

| NIST SP 800-63A (rev.3) SAC & SoCA v4.0 | | | | Applies to: | | | | THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service | | | IAL | | CRITERION APPLICABILITY (SoCA) |
|---|------|----------------------|---|-------------|----|----|-------------------|---|-------|---|-----|---|--------------------------------|
| § | (..) | Clause title | Requirement | CS P | RP | FA | US Fed Agcy | 63A tag | index | KI_criterion (text in red is new this version) | 2 | 3 | read this comment |
| 4,2 | 1 | General Requirements | Identity proofing SHALL NOT be performed to determine suitability or entitlement to gain access to services or benefits. | ✓ | | | | 63A#0010 | | The CSP SHALL NOT perform identity proofing to determine suitability or entitlement to gain access to services or benefits. | ✓ | ✓ | In scope - Applicable |
| 4,2 | 2 | General Requirements | Collection of PII SHALL be limited to the minimum necessary to validate the existence of the claimed identity and associate the claimed identity with the applicant providing identity evidence for appropriate identity resolution, validation, and verification. This MAY include attributes that correlate identity evidence to authoritative sources and to provide RPs with attributes used to make authorization decisions. | ✓ | | | | 63A#0020 | | The CSP SHALL limit collection of PII to the minimum necessary to validate and resolve the existence of the claimed identity uniquely in a given context, and to associate the claimed identity with the Applicant providing identity evidence for appropriate identity resolution, validation, and verification. | ✓ | ✓ | In scope - Applicable |
| 4,2 | 3 | General Requirements | The CSP SHALL provide explicit notice to the applicant at the time of collection regarding the purpose for collecting and maintaining a record of the attributes necessary for identity proofing, including whether such attributes are voluntary or mandatory to complete the identity proofing process, and the consequences for not providing the attributes. | ✓ | | | | 63A#0030 | | The CSP SHALL document and publish a Privacy Notice which describes its purposes in collecting and maintaining a record of the attributes necessary for identity proofing, including whether such attributes are voluntary or mandatory to complete the identity proofing process, and the consequences for not providing the attributes. | ✓ | ✓ | In scope - Not Applicable. |

| NIST SP 800-63A (rev.3) SAC & SoCA v4.0 | | | | Applies to: | | | | THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service | | | IAL | | CRITERION APPLICABILITY (SoCA) |
|---|------|----------------------|---|-------------|----|----|-------------------|---|-------|---|-----|---|--------------------------------|
| § | (..) | Clause title | Requirement | CS P | RP | FA | US Fed Agcy | 63A tag | index | KI_criterion (text in red is new this version) | 2 | 3 | read this comment |
| 4,2 | 3+ | General Requirements | | ✓ | | | | 63A#0040 | | The CSP SHALL explicitly make its Privacy Notice available to the Applicant at the time of collection of the attributes necessary for the Applicant's identity proofing, | ✓ | ✓ | In scope - Not Applicable. |
| 4,2 | 4 | General Requirements | If CSPs process attributes for purposes other than identity proofing, authentication, or attribute assertions (collectively "identity service"), related fraud mitigation, or to comply with law or legal process, ... | ✓ | | | | 63A#0050 | | If the CSP processes attributes which it collects and stores for purposes other than identity proofing, authentication, or attribute assertions, related fraud mitigation, or to comply with law or legal process), it SHALL: | ✓ | ✓ | In scope - Applicable |
| 4,2 | 4 | General Requirements | ... CSPs SHALL implement measures to maintain predictability and manageability commensurate with the privacy risk arising from the additional processing. | ✓ | | | | 63A#0050 | a) | document and apply predictability and manageability measures associated with those additional processes based on the results of its privacy risk assessment; (see 63A#0160) | ✓ | ✓ | In scope - Applicable |
| 4,2 | 4 | General Requirements | When CSPs use consent measures,CSPs SHALL NOT make consent with these additional purposes a condition of the service. | ✓ | | | | 63A#0050 | b) | NOT make consent to processing of these additional attributes a condition of provision of the service. | ✓ | ✓ | In scope - Applicable |
| 4,2 | 5 | General Requirements | The CSP SHALL provide mechanisms for redress of applicant complaints or problems arising from the identity proofing. These mechanisms SHALL be easy for applicants to find and use. | ✓ | | | | 63A#0060 | | The CSP SHALL provide mechanisms to redress Applicant complaints or problems arising from their use of the identity proofing service. | ✓ | ✓ | In scope - Applicable |
| | | | | ✓ | | | | 63A#0062 | | The CSP SHALL document and publish its redress mechanisms in a manner which is easy for Applicants to find and use. | ✓ | ✓ | In scope - Applicable |

| NIST SP 800-63A (rev.3) SAC & SoCA v4.0 | | | | Applies to: | | | | THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service | | | IAL | | CRITERION APPLICABILITY (SoCA) |
|---|------|----------------------|---|-------------|----|----|-------------------|---|-------|---|-----|---|--------------------------------|
| § | (..) | Clause title | Requirement | CS P | RP | FA | US Fed Agcy | 63A tag | index | KI_criterion (text in red is new this version) | 2 | 3 | read this comment |
| 4,2 | 5 | General Requirements | The CSP SHALL assess the mechanisms for their efficacy in achieving resolution of complaints or problems. | ✓ | | | | 63A#0070 | | The CSP SHALL <i>review</i> its redress mechanisms <i>at least every 12 months and assess</i> their efficacy in achieving resolution of complaints or problems , <i>implementing</i> corrective action when efficacy falls below defined thresholds of performance or accomplishment. | ✓ | ✓ | In scope - Applicable |
| 4,2 | 6 | General Requirements | The identity proofing and enrollment processes SHALL be performed according to an applicable written policy ... | ✓ | | | | 63A#0080 | | The CSP SHALL: | ✓ | ✓ | In scope - Applicable |
| 4,2 | 6 | General Requirements | | ✓ | | | | 63A#0080 | a) | document in a Credential Policy (CrP) its identity proofing and enrollment policy/ies; | ✓ | ✓ | In scope - Applicable |
| 4,2 | 6 | General Requirements | <i>Kantara note - see SP 800-63-3 definition of 'Authoritative Source'.</i> | ✓ | | | | 63A#0080 | b) | for each type of identity proofing offered (see 63A#0260), state which issuing and authoritative sources are used to prove identities; | ✓ | ✓ | In scope - Applicable |
| 4,2 | 6 | General Requirements | | ✓ | | | | 63A#0080 | c) | <i>state any eligibility requirements or limitations which it applies to the scope of Applicants to its identity proofing service, subject to such limitations not breaching the restriction placed by 63A#0010;</i> | ✓ | ✓ | In scope - Not Applicable |
| 4,2 | 6 | General Requirements | | ✓ | | | | 63A#0080 | d) | publish its CrP such that it is available to members of the intended community (e.g. Applicants, Subscribers, Relying Parties, ...) before they are required to commit to signing-up to being a subject of the policy. | ✓ | ✓ | In scope - Not Applicable |
| 4,2 | 6 | General Requirements | ... or *practice statement* that specifies the particular steps taken to verify identities. | ✓ | | | | 63A#0090 | | The CSP SHALL document in its Credentialing Practices Statement (CrPS) the practices which it implements to fulfil its CrP intentions. | ✓ | ✓ | In scope - Applicable |

| NIST SP 800-63A (rev.3) SAC & SoCA v4.0 | | | | Applies to: | | | | THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service | | | IAL | | CRITERION APPLICABILITY (SoCA) |
|---|------|----------------------|---|-------------|----|----|-------------|---|-------|---|-----|---|--------------------------------|
| § | (..) | Clause title | Requirement | CS P | RP | FA | US Fed Agcy | 63A tag | index | KI_criterion (text in red is new this version) | 2 | 3 | read this comment |
| 4,2 | 6 | General Requirements | The *practice statement* SHALL include control information detailing how the CSP handles proofing errors that result in an applicant not being successfully enrolled. For example, the number of retries allowed, proofing alternatives (e.g., in-person if remote fails), or fraud counter-measures when anomalies are detected. | ✓ | | | | 63A#0100 | | The CSP's CrPS SHALL reflect the structure of its CrP and SHALL include control information detailing how the CSP handles proofing errors or other circumstances that result in an Applicant not being successfully enrolled. | ✓ | ✓ | In scope - Applicable |
| 4,2 | 7+ | General Requirements | The CSP SHALL conduct a risk management process, including assessments of privacy and security risks to determine: | ✓ | | | | 63A#0110 | | The CSP SHALL document both its risk management process (at least in the context of its identity proofing policy and practices) and the outcomes of applying that process. | ✓ | ✓ | In scope - Applicable |
| | | | | ✓ | | | | 63A#0120 | | The CSP SHALL conduct its risk management process at least once every six months and whenever there is a material change to its CrP, and SHALL include assessment of privacy and security risks, accounting for: | ✓ | ✓ | In scope - Applicable |
| 4,2 | 7 | General Requirements | Any steps that it will take to verify the identity of the applicant beyond any mandatory requirements specified herein; | ✓ | | | | 63A#0120 | a) | Any steps that it will take to verify the identity of the Applicant beyond any mandatory requirements specified herein; | ✓ | ✓ | In scope - Applicable |
| 4,2 | 7 | General Requirements | The PII, including any biometrics, images, scans, or other copies of the identity evidence that the CSP will maintain as a record of identity proofing (Note: Specific federal requirements may apply.); and | ✓ | | | | 63A#0120 | b) | The PII which the CSP shall collect and store (per its CrP), including any biometrics, images, scans, or other copies of the identity evidence that the CSP will maintain as a record of identity proofing; and | ✓ | ✓ | In scope - Applicable |
| 4,2 | 7 | General Requirements | The schedule of retention for these records (Note: CSPs may be subject to specific retention policies in accordance with applicable laws, regulations, or policies, including any National Archives and Records Administration (NARA) records retention schedules that may apply). | ✓ | | | | 63A#0120 | c) | The CSP's Retention Schedule requirements for collected PII and associated records, accounting for applicable laws, regulations, contracts, and policies. | ✓ | ✓ | In scope - Applicable |
| 4,2 | 7 | General Requirements | The CSP SHALL maintain a record, including audit logs, of ... | ✓ | | | | 63A#0130 | | The CSP SHALL maintain a record, including audit logs, of: | ✓ | ✓ | In scope - Applicable |
| 4,2 | 7 | General Requirements | | ✓ | | | | 63A#0130 | a) | the type of identity proofing performed; | ✓ | ✓ | In scope - Applicable |

| NIST SP 800-63A (rev.3) SAC & SoCA v4.0 | | | | Applies to: | | | | THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service | | | IAL | | CRITERION APPLICABILITY (SoCA) |
|---|------|----------------------|--|-------------|----|----|-------------------|---|-------|---|-----|---|--------------------------------|
| § | (..) | Clause title | Requirement | CS P | RP | FA | US Fed Agcy | 63A tag | index | KI_criterion (text in red is new this version) | 2 | 3 | read this comment |
| 4,2 | 7 | General Requirements | ... all steps taken to verify the identity of the applicant and ... [see e]] | ✓ | | | | 63A#0130 | b) | the types of and a unique reference to identity evidence collected from the Applicant in the proofing process; | ✓ | ✓ | In scope - Applicable |
| 4,2 | 7 | General Requirements | | ✓ | | | | 63A#0130 | c) | PII or other responses collected from authoritative and/or issuing sources; | ✓ | ✓ | In scope - Applicable |
| 4,2 | 7 | General Requirements | ... SHALL record the types of identity evidence presented in the proofing process. [see b]] | ✓ | | | | 63A#0130 | d) | all steps taken to validate the identity evidence; | ✓ | ✓ | In scope - Applicable |
| 4,2 | 7 | General Requirements | | ✓ | | | | 63A#0130 | e) | all steps taken to verify the identity of the Applicant; | ✓ | ✓ | In scope - Applicable |
| 4,2 | 7 | General Requirements | | ✓ | | | | 63A#0130 | f) | the outcome of each step, culminating in the final proofing result. | ✓ | ✓ | In scope - Applicable |
| 4,2 | 8 | General Requirements | All PII collected as part of the enrollment process SHALL be protected to ensure confidentiality, integrity, and attribution of the information source. | ✓ | | | | 63A#0140 | | The CSP SHALL protect all PII collected as part of the enrollment process, including validation and verification sources used, to ensure its confidentiality, integrity, and attribution of the information source. | ✓ | ✓ | In scope - Applicable |
| 4,2 | 9 | General Requirements | The entire proofing transaction, including transactions that involve a third party, SHALL occur over an authenticated protected channel. | ✓ | | | | 63A#0150 | | The CSP shall use authenticated protected channels during the entire proofing transaction, including exchanges with third parties. | ✓ | ✓ | In scope - Applicable |
| 4,2 | 10 | General Requirements | In the event the CSP uses fraud mitigation measures, the CSP SHALL conduct a privacy risk assessment for these mitigation measures. Such assessments SHALL include any privacy risk mitigations (e.g., risk acceptance or transfer, limited retention, use limitations, notice) or other technological mitigations (e.g., cryptography), and be documented per requirement 4.2(7) above. | ✓ | | | | 63A#0160 | | IF the CSP uses fraud mitigation measures, it SHALL include these measures in its privacy risk assessment for these mitigation measures. | ✓ | ✓ | In scope - Applicable |

| NIST SP 800-63A (rev.3) SAC & SoCA v4.0 | | | | Applies to: | | | | THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service | | | IAL | | CRITERION APPLICABILITY (SoCA) |
|---|--------|------------------------------------|--|-------------|----|----|-------------------|---|-------|--|-----|---|--|
| § | (..) | Clause title | Requirement | CS P | RP | FA | US Fed Agcy | 63A tag | index | KI_criterion (text in red is new this version) | 2 | 3 | read this comment |
| 4,2 | 11 | General Requirements | In the event a CSP ceases to conduct identity proofing and enrollment processes, the CSP SHALL be responsible for fully disposing of or destroying any sensitive data including PII, or its protection from unauthorized access for the duration of retention. | ✓ | | | | 63A#0170 | | The CSP SHALL define the practices in place for fully disposing of or destroying any sensitive data including PII, or its protection from unauthorized access for the duration of retention. Specific details of these practices must be made available. | ✓ | ✓ | In scope - Applicable |
| 4.4.1.2 | (IAL2) | Evidence Collection Requirements | The CSP SHALL collect the following from the applicant: | ✓ | | | | 63A#0180 | | The CSP SHALL collect from the Applicant at least the following strength of evidence, as determined by the further requirements in Table 5-1: | ✓ | | In scope - Applicable |
| 4.4.1.2 | (IAL2) | 1 Evidence Collection Requirements | One piece of SUPERIOR or STRONG evidence if the evidence's issuing source, during its identity proofing event, confirmed the claimed identity by collecting two or more forms of SUPERIOR or STRONG evidence and the CSP validates the evidence directly with the issuing source; OR | ✓ | | | | 63A#0180 | a) | One piece of STRONG evidence IF the evidence's issuing source, during its identity proofing event, confirmed the claimed identity by collecting two or more forms of SUPERIOR or STRONG evidence AND the CSP validates the evidence directly with the issuing source; OR | ✓ | | In scope - Not Applicable Option b) selected |
| 4.4.1.2 | (IAL2) | 2 Evidence Collection Requirements | Two pieces of STRONG evidence; OR | ✓ | | | | 63A#0180 | b) | Two pieces of STRONG evidence; OR | ✓ | | In scope - Applicable |
| 4.4.1.2 | (IAL2) | 3 Evidence Collection Requirements | One piece of STRONG evidence plus two pieces of FAIR evidence. | ✓ | | | | 63A#0180 | c) | One piece of STRONG evidence plus two pieces of FAIR evidence. | ✓ | | In scope - Not Applicable Option b) selected |
| 4.4.1.2 | (IAL2) | Evidence Collection Requirements | | ✓ | | | | 63A#0190 | | The CSP SHALL document its justification, for each form of evidence it recognises and collects in fulfilling its CrP and these criteria, of how the strength of the evidence it collects satisfies the qualities identified in Table 5-1 [see worksheet 63A_T5-1]. | ✓ | | In scope - Applicable |

| NIST SP 800-63A (rev.3) SAC & SoCA v4.0 | | | | Applies to: | | | | THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service | | | IAL | | CRITERION APPLICABILITY (SoCA) |
|---|--------|-----------------------------|--|-------------|----|----|-------------|---|-------|---|-----|---|--------------------------------|
| § | (..) | Clause title | Requirement | CSP | RP | FA | US Fed Agcy | 63A tag | index | KI_criterion (text in red is new this version) | 2 | 3 | read this comment |
| 4.4.1.3 | (IAL2) | Validation Requirements | The CSP SHALL validate identity evidence with a process that can achieve the same strength as the evidence presented. For example, if two forms of STRONG identity evidence are presented, each piece of evidence will be validated at a strength of | ✓ | | | | 63A#0200 | | The CSP SHALL, at a minimum, validate identity evidence at the same strength as that at which the evidence was collected. | ✓ | ✓ | In scope - Applicable |
| | | | Kantara-specific requirement | ✓ | | | | 63A#0210 | | The CSP SHALL document its justification, for each form of evidence it recognises and collects in fulfilling its CrP and these criteria, of how the strength of validation of the evidence it collects satisfies the qualities identified in Table 5-2 [see worksheet 63A_T5-2]. | ✓ | ✓ | In scope - Applicable |
| 4.4.1.3 | (IAL2) | Validation Requirements | Training requirements for personnel validating evidence SHALL be based on the policies, guidelines, or requirements of the CSP or RP. | ✓ | | | | 63A#0220 | | The CSP SHALL document its policies, guidelines, and requirements for the training of personnel validating evidence | ✓ | ✓ | In scope - Not Applicable. |
| 4.4.1.4 | (IAL2) | 1 Verification Requirements | At a minimum, the applicant's binding to identity evidence must be verified by a process that is able to achieve a strength of STRONG. | ✓ | | | | 63A#0230 | | The CSP SHALL, at a minimum, verify the Applicant's binding to the identity evidence at a strength of STRONG; | ✓ | | In scope - Applicable |
| 4.4.1.4 | (IAL2) | 2 Verification Requirements | Knowledge-based verification (KBV) SHALL NOT be used for in-person (physical or supervised remote) identity verification. | ✓ | | | | 63A#0240 | | Knowledge-based verification (KBV) SHALL NOT be used for Supervised (In-person or Remote) identity verification. | ✓ | | In scope - Not Applicable. |
| 4.4.1.4 | (IAL2) | Verification Requirements | | ✓ | | | | 63A#0250 | | The CSP SHALL document its justification, for each form of evidence it recognises in fulfilling its CrP and these criteria, of how the strength of verification of the evidence it collects meets, at a minimum, the STRONG qualities identified in Table 5-3 [see worksheet 63A_T5-3]. | ✓ | | In scope - Applicable |
| 4.4.1.4 | (IAL2) | Verification Requirements | See Section 5.3 Identity Verification for more information on acceptable identity evidence. | ✓ | | | | | | Refer to Worksheet 63A T5-3 | ✓ | | In scope - Applicable |

| NIST SP 800-63A (rev.3) SAC & SoCA v4.0 | | | | Applies to: | | | | THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service | | | IAL | | CRITERION APPLICABILITY (SoCA) |
|---|--------|------------------------|--|-------------|----|----|-------------------|---|-------|--|-----|---|--------------------------------|
| § | (..) | Clause title | Requirement | CS P | RP | FA | US Fed Agcy | 63A tag | index | KI_criterion (text in red is new this version) | 2 | 3 | read this comment |
| 4.4.1.5 | (IAL2) | Presence Requirement | The CSP SHALL support in-person or remote identity proofing. The CSP SHOULD offer both in-person and remote proofing. | ✓ | | | | 63A#0260 | | The CSP SHALL offer at least one of the following types of identity proofing and SHALL clearly state in its CrP which of those types it provides, describing | ✓ | | In scope - Applicable |
| 4.4.1.5 | (IAL2) | Presence Requirement | | ✓ | | | | 63A#0260 | a) | Supervised (In-person); | ✓ | | In scope - Not Applicable. |
| 4.4.1.5 | (IAL2) | Presence Requirement | | ✓ | | | | 63A#0260 | b) | Supervised (Remote); | ✓ | | In scope - Not Applicable. |
| 4.4.1.5 | (IAL2) | Presence Requirement | | ✓ | | | | 63A#0260 | c) | Unsupervised. | ✓ | | In scope - Applicable |
| 4.4.1.6 | (IAL2) | 2 Address Confirmation | The CSP SHALL confirm address of record. The CSP SHOULD confirm address of record through validation of the address contained on any supplied, valid piece of identity evidence. The CSP MAY confirm address of record by validating information supplied by the applicant that is not contained on any supplied piece of identity evidence. | ✓ | | | | 63A#0270 | | The CSP SHALL validate and confirm the Applicant's address of record by relying only upon issuing source(s) or authoritative source(s). | ✓ | ✓ | In scope - Applicable |
| 4.4.1.6 | (IAL2) | 3 Address Confirmation | Self-asserted address data that has not been confirmed in records SHALL NOT be used for confirmation. | ✓ | | | | 63A#0280 | | The CSP SHALL NOT accept un-validated self-asserted addresses. | ✓ | ✓ | In scope - Applicable |
| 4.4.1.6 | (IAL2) | 4 Address Confirmation | If CSP performs in-person proofing (physical or supervised remote): | ✓ | | | | 63A#0290 | | If the CSP performs Supervised (In-person or Remote) proofing it SHALL document the maximum validities it allows for enrollment codes and only issue codes that meet that limitation, which SHALL NOT exceed 7 days. | ✓ | ✓ | In scope - Not Applicable. |
| 4.4.1.6 | (IAL2) | 5 Address Confirmation | If the CSP performs remote proofing (unsupervised): | ✓ | | | | 63A#0300 | | If the CSP performs Unsupervised proofing it SHALL: | ✓ | | In scope - Applicable |
| 4.4.1.6 | (IAL2) | 5 Address Confirmation | The CSP SHALL send an enrollment code to a confirmed address of record for the applicant. | ✓ | | | | 63A#0300 | a) | send an enrollment code to a confirmed address of record for the Applicant; | ✓ | | In scope - Applicable |

| NIST SP 800-63A (rev.3) SAC & SoCA v4.0 | | | | Applies to: | | | | THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service | | | IAL | | CRITERION APPLICABILITY (SoCA) |
|---|------|----------------------|---|-------------|----|----|-------------|---|---------|---|-----|---|--------------------------------|
| § | (..) | Clause title | Requirement | CS P | RP | FA | US Fed Agcy | 63A tag | index | KI_criterion (text in red is new this version) | 2 | 3 | read this comment |
| 4.4.1.6 | 5 | Address Confirmation | The applicant SHALL present a valid enrollment code to complete the identity proofing process. | ✓ | | | | 63A#0300 | b) | require the Applicant to present a valid enrollment code to complete the identity proofing process; | ✓ | | In scope - Applicable |
| 4.4.1.6 | 5 | Address Confirmation | If the enrollment code is also intended to be an authentication factor, it SHALL be reset upon first use. | ✓ | | | | 63A#0300 | c) | If the enrollment code is also intended to be an authentication factor, reset the code upon first use; | ✓ | | In scope - Applicable |
| 4.4.1.6 | 5 | Address Confirmation | Enrollment codes SHALL have the following maximum validities: | ✓ | | | | 63A#0300 | d) | document the maximum validities it allows for enrollment codes and only issue codes that meet the following limitations: | ✓ | | In scope - Applicable |
| 4.4.1.6 | 5 | Address Confirmation | 10 days when sent to a postal address of record within the contiguous United States; | ✓ | | | | 63A#0300 | d) i) | 10 days, when sent to a postal address of record within the contiguous United States; | ✓ | | In scope - Applicable |
| 4.4.1.6 | 5 | Address Confirmation | 30 days when sent to a postal address of record outside the contiguous United States; | ✓ | | | | 63A#0300 | d) ii) | 30 days, when sent to a postal address of record outside the contiguous United States; | ✓ | | In scope - Applicable |
| 4.4.1.6 | 5 | Address Confirmation | 10 minutes when sent to a telephone of record (SMS or voice); | ✓ | | | | 63A#0300 | d) iii) | 10 minutes, when sent to a telephone number of record (SMS or voice); | ✓ | | In scope - Applicable |
| 4.4.1.6 | 5 | Address Confirmation | 24 hours when sent to an email address of record | ✓ | | | | 63A#0300 | d) iv) | 24 hours, when sent to an email address of record. | ✓ | | In scope - Applicable |
| 4.4.1.6 | 5 | Address Confirmation | The CSP SHALL ensure the enrollment code and notification of proofing are sent to different addresses of record. For example, if the CSP sends an enrollment code to a phone number validated in records, a proofing notification will be sent to the postal address validated in records or obtained from validated and verified | ✓ | | | | 63A#0300 | e) | ensure that the enrollment code and notification of proofing are sent to different addresses of record. | ✓ | | In scope - Applicable |
| 4.4.1.8 | | Security Controls | The CSP SHALL employ appropriately tailored security controls, to include control enhancements, from the moderate or high baseline of security controls defined in SP 800-53 or equivalent federal (e.g., FEDRAMP) or industry standard. | ✓ | | | | 63A#0310 | | The CSP SHALL employ appropriately-tailored security controls, to include control enhancements, from the moderate or high baseline of security controls, as defined in SP 800-53 or equivalent federal (e.g., FEDRAMP) or industry standards. | ✓ | | In scope - Applicable |

| NIST SP 800-63A (rev.3) SAC & SoCA v4.0 | | | | Applies to: | | | | THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service | | | IAL | | CRITERION APPLICABILITY (SoCA) |
|---|--------|--|--|-------------|----|----|-------------|---|-------|---|-----|---|--|
| § | (..) | Clause title | Requirement | CSP | RP | FA | US Fed Agcy | 63A tag | index | KI_criterion (text in red is new this version) | 2 | 3 | read this comment |
| 4.4.1.8 | (IAL2) | Security Controls | The CSP SHALL ensure that the minimum assurance-related controls for moderate-impact systems or equivalent are satisfied. | ✓ | | | | 63A#0320 | | When fulfilling criterion 63A#0310 the CSP SHALL ensure that the minimum assurance-related controls for moderate-impact systems or equivalent | ✓ | | In scope - Applicable |
| 4.4.2 | | IAL2 Trusted Referee proofing requirements | In instances where an individual cannot meet the identity evidence requirements specified in Section 4.4.1, the agency MAY use a trusted referee to assist in identity proofing the applicant. See Section 5.3.4 for more details. | ✓ | | | | 63A#0330 | | CSPs SHALL identity-proof Trusted Referees according to the same criteria and , as a minimum, at the same IAL that are applied to normal Applicants on whose behalf they act. | ✓ | ✓ | In scope - Not Applicable. |
| 4,6 | | Enrollment Code | An enrollment code SHALL be comprised of one of the following: | ✓ | | | | 63A#0450 | | The CSP SHALL only issue enrollment codes that are, minimally, a random six character alphanumeric sequence or other value of equivalent | ✓ | ✓ | In scope - Applicable |
| 4,6 | 1 | Enrollment Code | Minimally, a random six character alphanumeric or equivalent entropy. For example, a code generated using an approved random number generator or a serial number for a physical hardware | ✓ | | | | 63A#0450 | a) | a human-readable text string; OR | ✓ | ✓ | In scope - Applicable |
| 4,6 | 2 | Enrollment Code | A machine-readable optical label, such as a QR Code, that contains data of similar or higher entropy as a random six character | ✓ | | | | 63A#0450 | b) | A machine-readable optical label. | ✓ | ✓ | In scope - Not Applicable Option a) is used |
| 5.2.1 | | Identity Evidence Quality Requirements | Table 5 1 lists strengths, ranging from unacceptable to superior, of identity evidence that is collected to establish a valid identity. Unless otherwise noted, to achieve a given strength the evidence SHALL, at a minimum, meet all the qualities listed. | | | | | n/a | | Refer to Worksheet 63A T5-1 | ✓ | ✓ | In scope - Applicable |

| NIST SP 800-63A (rev.3) SAC & SoCA v4.0 | | | | Applies to: | | | | THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service | | | IAL | | CRITERION APPLICABILITY (SoCA) |
|---|------|---|---|-------------|----|----|-------------------|---|-------|--|-----|---|--------------------------------|
| § | (..) | Clause title | Requirement | CS P | RP | FA | US Fed Agcy | 63A tag | index | KI_criterion (text in red is new this version) | 2 | 3 | read this comment |
| 5.2.2 | | Validating Identity Evidence | Table 5-2 lists strengths, ranging from unacceptable to superior, of identity validation performed by the CSP to validate the evidence presented for the current proofing session and the information contained therein. Unless otherwise noted, to achieve a given strength the evidence SHALL, at a minimum, meet all the qualities | | | | | n/a | | Refer to Worksheet 63A T5-2 | ✓ | ✓ | In scope - Applicable |
| 5.3.1 | | Identity Verification Methods | Table 5-3 details the verification methods necessary to achieve a given identity verification strength. Unless otherwise noted, to achieve a given strength the evidence SHALL, at a minimum, meet all the qualities listed. | | | | | n/a | | Refer to Worksheet 63A T5-3 | ✓ | ✓ | In scope - Applicable |
| 5.3.1 | | | The CSP SHALL adhere to the requirements in Section 5.3.2 if KBV is used to verify an identity. | ✓ | | | | 63A#0460 | | <i>If the CSP uses KBV to verify identities it SHALL observe the practices required by 63A#0470 and 63A#0480.</i> | ✓ | | In scope - Not Applicable |
| 5.3.2 | 3 | Knowledge-Based Verification Requirements | The CSP SHALL allow a resolved and validated identity to opt out of KBV and leverage another process for verification. <i>THIS SOURCE CLAUSE HAS BEEN DELIBERATELY REPOSITIONED SINCE IT DOES NOT 'FLOW' WITH THE OTHER REQUIREMENTS IN THIS SECTION</i> | ✓ | | | | 63A#0470 | | <i>If the CSP uses KBV to verify identities it SHALL allow the Applicant the choice to opt-out of the KBV process and SHALL employ other means of equivalent rigour to achieve verification (in accordance with T5-3).</i> | ✓ | | In scope - Not Applicable |

| NIST SP 800-63A (rev.3) SAC & SoCA v4.0 | | | | Applies to: | | | | THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service | | | IAL | | CRITERION APPLICABILITY (SoCA) |
|---|------|---|--|-------------|----|----|-------------------|---|--------|--|-----|---|--------------------------------|
| § | (..) | Clause title | Requirement | CS P | RP | FA | US Fed Agcy | 63A tag | index | KI_criterion (text in red is new this version) | 2 | 3 | read this comment |
| 5.3.2 | 1 | Knowledge-Based Verification Requirements | The CSP SHALL NOT use KBV to verify an applicant's identity against more than one piece of validated identity evidence. | ✓ | | | | 63A#0480 | | The CSP SHALL verify an Applicant's identity against only a single piece of validated evidence, in accordance with the following restrictions: | ✓ | | In scope - Not Applicable |
| 5.3.2 | 2 | Knowledge-Based Verification Requirements | The CSP SHALL only use information that is expected to be known only to the applicant and the authoritative source, to include any information needed to begin the KBV | ✓ | | | | 63A#0480 | a) | information used to formulate KBQ/KBA SHALL be expected to be known only to the Applicant and the authoritative source; | ✓ | | In scope - Not Applicable |
| 5.3.2 | 4 | Knowledge-Based Verification Requirements | The CSP SHALL ensure that transaction information has at least 20 bits of entropy. For example, to reach minimum entropy requirements, the CSP could ask the applicant for verification of the amount(s) and transaction numbers(s) of a micro-deposit(s) to a valid bank account, so long as the total number of digits is seven or | ✓ | | | | 63A#0480 | b) | KBQ/KBA SHALL be composed so as to ensure that the information transacted has at least 20 bits of entropy; | ✓ | | In scope - Not Applicable |
| 5.3.2 | 5 | Knowledge-Based Verification Requirements | The CSP SHALL require a minimum of four KBV questions with each requiring a correct answer to successfully complete the KBV | ✓ | | | | 63A#0480 | c) | a minimum of four KBQ SHALL be presented and each question SHALL | ✓ | | In scope - Not Applicable |
| 5.3.2 | 5 | Knowledge-Based Verification | The CSP SHOULD require free-form response KBV questions. The CSP MAY | ✓ | | | | 63A#0480 | c) i) | have a minimum of four possible answers of which only one SHALL be correct. OR | ✓ | | In scope - Not Applicable |
| 5.3.2 | 5 | Knowledge-Based Verification Requirements | ... however, if multiple choice questions are provided, the CSP SHALL require a minimum of four answer options per | ✓ | | | | 63A#0480 | c) ii) | require responses which are not based on a selection from a pre-determined list. | ✓ | | In scope - Not Applicable |
| 5.3.2 | 5 | Knowledge-Based Verification Requirements | A CSP SHALL NOT allow more than three attempts to complete the KBV. | ✓ | | | | 63A#0480 | d) | a maximum of three attempts to answer each question SHALL be permitted; | ✓ | | In scope - Not Applicable |
| 5.3.2 | 5 | Knowledge-Based Verification Requirements | The CSP SHALL time out KBV sessions after two minutes of inactivity per question. | ✓ | | | | 63A#0480 | e) | the KBV session SHALL terminate if no attempt has been made to submit a response to a question within 2 minutes; | ✓ | | In scope - Not Applicable |
| 5.3.2 | 5 | Knowledge-Based Verification Requirements | In cases of session timeout, the CSP SHALL restart the entire KBV process and consider this a failed attempt. | ✓ | | | | 63A#0480 | f) | termination of a session SHALL require a complete re-start of the KBV process; | ✓ | | In scope - Not Applicable |

| NIST SP 800-63A (rev.3) SAC & SoCA v4.0 | | | | Applies to: | | | | THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service | | | IAL | | CRITERION APPLICABILITY (SoCA) |
|---|------|---|---|-------------|----|----|-------------------|---|-------|--|-----|---|--------------------------------|
| § | (..) | Clause title | Requirement | CS P | RP | FA | US Fed Agcy | 63A tag | index | KI_criterion (text in red is new this version) | 2 | 3 | read this comment |
| 5.3.2 | 5 | Knowledge-Based Verification Requirements | The CSP SHALL NOT present a majority of diversionary KBV questions (i.e., those where "none of the above" is the correct | ✓ | | | | 63A#0480 | g) | the presence of 'diversionary' questions in the set of possible responses SHALL be minimised; | ✓ | | In scope - Not Applicable |
| 5.3.2 | 5 | Knowledge-Based Verification Requirements | The CSP SHALL NOT ask a KBV question that provides information that could assist in answering any future KBV question in a single session or a subsequent session after a failed attempt. | ✓ | | | | 63A#0480 | h) | no question SHALL provide the Applicant the opportunity to infer answers to any other KBQs in any subsequent session; | ✓ | | In scope - Not Applicable |
| 5.3.2 | 5 | Knowledge-Based Verification Requirements | CSP SHALL ensure that any KBV question does not reveal PII that the applicant has not already provided, nor personal information that, when combined with other | ✓ | | | | 63A#0480 | i) | no question SHALL offer the Applicant the opportunity to infer answers to any other KBQs; | ✓ | | In scope - Not Applicable |
| 5.3.2 | 5 | Knowledge-Based Verification Requirements | The CSP SHALL NOT use KBV questions for which the answers do not change (e.g., "What was your first car?"). | ✓ | | | | 63A#0480 | j) | KBQ/KBA SHALL be composed] dynamically and NOT use KBQ for which the answer is in any way static. | ✓ | | In scope - Not Applicable |
| 5.3.3.1 | 1 | General Requirements | The CSP SHALL have the operator view the biometric source (e.g., fingers, face) for presence of non-natural materials and perform such inspections as part of the proofing process. | ✓ | | | | 63A#0490 | | If the CSP provides Supervised (In-person) proofing it SHALL document and apply technologies and procedures which ensure that the Proofing Supervisor reviews the biometric source (e.g., fingers, face) for presence of non-natural materials and perform such inspections as part of the | ✓ | ✓ | In scope - Not Applicable |
| 5.3.3.1 | 2 | General Requirements | The CSP SHALL collect biometrics in such a way that ensures that the biometric is collected from the applicant, and not another subject. | ✓ | | | | 63A#0500 | | If the CSP provides Supervised (In-person) proofing it SHALL document and apply technologies and procedures such that the Proofing Supervisor SHALL ensure that biometric samples are taken from the Applicant themselves and not from another person. | ✓ | ✓ | In scope - Not Applicable |
| 5.3.3.1 | 2 | General Requirements | All biometric performance requirements in SP 800-63B, Section 5.2.3 apply. | ✓ | | | | 63A#0510 | | If the CSP provides Supervised (In-person) proofing it SHALL ensure that the technologies and procedures applied by the Proofing Supervisor fulfill the biometric performance requirements expressed in 63A#0620 to 63A#0680 inclusive. | ✓ | ✓ | In scope - Not Applicable |

| NIST SP 800-63A (rev.3) SAC & SoCA v4.0 | | | | Applies to: | | | | THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service | | | IAL | | CRITERION APPLICABILITY (SoCA) |
|---|------|---|---|-------------|----|----|-------------------|---|-------|--|-----|---|--------------------------------|
| § | (..) | Clause title | Requirement | CS P | RP | FA | US Fed Agcy | 63A tag | index | KI_criterion <i>(text in red is new this version)</i> | 2 | 3 | <i>read this comment</i> |
| 5.3.3.2 | 1 | Requirements for Supervised Remote In-Person Proofing | The CSP SHALL monitor the entire identity proofing session, from which the applicant SHALL NOT depart — for example, by a continuous high-resolution video transmission of the applicant. | ✓ | | | | 63A#0520 | | The CSP SHALL supervise the entirety of a Remote proofing session, from which the Applicant SHALL NOT depart. | ✓ | ✓ | In scope - Not Applicable |
| 5.3.3.2 | 2 | Requirements for Supervised Remote In-Person Proofing | The CSP SHALL have a live operator participate remotely with the applicant for the entirety of the identity proofing session. | ✓ | | | | 63A#0530 | | The CSP SHALL ensure that a live operator participates with the Applicant for the entirety of a Remote identity proofing session. | ✓ | ✓ | In scope - Not Applicable |
| 5.3.3.2 | 3 | Requirements for Supervised Remote In-Person Proofing | The CSP SHALL require all actions taken by the applicant during the identity proofing session to be clearly visible to the remote | ✓ | | | | 63A#0540 | | The CSP SHALL ensure that a live operator clearly witnesses all actions taken by the Applicant, for the entirety of a Remote identity proofing session. | ✓ | ✓ | In scope - Not Applicable |
| 5.3.3.2 | 4 | Requirements for Supervised Remote In-Person Proofing | The CSP SHALL require that all digital verification of evidence (e.g., via chip or wireless technologies) be performed by | ✓ | | | | 63A#0550 | | The CSP SHALL ensure that all digital verification of evidence is performed by scanners and sensors which are integrated into the CSP-owned/managed | ✓ | ✓ | In scope - Not Applicable |
| 5.3.3.2 | 5 | Requirements for Supervised Remote In-Person Proofing | The CSP SHALL require operators to have undergone a training program to ... | ✓ | | | | 63A#0560 | | The CSP SHALL train its live operators such that they: | ✓ | ✓ | In scope - Not Applicable |
| 5.3.3.2 | | | ... detect potential fraud and ... | ✓ | | | | 63A#0560 | a) | are competent to detect potential fraud; and | ✓ | ✓ | In scope - Not Applicable |
| 5.3.3.2 | | | ... to properly perform a virtual in-process proofing session. | ✓ | | | | 63A#0560 | b) | are capable of properly performing a virtual in-process proofing session. | ✓ | ✓ | In scope - Not Applicable |
| 5.3.3.2 | 6 | Requirements for Supervised Remote In-Person Proofing | The CSP SHALL employ physical tamper detection and resistance features appropriate for the environment in which it is located. For example, a kiosk located in a restricted area or one where it is monitored by a trusted individual requires less tamper detection than one that is located in a semi-public area such as a shopping mall | ✓ | | | | 63A#0570 | | The CSP SHALL employ physical tamper detection and resistance features at its Remote proofing terminal appropriate for the environment in which it is located. | ✓ | ✓ | In scope - Not Applicable |

| NIST SP 800-63A (rev.3) SAC & SoCA v4.0 | | | | Applies to: | | | | THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service | | | IAL | | CRITERION APPLICABILITY (SoCA) |
|---|------|---|--|-------------|----|----|-------------------|---|-------|---|-----|---|--------------------------------|
| § | (..) | Clause title | Requirement | CS P | RP | FA | US Fed Agcy | 63A tag | index | KI_criterion (text in red is new this version) | 2 | 3 | read this comment |
| 5.3.3.2 | 7 | Requirements for Supervised Remote In-Person Proofing | The CSP SHALL ensure that all communications occur over a mutually authenticated protected channel. | ✓ | | | | 63A#0580 | | The CSP SHALL ensure that all communications between the live operator and the remote proofing terminal occur over mutually authenticated | ✓ | ✓ | In scope - Not Applicable |
| 5.3.4 | 2 | Trusted Referee Requirements | The CSP SHALL establish written policy and procedures as to ... | ✓ | | | | 63A#0590 | | The CSP SHALL include in its CrP the following: | ✓ | ✓ | In scope - Not Applicable |
| 5.3.4 | 2 | Trusted Referee Requirements | ... how a trusted referee is determined and ... | ✓ | | | | 63A#0590 | a) | how a Trusted Referee is determined; | ✓ | ✓ | In scope - Not Applicable |
| 5.3.4 | 2 | Trusted Referee Requirements | ... the lifecycle by which the trusted referee retains their status as a valid referee, ... | ✓ | | | | 63A#0590 | b) | the lifecycle by which the Trusted Referee retains their status as a valid referee; | ✓ | ✓ | In scope - Not Applicable |
| 5.3.4 | 2 | Trusted Referee Requirements | ... to include any restrictions, as well as any revocation and suspension requirements. | ✓ | | | | 63A#0590 | c) | any restrictions, as well as any revocation and suspension requirements, which are applicable to Trusted Referees; | ✓ | ✓ | In scope - Not Applicable |
| 5.3.4 | | | In addition, the CSP SHALL determine the minimum evidence required to bind the relationship between the trusted referee and the applicant. | ✓ | | | | 63A#0600 | d) | the minimum evidence required to bind the relationship between the Trusted Referee and the Applicant. | ✓ | ✓ | In scope - Not Applicable |
| 5.3.4.1 | 1 | Additional Requirements for Minors | ... the legal restrictions of interacting with minors unable to meet the evidence requirements of identity proofing to ensure compliance with the Children's Online Privacy Protection Act of 1998 (COPPA) [COPPA], and other laws, as applicable. | ✓ | | | | 63A#0610 | | The CSP SHALL document and apply policies and practices which show that it identifies and complies with all applicable laws and regulations, concerning interacting with minors unable to meet the evidence requirements of identity proofing . | ✓ | ✓ | In scope - Applicable |
| End of 63A criteria | | | | | | | | End of 63A criteria | | | | | |
| | | | | | | | | Referenced 63B_SAC criteria - NOTE - the following criteria are required to be met in the context of 63A#0510 and evidence for that purpose may differ from evidence to meet these criteria under AAL2 / 63B or under 63A Table 5-3. They are therefore replicated here under 63A and have been given discrete '63A#' tags to indicate their discrete 63A applicability: | | | | | |
| 5.2.3 | | Use of Biometrics | The biometric system SHALL ... | ✓ | | | | 63A#0620 | | The CSP shall implement biometric systems which have at least the following characteristics: | ✓ | ✓ | In scope - Applicable |

| NIST SP 800-63A (rev.3) SAC & SoCA v4.0 | | | | Applies to: | | | | THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service | | | IAL | | CRITERION APPLICABILITY (SoCA) |
|---|------|-------------------|--|-------------|----|----|-------------------|---|-------|---|-----|---|---|
| § | (..) | Clause title | Requirement | CS P | RP | FA | US Fed Agcy | 63A tag | index | KI_criterion (text in red is new this version) | 2 | 3 | read this comment |
| 5.2.3 | | Use of Biometrics | ... operate with an FMR [ISO/IEC 2382-37] of 1 in 1000 or better. | ✓ | | | | 63A#0620 | a) | operate with an FMR [ISO/IEC 2382-37] of 1 in 1000 or better; | ✓ | ✓ | In scope - Applicable |
| 5.2.3 | | Use of Biometrics | This FMR SHALL be achieved under conditions of a conformant attack (i.e., zero-effort impostor attempt) as defined | ✓ | | | | 63A#0620 | b) | achieved that FMR operation under conditions of a conformant attack (i.e., zero-effort impostor attempt) in accordance with ISO/IEC 30107-1. | ✓ | ✓ | In scope - Applicable |
| 5.2.3 | | Use of Biometrics | Testing of presentation attack resistance SHALL be in accordance with Clause 12 of ISO/IEC 30107-3. | ✓ | | | | 63A#0630 | | If Presentation Attack Detection is implemented the CSP SHALL perform testing of presentation attack resistance in accordance with §12 of ISO/IEC 30107-3. | ✓ | ✓ | In scope - Applicable |
| 5.2.3 | | Use of Biometrics | The biometric system SHALL allow no more than 5 consecutive failed authentication attempts or 10 consecutive failed attempts if PAD meeting the above requirements is implemented. | ✓ | | | | 63A#0640 | | | ✓ | ✓ | In scope - Not Applicable. The client CSP or agency would control the number of times a biometric is presented to RDP at the API. |
| 5.2.3 | | | | ✓ | | | | 63A#0640 | a) | where analysis has shown at least 90% resistance to presentation attacks for each relevant attack type (i.e., species), where resistance is defined as the number of thwarted presentation attacks divided by the number of trial presentation attacks, THEN up to 10 consecutive failed authentication attempts can occur; OTHERWISE | ✓ | ✓ | In scope - Not Applicable. (see 63A#0640) |

| NIST SP 800-63A (rev.3) SAC & SoCA v4.0 | | | | Applies to: | | | | THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service | | | IAL | | CRITERION APPLICABILITY (SoCA) |
|---|------|-------------------|--|-------------|----|----|-------------------|---|-------|--|-----|---|---|
| § | (..) | Clause title | Requirement | CS P | RP | FA | US Fed Agcy | 63A tag | index | KI_criterion (text in red is new this version) | 2 | 3 | read this comment |
| 5.2.3 | | | | ✓ | | | | 63A#0640 | b) | no more than 5 consecutive failed authentication attempts can occur. | ✓ | ✓ | In scope - Not Applicable. (see 63A#0640) |
| 5.2.3 | | Use of Biometrics | Once that limit has been reached, the biometric authenticator SHALL either: | ✓ | | | | 63A#0650 | | If either limit set in 63A#0640 is reached the CSP SHALL: | ✓ | ✓ | In scope - Not Applicable. (see 63A#0640) |
| 5.2.3 | | Use of Biometrics | · Impose a delay of at least 30 seconds before the next attempt, increasing exponentially with each successive attempt <i>(e.g., 1 minute before the following failed)</i> | ✓ | | | | 63A#0650 | a) | disable the biometric user authentication, and if an alternative authentication factor is already available use that other factor; OR OTHERWISE | ✓ | ✓ | In scope - Not Applicable. (see 63A#0640) |
| 5.2.3 | | Use of Biometrics | · Disable the biometric user authentication and offer another factor (e.g., a different biometric modality or a PIN/Passcode if it is not already a required factor) if such an alternative method is already available. | ✓ | | | | 63A#0650 | b) | impose a delay of at least 30 seconds before the next attempt, increasing exponentially with each successive attempt. | ✓ | ✓ | In scope - Not Applicable. (see 63A#0640) |
| 5.2.3 | | Use of Biometrics | The verifier SHALL make a determination of sensor and endpoint performance, integrity, and authenticity. | ✓ | | | | 63A#0660 | | No stipulation - not applicable to identity proofing. | ✓ | ✓ | In scope - Not Applicable. 63A#0510 not applicable Unsupervised proofing used |
| 5.2.3 | | Use of Biometrics | If comparison is performed centrally: | ✓ | | | | 63A#0670 | | If biometric comparison is performed centrally rather than locally the CSP SHALL: | ✓ | ✓ | In scope - Applicable |
| 5.2.3 | | Use of Biometrics | · Use of the biometric as an authentication factor SHALL be limited to one or more specific devices that are | ✓ | | | | 63A#0670 | a) | limit use of the biometric as an authentication factor to one or more specific devices that are authenticated using approved cryptography; | ✓ | ✓ | In scope - Applicable |
| 5.2.3 | | Use of Biometrics | Since the biometric has not yet unlocked the main authentication key, a separate key SHALL be used for identifying the device | ✓ | | | | 63A#0670 | b) | use a separate key to identify the device; | ✓ | ✓ | In scope - Applicable |
| 5.2.3 | | Use of Biometrics | · Biometric revocation, referred to as biometric template protection in ISO/IEC 24745, SHALL be implemented. | ✓ | | | | 63A#0670 | c) | implement biometric revocation (a.k.a. biometric template protection); Note - this is for both revocation of the credential as much as for privacy protection | ✓ | ✓ | In scope - Applicable |

| NIST SP 800-63A (rev.3) SAC & SoCA v4.0 | | | | Applies to: | | | | THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service | | | IAL | | CRITERION APPLICABILITY (SoCA) |
|---|------|------------------------------------|---|-------------|----|----|-------------------|---|-------|---|-----|---|--------------------------------|
| § | (..) | Clause title | Requirement | CS P | RP | FA | US Fed Agcy | 63A tag | index | KI_criterion (text in red is new this version) | 2 | 3 | read this comment |
| 5.2.3 | | Use of Biometrics | All transmission of biometrics SHALL be over the authenticated protected channel. | ✓ | | | | 63A#0670 | d) | transmit all biometric data over an authenticated protected channel. | ✓ | ✓ | In scope - Applicable |
| 5.2.3 | | Use of Biometrics | Biometric samples and any biometric data derived from the biometric sample such as a probe produced through signal processing SHALL be zeroized immediately after any training or research data has been derived. | ✓ | | | | 63A#0680 | | The CSP SHALL zeroize the biometric sample (including any associated biometric data) immediately after any training or research data has been derived. | ✓ | ✓ | In scope - Applicable |
| End of 'referenced' 63B criteria | | | | | | | | | | | | | |
| | | Contracted policies and procedures | | | | | | CO#0320 | | Where the enterprise uses external suppliers for specific packaged components of the service or for resources that are integrated with its own operations and under its control, ensure that those parties are engaged through reliable and appropriate contractual arrangements which stipulate which critical policies, procedures, and practices subcontractors are required to fulfill. | | | In scope - Applicable |
| | | Visibility of Contracted Parties | | | | | | CO#0330 | | Where the enterprise uses external suppliers for specific packaged components of the service or for resources which are integrated with its own operations and under its control, ensure that the suppliers' compliance with contractually-stipulated policies and procedures, and thus with the IAF Service Assessment Criteria, can be independently verified, and subsequently monitored if necessary. | | | In scope - Applicable |