| at | Svrt | Section/Line/Unique ref. | Reviewer’s comment/observation | Reviewer’s proposed revision/action | Editor’s proposed resolution |
| --- | --- | --- | --- | --- | --- |
| RAF23 | F | 5.3.1.4.12 | **Current citation is listed as:**  AL4\_ID\_SCV#010: Secondary checks  Have in place additional measures (e.g., require additional documentary evidence, delay completion while out-of-band checks are undertaken) to deal with any anomalous circumstances that can reasonably be anticipated (e.g., a legitimate and recent change of address that has yet to be established as the address of record).  Suggest a more appropriate reference is:  AL4\_ID\_ROC#010 Authenticate Original Credential  Prior to issuing any derived credential the original credential on which the identity-proofing relies must be:   1. authenticated by a source trusted by the CSP as being valid and un-revoked; 2. issued atAssurance Level 4; 3. issued in the same name as that which the Applicant is claiming; 4. proven to be in the possession and under the control of the Applicant**, who shall be physically present**. |  | ACCEPTED WITH MODIFICATION *PRO TEMPORE*: Exactly right – that is why this criterion was added!! Applied at all AL.  HOWEVER – the whole notion of derived credentials is a mess in -63. Cf. §5.3.5, and explain that!! |
| RAF 04 | F | * + - * 1. *For levels 2 and above ...* The CSP shall have the capability to provide records of identity proofing to RPs if required, to the extent permitted by applicable legislation and/or agreed by the Subscriber[[1]](#footnote-1). [*KI-IAF: AL2\_CO\_ESM#050 (oblique reference to understanding legislation), AL2\_ID\_VRC#025*] | The cited references do not address providing identity proofing data to RPs. | Suggest this reference be changed to AL2\_CM\_CRN#035: Convey credentialBe capable of conveying the unique identity information associated with a credential to Verifiers and Relying Parties. | ACCEPTED WITH MODIFICATION: Whereas:   1. ‘VRC#025’ refers to ‘qualifying parties’, which is a nice catch-all; 2. The title of VRC#025 refers to ‘identity records’, and; 3. CRN#035 is specifically about the credential, not information associated with p[roofing (which precedes the issuance of the credential):   Reword VRC#025 as follows (at all AL) – mark-up shown: ALn\_ID\_VRC#025 Provide Subject identity records  **As permitted by applicable legislation and/or agreed-to by the Subscriber, provide to qualifying parties unique identity and other necessary identity-pertinent information, relating to the Subject’s identity proofing and their associated tokens and credentials.** |
| RAF22 |  | 5.3.1.4.9 | What is the requirement? |  | ACCEPTED WITH MODIFICATION:Per 5.3.1.1.9, context for which is “*At all levels ...*”. Therefore, to be consistent with other usage, this should refer to AL3, which already refers to AL2, which replicates the text from AL1 but which has now been edited to simply refer to AL1. DISCUSS: Is it better to optimize the repetition or to commit to it? |
| RAF26 | S | 5.3.1.6.2.c.ii | Author suggest this only applies at level 3 when it fact also applies for level4. | Delete author comment | ACCEPTED WITH MODIFICATION: Note the subtle wording difference bt AL3 (which MAY be physical, but need not ne) and AL4 (which MUST be physical). |
| RAF15-a | F | 5.3.1.3.5 *All ...* The CSP shall:  b) be capable of conveying this information to Verifiers;  [*KI-IAF: AL3\_CO\_VRC#025, AL2\_CM\_CRN#035*] | See previous comments at LoA2 |  | ACCEPTED WITH MODIFICATION: See RAF02 |
| RAF06 | F | 5.3.1.2.5.b be capable of conveying this information to Verifiers;[*KI-IAF: AL2\_ID\_VRC#025, AL2\_CM\_CRN#035*] | Most appropriate reference is AL2\_CM\_CRN#35 | Remove non-applicable reference | ACCEPTED WITH MODIFICATION: See RAF02. |
| RAF 02 | F | 5.3.1.1.5 b) be capable of conveying this information to Verifiers;[*KI-IAF: AL1\_ID\_VRC#025,* ] | Suggest a more appropriate citation is:  AL2\_CM\_CRN#035 Convey credential  **Be capable of conveying the unique identity information associated with a credential to Verifiers and Relying Parties.** | Change citation | ACCEPTED WITH MODIFICATION: The text quoted is AL1, the suggested replacement is AL2 ... AL1 has no CRN#035 ... but why not, since the applicable -63 text says ‘All’. Therefore, suggest adding CRN#035 to AL1, retaining both it and VRC#025, as cited for all other levels, i.e.: [*KI-IAF: ALn\_ID\_VRC#025, ALn\_CM\_CRN#035*] |
| RAF10 | F | 5.3.1.2.11 *At Level 2 and higher ...* For an *ab initio* application, the Applicant supplies his or her full legal name, an address of record, and date of birth, and may, subject to the policy of the RA or CSP, also supply other PII. Specifically: iv. Any secret sent over an unprotected session shall be reset upon first use.[*KI-IAF: AL2\_CM\_CRD#016*] | **The referenced criteria actually reads:** AL2\_CM\_CRD#016 Confirm Applicant’s identity (remotely)  **Prior to delivering the credential, require the Applicant to identify themselves in any new electronic transaction (beyond the first transaction or encounter) by presenting a temporary secret which was established during a prior transaction or encounter, or sent to the Applicant’s phone number, email address, or physical address of record.**  **It does not require reset** | Either remove or correct reference. Correct reference should be: [*KI-IAF: AL2\_ID\_RPV#020 e)*] | ACCEPTED: |
| RAF40 | S | 8.3.2.2.6 | Referenced criteria does not mention FISMA. Unless the reader is familiar with FISMA they will have no idea if they are compliant. FISMA is also extremely complicated and difficult to go thru | Not sure what to do since FISMA is noted directly in the NIST 80-63-2 guidance. Perhaps just leave it alone and let the reader figure it out | ACCEPTED: (The ‘leave it alone’ part ;-) Note that ‘US profiling’ is cited, i.e. this goes further than generic criteria for KI and requires profiling for US Federal application (as used liberally elsewhere). Those who need to be US FISMA-compliant will have no option but to work it out – others may ignore. |
| RAF17 |  | 5.3.1.3.11 | Agree with Richard that address & DOB need to be included at level 3. | Add address and DoB as noted | ACCEPTED: Also applied at AL4. In addition, report anomaly to Bill Burr (NIST) |
| RAF13 |  | 5.3.1.2.13 *At Level 2 and higher ...* Sensitive data collected during the registration and identity proofing stage shall be protected during transmission and storage so as to ensure their security and confidentiality. [KI-*IAF: AL2\_?? +US / EZP800-63-2 Profiling*)] *NOT IN SAC??* | There do appear to be SAC criteria that could cover this. | The following SAC criteria might apply:  AL2\_CO\_ESM#050 Data Retention and Protection Specifically set out and demonstrate that it understands and complies with those legal and regulatory requirements incumbent upon it concerning the retention and destruction of personally identifiable information (PII) (personal and business - i.e. its secure storage and protection against loss, accidental public exposure, and/or improper destruction) and the protection of Subjects’ PII) against unlawful or unauthorized access, excepting that permitted by the information owner or required by due process. AL2\_CO\_SCO#010 Secure remote communications  **If the specific service components are located remotely from and communicate over a public or unsecured network with other service components or other CSPs which it services, the communications must be cryptographically authenticated, including long-term and session tokens, by an authentication method that meets, at a minimum, the requirements of AL2 and encrypted using a [**[**FIPS140-2**](#FIPS1402)**] Level 1-compliant encryption method or equivalent, as established by a recognized national technical authority.** | ACCEPTED: Furthermore, no need for profiling required. |
| RAF15-b | F | 5.3.1.3.5 *All ...* The CSP shall:  c) **ensure that the name associated with the Subscriber is provided by the Applicant and accepted without verification.**[*Zygma: this makes no sense at AL2 and above – does 63-2 need to be modified (or did I mis-read the reqt)??*] | See previous comments at LoA2 |  | ACCEPTED: See RAF07 |
| rAF21 |  | 5.3.1.4.5.c | See RAF 07 | Make appropriate changes to mapping | ACCEPTED: See RAF07 |
| RAF19 |  | 5.3.1.3.12-13 | Document suggest there are no requirements in the SAC: 5.3.1.3.13 *At Level 2 and higher ...* Sensitive data collected during the registration and identity proofing stage shall be protected during transmission and storage so as to ensure their security and confidentiality. [*KI-IAF: AL3\_?? +US / EZP800-63-2 Profiling*)] ***NOT IN SAC??***  5.3.1.3.14 *At Level 2 and higher ...* Additionally, the results of the identity proofing step (which may include background investigations of the Applicant) have to be protected to ensure source authentication, confidentiality, and integrity. 3[*KI-IAF: AL3\_ ?? +US / EZP800-63-2 Profiling*)] ***NOT IN SAC??***  Suggest review of my comment 13 but at level 3: AL3\_CO\_ESM#050 Data Retention and Protection and AL3\_CO\_SCO#010 Secure remote communications | Revise draft to reflect cited criteria | ACCEPTED: See RAF13 |
| RAF24 | F | 5.3.1.3.13-14 | See RAF 19 | Revise as suggested | ACCEPTED: See RAF13 |
| RAF30 | F | 6.3.1.1.1.b | Cited reference AL1\_CM\_CRN#040 cannot be found in the SAC | Correct | ACCEPTED: See RAF29 |
| RAF31 | S | 6.3.1.1.2.a | More appropriate reference would be: AL1\_CM\_CRN#030 Credential uniqueness  Allow the Subject to select a credential (e.g., UserID) that is verified to be unique within the specified service’s community and assigned uniquely to a single identity Subject.  [US / EZP800-63-2: §5.3.1.1.5 a)]  Ensure that the single-factor token associated with the credential has the one of the following set of characteristics:   * + 1. For a memorized secret, apply a rule-set such that there shall be a minimum of 14 bits of entropy in the pin or pass-phrase;  [US / EZP800-63-2: §6.3.1.1.1 a), b)]     2. For a knowledge-based question, apply a rule-set such that there shall be:        1. a minimum of 14 bits of entropy in the pin or pass-phrase OR;        2. a set of knowledge-based questions created by the user OR;        3. a set of knowledge-based questions selected by the user from a service-generated list of at least five questions.   Note – null or empty answers in either case above shall not be permitted. [US / EZP800-63-2: §6.3.1.1.2 a), c), d), e)]   Only allow password tokens that have a resistance to online guessing attack against a selected user/password of at least 1 in 214 (16,384), accounting for state-of-the-art attack strategies, and at least 10 bits of min-entropy3. |  | ACCEPTED: See RAF29 |
| RAF29 | F | 6.3.1.1.1.a | Cannot find cited reference, AL1\_CM\_CRN#040 and 50in the SAC | Correct reference, | ACCEPTED: Title for ’CRN#040 omitted (appeared as ’#030). Ref to ‘’#050 removed. |
| RAF 18 | F | 5.3.1.3.12 | Current citation is AL4\_ID\_SCV#010. More appropriate citation would be AL3\_ID\_ROC#010: Prior to issuing any derived credential the original credential on which the identity-proofing relies must be:   1. authenticated by a source trusted by the CSP as being valid and un-revoked; 2. issued at **Assurance Level 4**; 3. issued in the same name as that which the Applicant is claiming;  proven to be in the possession and under the control of the Applicant | Change citation | ACCEPTED: Victim of cut’n’haste. |
| RAF07 | F | c) ensure that the name associated with the Subscriber is provided by the Applicant and accepted without verification.[*Zygma: this makes no sense at AL2 and above – does 63-2 need to be modified (or did I mis-read the reqt)??*] | Suggest you did mis-read the requirement since it applies ONLY to LoA1. NIST 800-62-2 wording specifically states ‘At Level 1, the name associated with the Subscriber is provided by the Applicant and accepted without verification. | Since this requirement only applies at LoA1, revise to reflect same. | ACCEPTED: Was debated during IAWG telecom of 2013-06-27 and this was the consensus reached. Doc has been amended to apply this at AL1 only. |
| RAF 03 | F | **5.3.1.1.9:** *At all levels ...* Personally identifiable information (PII) collected as part of the registration process shall be protected, and all privacy requirements shall be satisfied.[*KI-IAF: AL1\_CO\_ESM#050, ’ ESM#055*] | The referenced criteria ESM#50 does not apply at LoA1. Note: AL1\_CO\_ESM#050 No stipulation  AL1\_CO\_ESM#055 Termination provisions. Define the practices in place for the protection of Subjects' private and secret information related to their use of the service which must ensure the ongoing secure preservation and protection of legally required records and for the secure destruction and disposal of any such information whose retention is no longer legally required. Specific details of these practices must be made available.  The ESM#50 requirements starts at LoA2. There are other requirements in the AL1\_CO-NUI series that are also applicable | Revise to reflect accurate references. | ALREADY APPLIED: In the reference doc for this mapping, “Kantara IAF-1400 SAC-63-2 v0-2”, ESM#050 has been introduced at AL1 in order to achieve alignment to -63.  Methinks, Rich, you’ve been looking at SAC v3-0 ??  Please identify other NUI criteria which apply. |
| RAF27 | F | 5.3.1.6.3 | Author suggests tokens if issued in multiples do not have to be unique. Disagree since the next sentence specifies that “This is permissible as long as the tokens individually meet the appropriate assurance level.” and to meet this requirement they must be unique | Delete author comment | DISCUSS – Editor disagrees with reviewer! ;-) The commented text implies that, so long as the quantity is agreed early enough, the tokens NEED NOT be distinguishable. |
| RAF38 |  | 7.3.1.3.b.iii | The referenced citation does not meet the requirements. The following part of the requirement is not covered: “but long-term shared secrets shall not be shared with any third parties, including third party Verifiers” | Include correct reference | DISCUSS: ’SCO#020 could apply – see a); yet c) contradicts, and always will, even if another matching criterion is found. |
| RAF25 | S | 5.3.1.5.1-2 | 5.1.5.2 specifies that :b above is only permitted for email. RGW suggest changing wording to specify use of phone which contradicts 5.3.1.5.2. | Suggest leaving wording as in the original NIST phrasing. | DISCUSS: I question the logic – no change proposed because I have yet to comprehend it. |
| RAF32 | F | 6.3.1.1.2.c | Do not understand how the reference AL1\_CM\_CTR#020 applies. Second reference cannot be found in the SAC | Correct references | DISCUSS: the meaning of NIST’s text is not very clear (to the Editor) |
| RAF28 |  | 5.3.5.4 | Concur with author assessment |  | NO CHANGE REQUIRED:Feedback appreciated. |
| RAF35 | F | 7.3.1.1.a.i, ii | Referenced citation cannot be found in the SAC |  | NO CHANGE REQUIRED:Referenced citation appears in reference version of SAC – perhaps search included a space after tag? |
| RAF16 |  | 5.3.1.3.9 and 5.3.1.3.10 | Kantara allows both at LoA2 and has “No stipulation” for current relationship at LoA3. See SAC section 5.1.14.5 | Suggests that Kantara also allow current relationship proofing at LoA 3 based on a valid level 2 credential to support trust elevation which is a significant topic of discussion in various forums at present. | REJECTED, WITH DISCUSSION:Don’t understand ref to SAC.5.3.1.3.9 appears to have no relevance.The proposed inclusion of ‘current relationship’ at AL3 is outside the scope of this mapping UNLESS the reviewer wishes to explain how -63 also permits it (the Editor argues that, by its omission, it is not permitted, but admittedly with this doc, almost anything goes). The fact that (at present) KI allows other proofing methods is OK so long as an Applicant doesn’t want to use them and claim compliance with -63.In the event that we did pursue the path suggested, would / should we require that the AL2 crednl be issued by a KI-Approved CSP?? Wouldn’t that be consistent with the need to have KI‑Approved service elements to maintain the credibility of KI’s assurance? Editor suggests this should be a separate proposal for SAC revision. |
| RAF 01 | F | 5.3.1.1.5.a: bullet reading: be able to uniquely identify each Subscriber and the associated tokens and the credentials issued to that Subscriber; [*KI-IAF: AL1\_ID\_POL#010, ’POL#020, AL1\_CM\_CRN#030*] | The requirement in the SAC actually reads: AL1\_ID\_POL#010 Unique service identity Ensure that a unique identity is attributed to the specific service, such that credentials issued by it can be distinguishable from those issued by other services, including services operated by the same entity. | ID\_POL#10 does not appear to be a valid reference here since it specifically addresses the identity of the service and not the subscriber. Other references are valid. Delete reference to POL#10. | REJECTED: ‘POL#010 is a necessary component in ensuring that the subscriber can, in the greater scheme, be uniquely identified. NIST doesn’t explicitly take a service-related perspective which Kantara does. POL#010 and POL#020 guarantee uniqeness |
| RAF37 | S | 7.3.1.2.f | Reference identifiers are concatenated making it difficult to understand the actual reference | Correct references | REJECTED: apostrophes indicate omission (of ‘AL2-CO-’), which is used frequently through-out doc. Need an extra space? |
| RAF34 | F | 6.3.1.1.2.e | See above | Correct references | REJECTED: e) does not refer to CTR#020 |
| RAF08 | S | *5.3.1.2.6 At Level 2 ...* The identifier associated with the Subscriber may be pseudonymous but the RA or CSP shall retain the actual identity of the Subscriber.[*KI-IAF: AL2\_CM\_CRN#090*] | The cited reference actually states: AL2\_CM\_CRN#090 Nature of Subject  Record the nature of the Subject of the credential (which must correspond to the manner of identity proofing performed), i.e., physical person, a named person acting on behalf of a corporation or other legal entity, corporation or legal entity, or corporate machine entity, in a manner that can be unequivocally associated with the credential and the identity that it asserts. If the credential is based upon a pseudonym this must be indicated in the credential. | Revise to reflect actual criteria requirement. Suggest the following criteria more accurately support the NIST requirement: AL2\_ID\_VRC#010 Verification Records for Personal Applicants Log, taking account of all applicable legislative and policy obligations, a record of the facts of the verification process, including a reference relating to the verification processes and the date and time of verification. AL2\_ID\_VRC#020 Verification Records for Affiliated Applicants  **In addition to the foregoing, log, taking account of all applicable legislative and policy obligations, a record of the additional facts of the verification process must be performed. At a minimum, records of identity information must include:**   1. **the Subject’s[[2]](#footnote-2) full name;** 2. **the Subject’s current address of record;** 3. **the Subject’s current telephone or email address of record;** 4. **the Subscriber’s acknowledgement for issuing the Subject with a credential;** 5. **type, issuing authority, and reference number(s) of all documents checked in the identity proofing process.** | REJECTED: Neither VRC#010 nor ’#020 explicitly capture the need to retain the real id, nor to permit (or require) that the credential reflects a pseudonymCreate new criterion (#095) for AL2 only, taking last sentence from #090, and make subtle modification to AL3\_CM\_CRN#090. **AL2\_CM\_CRN#095**  **If the credential is based upon a pseudonym this must be indicated in the credential and a record of the real identity retained.**  Incidentally, the VRC#020 text “must be performed” is superfluous. |
| RAF41 | S | 8.3.2.3.3 | Not certain what L3\_CO\_SCO#015 & 16 add | Delete these references | REJECTED: SCO#010 refers only to the communication layer, whereas ’015 and ’016 refer to the binding between the intrinsic message components (that’s how I read the requirements).SAC corrected at AL3 to state AL3, not AL2 (which is where the criteria were stolen from).. |
| RAF12 | F | **5.3.1.2.1 5.3.1.2.12 requires:** *All ...* If a valid credential has already been issued at Level 2 or higher, the CSP may issue another credential at Level 1 or 2. In this case, proof of possession and control of the original token may be substituted for repeating the identity proofing steps. (This is a special case of a derived credential. See Section 5.3.5 for procedures when the derived credential is issued by a different CSP.) Any requirements for credential delivery defined at §5.3.1.2.11 b) or d) (as applicable) shall still be satisfied.[*KI-IAF: AL2\_ID\_SCV#010 +US / EZP800-63-2 Profiling*)] | **The cited reference states:** AL2\_ID\_SCV#010 Secondary checks  Have in place additional measures (e.g., require additional documentary evidence, delay completion while out-of-band checks are undertaken) to deal with any anomalous circumstances that can be reasonably anticipated (e.g., a legitimate and recent change of address that has yet to be established as the address of record). This does not appear to be relevant to the requirement. | This requirement does not appear to be included in the SAC. | REJECTED: See argument to RAF11 as to why this is mapped. It allows a CSP seeking to meet -63 to use this criterion to map these ‘additional measures’. This specific -63 requirement seems to have no general value which we should adopt into the SAC (in this Editor’s opinion) – note -63’s comment re ‘special case’, hence the ‘profiling’ reference. |
| RAF15 |  | 5.3.1.3.5 *All ...* The CSP shall:  a) be able to uniquely identify each Subscriber and the associated tokens and the credentials issued to that Subscriber; [*KI-IAF: AL3\_ID\_POL#010, ’POL#020, AL3\_CM\_CRN#020, ’CRN#030*] | See previous comments at LoA2 |  | REJECTED: See RAF01 |
| RAF 05 | S | **5.3.1.2.5** *All ...* The CSP shall: a) be able to uniquely identify each Subscriber and the associated tokens and the credentials issued to that Subscriber; [*KI-IAF: AL2\_ID\_POL#010, ’POL#020, AL2\_CM\_CRN#020, ’CRN#030*] | Reference *AL2\_ID\_POL#010,* This reference relates to the Service and not the Subscriber. | Suggest this reference be removed | REJECTED: See RAF01. |
| RAF09 | F | 5.3.1.2.9 *At all levels ...* Personally identifiable information (PII) collected as part of the registration process shall be protected, and all privacy requirements shall be satisfied.[*KI-IAF: AL2\_CO\_ESM#050, ’ESM#055*] | Does not apply at LoA1 | Change reference to reflect “at LoA 2 and higher” vice “All levels” | REJECTED: See RAF03. Note that since the reference document is -63, against which the SAC is being compared, the proposed change to ‑63 cannot be accomplished. |
| RAF39 | S | 7.3.1.3.f | The last three references are incomplete in their format and do not include the full identification, e.g., SER#10 is actually AL3\_CM\_SER#010. Without full nomenclature, users will find it difficult to comply or map. | Suggest including full nomenclature | REJECTED: See RAF37 |
| RAF11 | F | **5.3.1.2.11.d.v:** For utility account numbers, confirmation shall be performed by verifying knowledge of recent account activity. (This technique may also be applied to some financial accounts.);[*KI-IAF: AL2\_ID\_SCV#010 +US / EZP800-63-2 Profiling*] | Cited reference “AL2\_ID\_SCV#010 Secondary checks  Have in place additional measures (e.g., require additional documentary evidence, delay completion while out-of-band checks are undertaken) to deal with any anomalous circumstances that can be reasonably anticipated (e.g., a legitimate and recent change of address that has yet to be established as the address of record).” Since this does not mention confirmation of activity, does not seem to apply here. | Suggest removal of AL2\_ID\_SCV#010 | REJECTED: The reason posited for removal is the very reason why it is mapped: SCV#010 is a ‘catch-all’ – in this mapping it allows a CSP seeking compliance with -63 and conformity to KI’s SAC to map through this criterion. It is there to capture anything which has to be done which doesn’t match the more explicit KI requirements. |
| RAF20 |  | 5.3.1.4.1-4 | Cannot comment since 800-63 wording is not included. | Include appropriate citations form 800-63 | REJECTED: There are none, other than repetition of AL3, which in turn refers to AL2, and the contextual framing from -63 is “*For levels 2 and above ...*”. -63 text therefore not replicated, but mapping elevated to AL4. |
| RAF36 | F | 7.3.1.2. b.i | Cited reference does not include stated requirements regarding Verifiers | Change citation | REJECTED: Verifiers are not direct agents of the CSP? If not, an alternative form of words is required for the SAC criterion, since nothing else matches. |
| RAF33 | F | 6.3.1.1.2.d | See above | Correct references | See RAF33 |
| RAF14 | F | *5.3.1.2.14 At Level 2 and higher ...* Additionally, the results of the identity proofing step (which may include background investigations of the Applicant) have to be protected to ensure source authentication, confidentiality, and integrity. [*KI-*IAF: AL2\_?? +*US / EZP800-63-2 Profiling*)] *NOT IN SAC??* | Suggest the following SAC criteria could be construed to provide coverage | AL2\_CO\_ESM#050 Data Retention and Protection Specifically set out and demonstrate that it understands and complies with those legal and regulatory requirements incumbent upon it concerning the retention and destruction of personally identifiable information (PII) (personal and business - i.e. its secure storage and protection against loss, accidental public exposure, and/or improper destruction) and the protection of Subjects’ PII) against unlawful or unauthorized access, excepting that permitted by the information owner or required by due process. | UNHAPPILY ACCEPTED: It is indeed a stretch to make it apply to this -63 clause, as is the case above.  DISCUSS: Introduction of a generic criterion, in the OP-SAC, which effects the implementation of measures alluded-to by AL2\_CO\_ESM#050? |

1. It is beyond the scope of this document to specify what circumstances make it is necessary and/or appropriate for the CSP to provide this information. Refer to applicable privacy laws, rules of evidence etc. [↑](#footnote-ref-1)
2. At this stage, the Subject is the entity acting in the role of Applicant, in anticipation of being issued a credential in which they shall be identified as the ‘Subject’ of that credential. [↑](#footnote-ref-2)