP SHALL provide the capability for subscribers to change or update the personal information contained in their subscriber account." This can not be met as intended for FIPS 201 compliant systems. After IAL3 is performed, that's it. No more changes from the applicant. There is not a self-service portal enabling the applicant to login and make changes. If there were one, what authenticator would be used? The claim of identity stands and is validated during background investigation. There are situations where the applicant goes to an authoritative source (HR, COR) to change there name/gender/home address/personal email. It is the authoritative source that initiates the change, not the applicant, within the FIPS 201 CSP subscriber account. Typically the applicant is re-enrolled at IAL3 to establish an authoritative link to the change.
Appian	35	63A	7.1	38	1319-1320	"Social Engineering" This definition of social engineering and its mitigation, described here, will not be effective against a core threat in Remote Identity Proofing for IAL1,2, most notably PHISHing. As a CSP, you can not stop an attacker from phishing your clientelle. Your trusted referrees or enrollment officials will have nothing to do with the attacker's actions and can not mitigate the attack.
Appian	36	63B	3	2	372-373	"It also provides recommendations on the lifecycle of authenticators, including revocation in the event of loss or theft." Lifecycle is way more than revocation. A cornerstone is the binding of a subscriber account to an authenticator at initial issuance. Subsequently the maintenance of that authenticator.
Appian	37	63B	3	2	375-377	"It does not address the authentication of a person for physical access (e.g., to a building), though some credentials used for digital access may also be used for physical access authentication." PACS are becoming authenticator and federation RPs and should NOT be excluded. They are a very important part of the ecosystem. It is not just about logical access.
Appian	38	63B	3	2	377-378	"This technical guideline also requires that federal systems and service providers participating in authentication protocols be authenticated to subscribers." What does this mean? Is it the intent that all uses of AALx shall be a mutually authenticated channel between subscriber and RP/SP?
Appian	39	63B	4	2	393	"...possession and control of two different authentication factors is required..." This is the first use of "authentication factors". What is this referring to? MFA meaning have/know/are? MFA meaning they are in posession and control of two separate authenticators?
Appian	40	63B	4	2	401-402	"In order to authenticate at AAL3, claimants are required to prove possession and control of two distinct authentication factors through secure authentication protocols." Here again is the use of undefined "authentication factors".
Appian	41	63B	4	6	428-430	"Subscriber identifiers SHOULD NOT be reused for a different subject but SHOULD be reused when a previously enrolled subject is re-enrolled by the CSP. Other attributes that identify the subscriber as a unique subject MAY also be provided." This appears to be an IAL requirement, not an AAL requirement, as it refers to re-enrollment by CSP. Likely the intent is that subscriber identifiers should be used by the service provider/relying party, as defined by AALx subscriber identifier that is defined by the CSP. If a CSP already knows the person and has subscriber identifiers, the CSP should most definitely re-use existing identifiers if the person re-enrolls. This is foundational to the federation ecosystem that depends on these identifiers as RPs.
Appian	42	63B	4.1.2	7	460	"...AAL1 SHALL use approved cryptography." Approved by who? Is there a list somewhere? Is this a FIPS 140 reference for approved cryptographic libraries and algorithms?
Appian	43	63B	4.1.2	7	468-469	This specifies verifiers to use FIPS 140 validated algorithms. Per comment on line 460, is FIPS 140 also required for authenticators?
Appian	44	63B	4.2.2	9	460	"...AAL2 SHALL use approved cryptography." Approved by who? Is there a list somewhere? Is this a FIPS 140 reference for approved cryptographic libraries and algorithms?
Appian	45	63B	4.2.3	9	551-552	"Reauthentication of a session that has not yet reached its time limit MAY require only a memorized secret or a biometric in conjunction with the still-valid session secret." This countermands the SHALL statements to use AAL2 during the time limits as defined in lines 545-550. It presents a significant relaxation of the authentication requiements.
Appian	46	63B	4.3.3	11	613-614	"Reauthentication SHALL use both authentication factors." This should specify re-use of the original AAL3 authenticator that started the session.

Appian	47	63B		Table 1	13	655-657		"Reauthentication" row uses the language of one or two factors of authentication instead of AALx authentication. It has always been a problem in NIST documents using have/know/are language (number of factors) in place of AALx language. This creates confusion. Just saying two factors does not mean you hit AAL2 or AAL3 for an authentication event. This document should use the language of AALx and leave the use of have/know/are to be within the definition of AALx. Using AALx, we could then see NIST SP800-116, or other related documents like FIPS 201, adopting IAL/AAL/FAL language consistently.
Appian	48	63B		Table 1	13	655-657		"Security Contols" row states the use of Low/Moderate/High. This table is informative, not normative. These controls should be made normative. The definitions within AAL1/2/3 state tailored controls per SP800-53, not referencing Low/Moderate/High decisions that fully guide control selection within SP800-53. The language of tailored controls still fits within this framework, but it adds considerable clarity for each AALx to be specific about L/M/H.
Appian	49	63B		5.1.1.2	16	766		"chosen arbitrarily" is not specific enough to ensure security of the salt and resulting hashed password.
Appian	50	63B		5.1.2.2	18	811		"arbitrarily chosen"
Appian	51	63B		5.1.4.1	24	969-970		"If a subscriber needs to change the device used for a software-based OTP authenticator, they SHOULD bind the authenticator application…" Re-binding an authenticator needs to be chain-of-trust based. It is usually not possible to do that when you replace a mobile device. The authenticator is wiped out on the old phone. This should be a SHALL.
Appian	52	63B		5.1.4.2	24	979 - 983		No discussion on HOW to protect symmetric keys.
Appian	53	63B		5.1.5.1	25-26	1024-1025		"…they SHOULD bind the authenticator application on the new device to their subscriber account…" Authenticators independent of identity should not be allowed. Chain-of-trust must be maintained.
Appian	54	63B		5.1.7.1	28	1098-1100		Export is not the only concern. Keys must also be generated on the token so no other party is ever knowledgeable of the secrets on the token.
Appian	55	63B		5.1.7.1	28	1107		"The challenge nonce SHALL be at least 64 bits in length." Crypto 101 says keep all keying material at equivalent security or the weakest is the resulting security of the transaction.
Appian	56	63B		5.1.7.1	28	1133		Because symmetric is allowed, need to protect keys in hardware storage.
Appian	57	63B		5.1.7.1	28	1134		"The challenge nonce SHALL be at least 64 bits in length…"
Appian	58	63B		5.1.9.1	30	1186		Export is not the only concern. Keys must also be generated on the token so no other party is ever knowledgeable of the secrets on the token.
Appian	59	63B		5.1.9.1	30	1196		"The challenge nonce SHALL be at least 64 bits in length."
Appian	60	63B		5.2.1	31	1229		"…upon notification from subscriber that loss or theft…" Must also include compromise of the authenticator.
Appian	61	63B		5.2.3	33	1306-1308		"Biometric comparison can be performed locally on the claimant's device or at a central verifier. Since the potential for attacks on a larger scale is greater at central verifiers, comparison SHOULD be performed locally." So far, this text requires either on-device-comparison or central verification. It does not allow for off-device-comparison by distributed verifiers (i.e. typical off-card-comparison as described in NIST SP800-73-4).
Appian	62	63B		5.2.3	33	1309-1313		"If comparison is performed centrally: •Use of the biometric as an authentication factor SHALL be limited to one or more specific devices that are identified using approved cryptography. Since the biometric has not yet unlocked the main authentication key, a separate key SHALL be used for identifying the device." This concept of off-device comparison for activation of the device introduces SIGNIFICANT issuance and verifier risk. If the device has constrained resources (e.g., smart card, USB dongle) it may not be able to handle asymmetric key processing and the required Trust Chain validation to ensure the keys presented are still valid.
Appian	63	63B		5.2.4	34	1328-1341		This concept of attestation is about manufacture of the authenticator, not about trust that the CSP (issuer) actually enabled the authenticator and put the authentication information on the device.
Appian	64	63B		5.2.9	37	1450-1453		"Depending on the modality, presentation of a biometric characteristic may or may not establish authentication intent. Behavioral biometrics similarly may or may not establish authentication intent because they do not always require a specific action on the claimant's part." Earlier on-device use of face/finger was allowed. This is truly not consistent and introduces confusion. Under what conditions would presentation of a biometric characteristic NOT establish authentication intent?

Appian	65	63B	5.2.10	38	1461-1463	"The use of a restricted authenticator requires that the implementing organization assess, understand, and accept the risks associated with that authenticator and acknowledge that risk will likely increase over time." The authenticator is not the only concern for the implementing organization. This should also discuss if the authenticator is or is not still bound to the CSP (issuer) that is asserting that the data on the authenticator is valid and that the authenticator itself is still in good standing. There is also risk of compromise, lost/stolen, from the bearer of the token to the overall scheme of authentication.
Appian	66	63B	5.2.11	38	1491-1493	"The authenticator SHALL contain a blocklist (either specified by specific values or by an algorithm) of at least 10 commonly used activation values and SHALL prevent their use as activation secrets." Requiring the blocklist on the authenticator is a significant burden for constrained devices (e.g., smart cards). In prior text, this is done by the issuer/client interacting with the authenticator to ensure the user can not select a blocklist activation secret. Prior text defined blocklist and it is likely not feasible to perform such blocklist functions on constrained devices.
Appian	67	63B	5.2.12	39	1531-1532	"An example of this is the pairing code used with the virtual contact interface specified in [SP800-73]." 800-73's use of pairing code is a fixed symmetric secret requiring the relying party to store and present the secret for every session. It is not a good implementation of pairing codes, as done in other protocols, that typically are randomly generated at time of presentation to establish a random session key. 800-73 does NOT use the pairing code to encrypt the channel, nor to establish an encrypted channel.
Appian	68	63B	6	41	1558-1559	"These events include binding, loss, theft, unauthorized duplication, expiration, and revocation." This is missing "maintenance" and "compromise" to update the authenticator (e.g., certificates, identity info) post-issuance.
Appian	69	63B	6.1	41	1566	"by issuance by the CSP as part of enrollment or" Enrollment is not the key issue. Issuance is binding the authenticator to the subscriber account at the CSP. It may or may not happen at time of enrollment. In FIPS 201 land, enrollment/issuance are often separated events, but the subscriber account (the PIV account) is used to maintain chain-of-trust throughout.
Appian	70	63B	6.1	41	1580	"...enrollment." You are not binding the authenticator to the enrollment. You could be "enrolling" the authenticator to the subscriber account, but that is confusing. So far, this text calls that binding the authenticator to the subscriber account.
Appian	71	63B	6.1	41	1580-1581	"If available, the record SHOULD also contain information about the source of unsuccessful authentications attempted with the authenticator." This is the relying party at time of authentication, not CSP binding to authenticator.
Appian	72	63B	6.1	41	1589-1590	"The same conditions apply when a key pair is generated by the authenticator and the public key is sent to the CSP." This is also when credential attestation is important.
Appian	73	63B	6.1.1	42	1597	"...as part of the enrollment process." This is part of binding to subscriber account, not at time of enrollment.
Appian	74	63B	6.1.1	42	1602-1604	"Preservation of online material or an online reputation makes it undesirable to lose control of a subscriber account due to the loss of an authenticator. The second authenticator makes it possible to securely recover from an authenticator loss." Here the use of authenticator is not appropriate. Actually it is about loss of PII/SPII/reputational information from the CSP to an adversary. Calling it an authenticator does not line up with AALx. It is also trying to say the subscriber is losing "control", or better stated access to, of the subscriber account at the CSP for loss of the AALx authenticator.
Appian	75	63B	6.1	41-46	1561-1754	This whole section is struggling to enable Fido. It doesn't have to. In a Fido setting, whoever receives the BYOD fido token is acting both as the CSP performing IALx enrollment and subsequent binding an authenticator to a subscriber account, as well as being the relying party and potentially a federation IdP with partners. It is critical that there is a true process for the CSP that encompasses: - Enrollment at an IALx - Establishing the subscriber account based on the verification of the enrollment - Binding one or more AALx authenticators to the subscriber account This enables a CSP to use Fido tokens as well as be the RP. We just have to be aware and recognize that they are fulfilling both roles. And if desired, as a CSP, they can be a federation IdP as well.

Appian	76	63B		6.1.2.3	43	1652-1653	"The situation where a subscriber loses control of authenticators necessary to successfully authenticate is commonly referred to as account recovery." Account recovery impacts two parties equally: CSP and RP. This is written from the RP context only.
Appian	77	63B		6.1.2.3	44	1669	"Subscriber accounts that have not been identity proofed (i.e., without IAL)…" Without IAL is actually why we need to define IAL0 and state it has not identity proofing requirements nor explict authenticator binding requirements to the subscriber account.
Appian	78	63B		6.1.4	46	1750-1751	"The process for this SHOULD conform closely to the binding process…" Binding is binding. 6.1.2 covers this reasonably well with a lot of flexibility. This ought to be a SHALL. If not, what rules exactly are being relaxed to enable this process? That impacts a RPs decision on trusting a token from a CSP.
Appian	79	63B		6.1.4	46	1754	"...the CSP MAY invalidate the authenticator…" This should be stronger. I get that an expired credential should not be honored and theoretically the time window is small here, but the CSP really should invalidate an authenticator once it has been replaced. Especially in BYOD where the CSP can not recover the authenticator from the subscriber to ensure it can't be used anymore.
Appian	80	63B		6.2	46	1755	"Loss, Theft, Damage, and Unauthorized Duplication" The title of this section should include Compromise and that would include unauthorized duplication.
Appian	81	63B		6.2	46	1756-1757	"Compromised authenticators include those that have been lost, stolen, or subject to unauthorized duplication." Compromise must also include compromise of the keying material (exfiltration), activation factors, so that an adversary can use the authenticator outside of the control of the subscriber.
Appian	82	63B		6.2	46	1761-1762	"One notable exception is a memorized secret that has been forgotten without other indications of having been compromised, such as having been obtained by an attacker." This is not an exception. It is one of the rules. If a PIN, Password, Passcode, or other activation factor is compromised, so is the authenticator itself.
Appian	83	63B		6.2	46	1763	"Suspension, revocation, or destruction of compromised authenticators SHOULD occur…" This is not a maybe. This is a shall.
Appian	84	63B		6.2	46	1766	"...reporting of the loss, theft, or damage to…" Needs compromise as part of the reporting process.
Appian	85	63B		6.3	47	1784	"The CSP SHALL require subscribers to surrender or prove destruction of any physical authenticator containing attribute certificates signed by the CSP…" Attribute certificates have specific meaning in a PKI sense for the CSP. So far, attribute certificates are not defined.
Appian	86	63B		6.4	47	1790-1792	"...when requested by the subscriber, or when the CSP determines that the subscriber no longer meets its eligibility requirements." This is missing when compromised.
Appian	87	63B		6.4	47	1793-1795	"The CSP SHALL require subscribers to surrender or certify destruction of any physical authenticator containing subscriber attributes, such as certificates signed by the CSP, as soon as practical after invalidation takes place."
Appian	88	63B		7.1	48	1822	"...subscriber's software or possession…" The use of a session secret shall be authenticated using cryptographic means. The grammar here seems incorrect.
Appian	89	63B		7.1	48	1832-1833	"A session SHOULD inherit the AAL properties of the authentication event which triggered its creation." This highlights a core issue. AALx is NOT independent of the IALx bound to that AALx authenticator, and it is a critical element of the authorization decision to be made. For a given authentication event, interiting properties of IALx and AALx are a SHALL to support an authorization decision for access.
Appian	90	63B		7.1	49	1840	"...contain at least 64 bits of entropy." Should be 112 bits of entropy.
Appian	91	63B		7.1	49	1856	"URLs or POST content…" RESTful uses both POST and PUT.
Appian	92	63B		7.1.1	49	1870	"...and SHOULD NOT contain cleartext PII." Protecting PII is everyone's responsibility. This is a SHALL.

Appian	93	63B		7.1.2	50	1879-1880	"The OAuth access token, and any associated refresh tokens, MAY be valid long after the authentication session has ended and the subscriber has left the application." This implies that OAuth tokens can be reused for multiple sessions as they will persist after the subscriber has left the application. This is a risk to the RP who depends on the AALx authenticator to establish a session.
Appian	94	63B		Table 2	7.2	50	If we truly are trying to walk away from use of passwords, providing guidance at AAL2 to use a memorized secret is counterintuitive.
Appian	95	63B		9.3	59	2012-2013	"CSPs may have various business purposes for processing attributes, including providing non-identity services to subscribers." Various business purposes includes selling ads based on identity attributes of the subscribers.
Appian	96	63B		10.1	62	2109	"...approved at the appropriate AAL…" Should include identity assuarance in this decision.
Appian	97	63B		A.4	82	2705-2706	"...verified centrally by the CSP’s verifier..." The CSP is not always the verifier.
Appian	98	63C		2	3	338-339	"In a federation scenario, the CSP provides a service known as an identity provider, or IdP." CSPs are not always the IdP. They are often separate entities.
Appian	99	63C		2	4	368	"The RP often maintains an RP subscriber account for the subscriber…" This is a confusing overload of the term subscriber. At the RP, need a different term than subscriber, as that is a CSP/IdP term.
Appian	100	63C		4.4	10	548	"...indication that no AAL claim is being made…" Another indicator why we need AAL0 in 800-63B where no claim is being made.
Appian	101	63C		4.4	10	559-560	"...considered to have “no IAL” and the RP cannot assume the account meets “IAL1”, the lowest numbered IAL described in this suite." Another indicator why we need IAL0 in 800-63A where no claim is being made.
Appian	102	63C		5.4	24	930	"RP Subscriber Accounts"
Appian	103	63C		6.1.2	36	1318…	"Bound Authenticators" This entire section avoids stating the AALx required as a minimum for bound authenticators. The diagrams assume Fido USB with touch activation. If properly certified, that token should be AAL3.
Appian	104	63C		6.1.2.1	37	1353-1354	"The RP would then prompt the subscriber to present the certificate from their smart card in order to reach FAL3." Presenting the certificate is insufficient. Must do challenge-response along with the identifying certificate.
Appian	105	63C		6.2	42	1433…	"Assertion Protection" This section references shared symmetric keys between IdP and RP. Any use of shared symmetric keys SHALL be protected and processed in a FIPS 140 Lx container.
Appian	106	63C		6.2.3	43	1471-1472	"For example, a SAML assertion can be encrypted using XML-Encryption, or an OpenID Connect ID Token can be encrypted using JSON Web Encryption (JWE)." This one is dependent on which federation model is used, either front channel or back channel. The examples are appropriate for front channel. For back channel, there is another way to do this: PKI based mutually authenticated TLS encrypted tunnel between IdP and RP.
Appian	108	63C		6.3	45	1536…	"Identity APIs" This whole section on sharing subscriber identity information en masse between IdP and RP is worrisome to me. Harkens back to Facebook scraping shadow accounts without the subscriber's consent.
Appian	107	63C		7.1	48	1611-1612	"The RP presents the assertion reference to the IdP, usually along with authentication of the RP itself, to fetch the assertion." The requirements below on 1623 make authentication of the RP a SHALL, not "usually".
Appian	109	63C		7.3	52	1692	"...request derived attribute values rather than full attribute values…" Derived attribute values is not a defined term. An example is found later at 1802-1803.
Appian	110	63C		8.1	53	1698	"...including the CSP which now acts as an IdP…" The IdP is not always the CSP.