Identity Assurance Framework: Service Assessment Criteria

Version: draft 0.9.1

Date: 2009-12-31

Editor: Richard G. Wilsher
Zygma LLC
Joni Brennan
IEEE-ISTO

Contributors

This document is a draft and not in final release form. The full list of contributors will be added prior to the final release of this document.

Abstract

The Kantara Initiative Identity Assurance Work Group (IAWG) was formed to foster adoption of identity trust services. The primary deliverable of the IAWG is the Identity Assurance Framework (IAF), which is comprised of many different documents that detail the levels of assurance and the certification program that bring the Framework to the marketplace. The IAF is comprised of a set of documents that includes an Overview publication, the IAF Glossary, a summary Assurance Levels document, and an Assurance Assessment Scheme (AAS), which encompasses the associated assessment and certification program, as well as several subordinate documents, among them the Service Assessment Criteria (SAC), which establishes baseline criteria for general organizational conformity, identity proofing services, credential strength, and credential management services against which all CSPs will be evaluated. The present document describes the Service Assessment Criteria component of the IAF, including setting out the Assurance Levels.

Filename: Kantara IAF-1400-Service Assessment Criteria.doc

Notice

This document has been prepared by Participants of Kantara Initiative. Permission is hereby granted to use the document solely for the purpose of implementing the Specification. No rights are granted to prepare derivative works of this Specification. Entities seeking permission to reproduce portions of this document for other uses must contact Kantara Initiative to determine whether an appropriate license for such use is available.

Implementation or use of certain elements of this document may require licenses under third party intellectual property rights, including without limitation, patent rights. The Participants of and any other contributors to the Specification are not and shall not be held responsible in any manner for identifying or failing to identify any or all such third party intellectual property rights. This Specification is provided "AS IS," and no Participant in Kantara Initiative makes any warranty of any kind, expressed or implied, including any implied warranties of merchantability, non-infringement of third party intellectual property rights, and fitness for a particular purpose. Implementers of this Specification are advised to review Kantara Initiative's website (http://www.kantarainitiative.org/) for information concerning any Necessary Claims Disclosure Notices that have been received by the Kantara Initiative Board of Trustees.

59 ## Contents
60

89
90

1 INTRODUCTION

Kantara Initiative formed the Identity Assurance Work Group (IAWG) to foster adoption of consistently managed identity trust services. Utilizing initial contributions from the e-Authentication Partnership (EAP), the US E-Authentication Federation, and Liberty Alliance, the IAWG's objective is to create a Framework of baseline policy requirements (criteria) and rules against which identity trust services can be assessed and evaluated. The goal is to facilitate trusted identity federation and to promote uniformity and interoperability amongst identity service providers, with a specific focus on the level of trust, or assurance, associated with identity assertions. The primary deliverable of IAWG is the Identity Assurance Framework (IAF).

The IAF leverages the EAP Trust Framework [EAPTrustFramework] and the US E-Authentication Federation Credential Assessment Framework ([CAF]) as baselines in forming the criteria for a harmonized, best-of-breed, industry-recognized identity assurance standard. The IAF is a Framework supporting mutual acceptance, validation, and life cycle maintenance across identity federations. The IAF is composed of a set of documents that includes an Overview publication, the IAF Glossary, a summary document on Assurance Levels, and an Assurance Assessment Scheme (AAS) document, which encompasses the associated assessment and certification program, as well as several subordinant documents. The present document, subordinant to the AAS, describes the Service Assessment Criteria component of the IAF, including setting-out the Assurance Levels.

Assurance Levels (ALs) are the levels of trust associated with a credential as measured by the associated technology, processes, and policy and practice statements controlling the operational environment. The IAF defers to the guidance provided by the U.S. National Institute of Standards and Technology (NIST) Special Publication 800-63 version 1.0.1 [NIST800-63] which outlines four levels of assurance, ranging in confidence level from low to very high. Use of ALs is determined by the level of confidence or trust (i.e. assurance) necessary to mitigate risk in the transaction.

The Service Assessment Criteria part of the IAF establishes baseline criteria for general organizational conformity, identity proofing services, credential strength, and credential management services against which all CSPs will be evaluated. The IAF will initially focus on baseline identity assertions and evolve to include attribute- and entitlement-based assertions in future releases. The IAF will also establish a protocol for publishing updates, as needed, to account for technological advances and preferred practice and policy updates.

2 ASSURANCE LEVELS

The IAF has adopted four Assurance Levels (ALs), based on the four levels of assurance posited by the U.S. Federal Government and described in OMB M-04-04 [M-04-04] and NIST Special Publication 800-63 [NIST800-63]. These are further described in the IAF publication Assurance Levels.

3 SERVICE ASSESSMENT CRITERIA

3.1 Context and Scope

The Service Assessment Criteria (SAC) are prepared and maintained by the Identity Assurance Work Group (IAWG) as part of its Identity Assurance Framework. These criteria set out the requirements for credential services and their providers at all assurance levels within the Framework. These criteria focus on the specific requirements for IAWG assessment at each Assurance Level (AL) for the following:

- The general business and organizational conformity of services and their providers;
- The functional conformity of identity proofing services; and
- The functional conformity of credential management services and their providers.

These criteria (at the applicable level) must be complied with by all services that are assessed for certification under the Identity Assurance Framework (IAF).

These criteria have been approved under the IAWG's governance rules as being suitable for use by Kantara-Accredited Assessors in the performance of their assessments of trust services whose providers are seeking recognition by IAWG.

In the context of the Identity Assurance Framework, the status of this document is normative. An applicant's trust service shall comply with all applicable criteria within this SAC at their nominated AL.

This document describes the specific criteria that must be met to achieve each of the four ALs supported by the IAWG. To be certified under the IAF Accreditation and Certification Scheme and earn the requisite Kantara Initiative Mark, services must comply with all criteria at the appropriate level.

3.2 Readership

This description of Service Assessment Criteria is required reading for all Kantara-Accredited Assessors, since it sets out the requirements with which service functions must be independently verified as being in compliance in order to be granted Kantara Recognition.

The description of criteria in Sections 3.5, 3.6 and 3.7 is required reading for all organizations wishing to become Kantara-Recognized Service Providers, and also for those wishing to become Kantara-Accredited Assessors. It is also recommended reading for those involved in the governance and day-to-day administration of the Identity Assurance Framework.

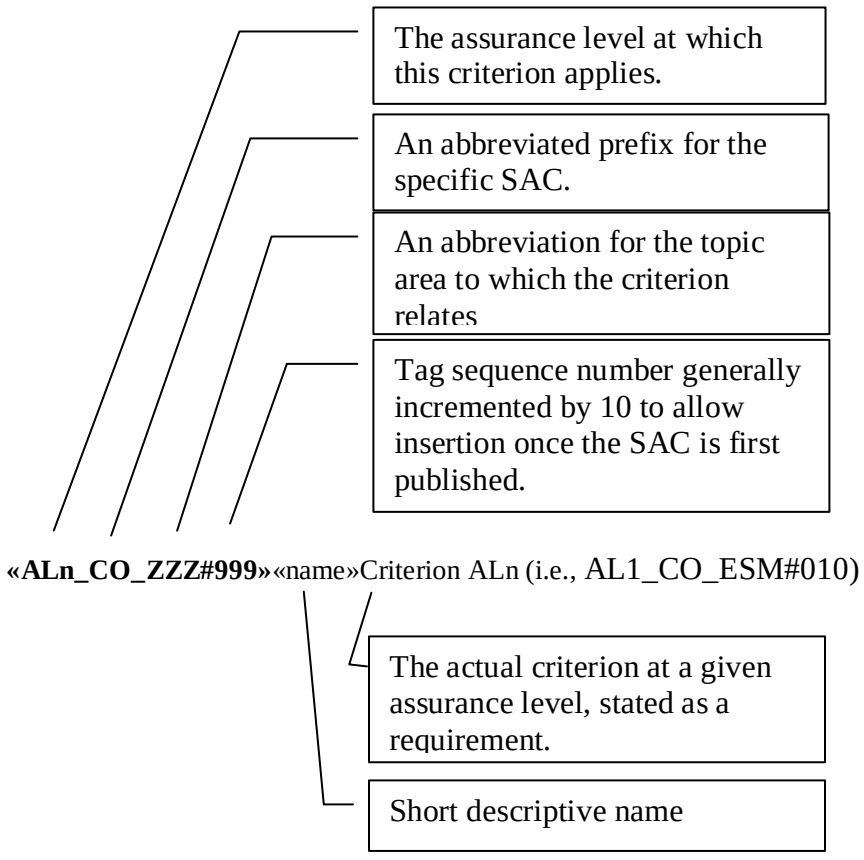
This document will also be of interest to those wishing to have a detailed understanding of the operation of the Identity Assurance Framework but who are not actively involved in its operations or in services that may fall within the scope of the Framework.

3.3 Criteria Descriptions

The Service Assessment Criteria are organized by AL. Subsections within each level describe the criteria that apply to specific functions. The subsections are parallel. Subsections describing the requirements for the same function at different levels of assurance have the same title.

Each criterion consists of three components: a unique alphanumeric tag, a short name, and the criterion (or criteria) associated with the tag. The tag provides a unique reference for each criterion that assessors and service providers can use to refer to that criterion. The name identifies the intended scope or purpose of the criterion.

The criteria are described as follows:



When a given criterion changes (i.e. becomes more rigorous) at higher Assurance Levels the new or revised text is **shown in bold** or '**[Omitted]**' is indicated where text has been

removed. With the obvious exception of AL1, when a criterion is first introduced it is also shown in bold.

As noted in the above schematic, when originally prepared, the tags had numbers incrementing in multiples of ten to permit the later insertion of additional criteria. Since then there has been addition and withdrawal of criteria.

Where a criterion is not used in a given AL but is used at a higher AL its place is held by the inclusion of a tag which is marked 'No stipulation'. A title and appropriate criteria will be added at the higher AL which occupies that position. Since in general higher ALs have a greater extent of criteria than lower ALs, where a given AL extends no further through the numbering range, criteria beyond that value are by default omitted rather than being included but marked 'No stipulation'.

Further, over time, some criteria have been removed, or withdrawn. In order to avoid the re-use of that tag such tags are retained but marked 'Withdrawn'.

Not only do these editorial practices preserve continuity they also guard against possible omission of a required criterion through an editing error.

3.4 Terminology

All special terms used in this description are defined in the IAF Glossary.

Note that when, in these criteria, the term 'Subscriber' is used it applies equally to 'Subscriber' and 'Subject' as defined in the IAF Glossary, according to the context in which used. The term 'Subject' is used when the reference is explicitly toward that party.

3.5 Common Organizational Service Assessment Criteria

The Service Assessment Criteria in this section establish the general business and organizational requirements for conformity of services and service providers at all ALs defined in Section 2 and in the Identity Assurance Framework: Levels of Assurance document. These criteria are generally referred to elsewhere within IAWG documentation as CO-SAC.

These criteria may only be used in an assessment in combination with one or more other SACs that address the technical functionality of specific service offerings.

3.5.1 Assurance Level 1

3.5.1.1 Enterprise and Service Maturity

These criteria apply to the establishment of the organization offering the service and its basic standing as a legal and operational business entity within its respective jurisdiction or country.

An enterprise and its specified service must:

AL1_CO_ESM#010 Established enterprise

Be a valid legal entity, and a person with the legal authority to commit the organization must submit the signed assessment package.

AL1_CO_ESM#020 Established service

Be fully operational in all areas described in the assessment package submitted for assessment.

Guidance: Kantara Initiative will not recognize a service which is not fully released for the provision of services to its intended user/client community. Systems, or parts thereof, which are not fully proven and released shall not be considered in an assessment and therefore should not be included within the scope of the assessment package. Parts of systems still under development, or even still being planned, are therefore ineligible for inclusion within the scope of assessment.

AL1_CO_ESM#030 Legal & Contractual compliance

Demonstrate that it understands and complies with any legal requirements incumbent on it in connection with operation and delivery of the specified service, accounting for all jurisdictions and countries within which its services may be used.

Guidance: 'Understanding' is implicitly the correct understanding. Both it and compliance are required because it could be that understanding is incomplete, incorrect or

even absent, even though compliance is apparent, and similarly, correct understanding may not necessarily result in full compliance. The two are therefore complementary.

AL1_CO_ESM#040 No stipulation

AL1_CO_ESM#050 No stipulation

AL1_CO_ESM#055 Termination provisions

Define the practices in place for the protection of subscribers' 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.

Guidance: Termination covers the cessation of the business activities, the service provider itself ceasing business operations altogether, change of ownership of the service-providing business, and other similar events which change the status and/or operations of the service provider in any way which interrupts the continued provision of the specific service.

3.5.1.2 Notices and User information

These criteria address the publication of information describing the service and the manner of and any limitations upon its provision.

An enterprise and its specified service must:

AL1_CO_NUI#010 General Service Definition

Make available to the intended user community a Service Definition that includes all applicable Terms, Conditions, and Fees, including any limitations of its usage. Specific provisions are stated in further criteria in this section.

Guidance: The intended user community encompasses potential and actual subscribers, subjects, and relying parties.

AL1_CO_NUI#020 Service Definition inclusions

Make available a Service Definition for the specified service containing clauses that provide the following information:

a) a Privacy Policy

AL1_CO_NUI#030 Due notification

Have in place and follow appropriate policy and procedures to ensure that it notifies Users in a timely and reliable fashion of any changes to the Service Definition and any applicable Terms, Conditions, and Privacy Policy for the specified service.

AL1_CO_NUI#040 User Acceptance

Require subscribers and subjects to:

a) indicate, prior to receiving service, that they have read and accept the terms of service as defined in the Service Definition;
b) at periodic intervals, determined by significant service provision events (e.g. issuance, re-issuance, renewal), re-affirm their understanding and observance of the terms of service;
c) always provide full and correct responses to requests for information.

AL1_CO_NUI#050 Record of User Acceptance

Obtain a record (hard-copy or electronic) of the subscriber's and subject's acceptance of the terms and conditions of service, prior to initiating the service and thereafter at periodic intervals, determined by significant service provision events (e.g. re-issuance, renewal).

3.5.1.3 Not used

3.5.1.4 Not used

3.5.1.5 Not used

3.5.1.6 Not used

3.5.1.7 Secure Communications

AL1_CO_SCO#010 No stipulation

AL1_CO_SCO#020 Limited access to shared secrets

Ensure that:

a) access to shared secrets shall be subject to discretionary controls which permit access to those roles/applications needing such access;
b) stored shared secrets are not held in their plaintext form unless given adequate physical or logical protection;
c) any plaintext passwords or secrets are not transmitted across any public or unsecured network.

3.5.2 Assurance Level 2

Criteria in this section address the establishment of the enterprise offering the service and its basic standing as a legal and operational business entity within its respective jurisdiction or country.

3.5.2.1 Enterprise and Service Maturity

These criteria apply to the establishment of the enterprise offering the service and its basic standing as a legal and operational business entity.

An enterprise and its specified service must:

AL2_CO_ESM#010 Established enterprise

Be a valid legal entity, and a person with legal authority to commit the organization must submit the signed assessment package.

AL2_CO_ESM#020 Established service

Be fully operational in all areas described in the assessment package submitted for assessment.

AL2_CO_ESM#030 Legal & Contractual compliance

Demonstrate that it understands and complies with any legal requirements incumbent on it in connection with operation and delivery of the specified service, accounting for all jurisdictions within which its services may be offered**. Any specific contractual requirements shall also be identified**.

Guidance: Kantara Initiative will not recognize a service which is not fully released for the provision of services to its intended user/client community. Systems, or parts thereof, which are not fully proven and released shall not be considered in an assessment and therefore should not be included within the scope of the assessment package. Parts of systems still under development, or even still being planned, are therefore ineligible for inclusion within the scope of assessment.

AL2_CO_ESM#040 Financial Provisions

Provide documentation of financial resources that allow for the continued operation of the service and demonstrate appropriate liability processes and procedures that satisfy the degree of liability exposure being carried.

Guidance: The organization must show that it has a budgetary provision to operate the service for at least a twelve-month period, with a clear review of the budgetary planning within that period so as to keep the budgetary provisions extended. It must also show

how it has determined the degree of liability protection required, in view of its exposure per 'service' and the number of users it has. This criterion helps ensure that Kantara Initiative does not grant Recognition to services that are not likely to be sustainable over at least this minimum period of time.

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 private and identifiable information (personal and business)(i.e. its secure storage and protection against loss, accidental public exposure, and/or improper destruction) and the protection of subscribers' private information (against unlawful or unauthorized access, excepting that permitted by the information owner or required by due process).

Guidance: Note that whereas the criterion is intended to address unlawful or unauthorized access arising from malicious or careless actions (or inaction) some access may be unlawful UNLESS authorized by the subscriber or effected as a part of a specifically-executed legal process.

AL2_CO_ESM#055 Termination provisions

Define the practices in place for the protection of subscribers' 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.

Guidance: Termination covers the cessation of the business activities, the service provider itself ceasing business operations altogether, change of ownership of the service-providing business, and other similar events which change the status and/or operations of the service provider in any way which interrupts the continued provision of the specific service.

3.5.2.2 Notices and User Information/Agreements

These criteria apply to the publication of information describing the service and the manner of and any limitations upon its provision, and how users are required to accept those terms.

An enterprise and its specified service must:

AL2_CO_NUI#010 General Service Definition

Make available to the intended user community a Service Definition that includes all applicable Terms, Conditions, and Fees, including any limitations of its usage, **and**

definitions of any terms having specific intention or interpretation. **Specific provisions are stated in further criteria in this section.**

Guidance: The intended user community encompasses potential and actual subscribers, subjects, and relying parties.

AL2_CO_NUI#020 Service Definition inclusions

Make available a Service Definition for the specified service containing clauses that provide the following information:

a) Privacy**, Identity Proofing & Verification, and Revocation and Termination Policies;**
b) the country in or legal jurisdiction under which the service is operated;
c) if different from the above, the legal jurisdiction under which subscriber and any relying party agreements are entered into;
d) applicable legislation with which the service complies;
e) obligations incumbent upon the CSP;
f) obligations incumbent upon the subscriber;
g) notifications and guidance for relying parties, especially in respect of actions they are expected to take should they choose to rely upon the service;
h) statement of warranties;
i) statement of liabilities toward both Subjects and Relying Parties;
j) procedures for notification of changes to terms and conditions;
k) steps the CSP will take in the event that it chooses or is obliged to terminate the service;
l) availability of the specified service *per se* and of its help desk facility.

AL2_CO_NUI#030 Due notification

Have in place and follow appropriate policy and procedures to ensure that it notifies subscribers and subjects in a timely and reliable fashion of any changes to the Service Definition and any applicable Terms, Conditions, Fees, and Privacy Policy for the specified service, **and provide a clear means by which subscribers and subjects must indicate that they wish to accept the new terms or terminate their subscription**.

AL2_CO_NUI#040 User Acceptance

Require subscribers and subjects to:

a) indicate, prior to receiving service, that they have read and accept the terms of service as defined in the Service Definition;
b) at periodic intervals, determined by significant service provision events (e.g. issuance, re-issuance, renewal) **and otherwise at least once every five years**, re-affirm their understanding and observance of the terms of service;
c) always provide full and correct responses to requests for information.

AL2_CO_NUI#050 Record of User Acceptance

Obtain a record (hard-copy or electronic) of the subscriber's and subject's acceptance of the terms and conditions of service, prior to initiating the service and thereafter at periodic intervals, determined by significant service provision events (e.g. re-issuance, renewal) **and otherwise at least once every five years**.

AL2_CO_NUI#060 Withdrawn

Withdrawn.

AL2_CO_NUI#070 Change of Subscriber Information

Require and provide the mechanisms for subscribers and subjects to provide in a timely manner full and correct amendments should any of their recorded information change, as required under the terms of their use of the service, and only after the subscriber's and/or subject's identity has been authenticated.

AL2_CO_NUI#080 Withdrawn

Withdrawn.

3.5.2.3 Information Security Management

These criteria address the way in which the enterprise manages the security of its business, the specified service, and information it holds relating to its user community. This section focuses on the key components that comprise a well-established and effective Information Security Management System (ISMS), or other IT security management methodology recognized by a government or professional body.

An enterprise and its specified service must:

AL2_CO_ISM#010 Documented policies and procedures

Have documented all security-relevant administrative, management, and technical policies and procedures. The enterprise must ensure that these are based upon recognized standards, published references or organizational guidelines, are adequate for the specified service, and are implemented in the manner intended.

AL2_CO_ISM#020 Policy Management and Responsibility

Have a clearly defined managerial role, at a senior level, in which full responsibility for the business's security policies is vested and from which review, approval, and promulgation of policy and related procedures is applied and managed. The latest approved versions of these policies must be applied at all times.

AL2_CO_ISM#030 Risk Management

Demonstrate a risk management methodology that adequately identifies and mitigates risks related to the specified service and its user community.

AL2_CO_ISM#040 Continuity of Operations Plan

Have and keep updated a Continuity of Operations Plan that covers disaster recovery and the resilience of the specified service.

AL2_CO_ISM#050 Configuration Management

Demonstrate that there is in place a configuration management system that at least includes:

a) version control for software system components;
b) timely identification and installation of all organizationally-approved patches for any software used in the provisioning of the specified service.

AL2_CO_ISM#060 Quality Management

Demonstrate that there is in place a quality management system that is appropriate for the specified service.

AL2_CO_ISM#070 System Installation and Operation Controls

Apply controls during system development, procurement installation, and operation that protect the security and integrity of the system environment, hardware, software, and communications.

AL2_CO_ISM#080 Internal Service Audit

Be audited at least once every 12 months for effective provision of the specified service by independent internal audit functions of the enterprise responsible for the specified service, unless it can show that by reason of its organizational size or due to other operational restrictions it is unreasonable to be so audited.

AL2_CO_ISM#090 Independent Audit

Be audited by an independent auditor at least every 24 months to ensure the organization's security-related practices are consistent with the policies and procedures for the specified service and the applicable SAC.

Guidance: The appointed auditor should have appropriate accreditation or other acceptable experience and qualification, comparable to that required of Kantara-Accredited Assessors. It is expected that it will be cost-effective for the organization to

use the same Kantara-Accredited Assessor for the purposes of fulfilling this criterion as they do for the maintenance of their grant of Kantara Recognition.

AL2_CO_ISM#100 Audit Records

Retain records of all audits, both internal and independent, for a period which, as a minimum, fulfills its legal obligations and otherwise for greater periods either as it may have committed to in its Service Definition or required by any other obligations it has with/to a subscriber, and which in any event is not less than 36 months. Such records must be held securely and be protected against unauthorized access, loss, alteration, public disclosure, or unapproved destruction.

AL2_CO_ISM#110 Termination provisions

This is now AL2_CO_ESM#055.

3.5.2.4 Security-relevant Event (Audit) Records

These criteria apply to the need to provide an auditable log of all events that are pertinent to the correct and secure operation of the service.

An enterprise and its specified service must:

AL2_CO_SER#010 Security event logging

Maintain a log of all relevant security events concerning the operation of the service, together with an accurate record of the time at which the event occurred (time-stamp), and retain such records with appropriate protection and controls to ensure successful retrieval, accounting for service definition, risk management requirements, applicable legislation, and organizational policy.

Guidance: It is sufficient that the accuracy of the time source is based upon an internal computer/system clock synchronized to an internet time source. The time source need not be authenticatable.

3.5.2.5 Operational infrastructure

These criteria apply to the infrastructure within which the delivery of the specified service takes place. These criteria emphasize the personnel involved and their selection, training, and duties.

An enterprise and its specified service must:

AL2_CO_OPN#010 Technical security

Demonstrate that the technical controls employed will provide the level of security protection required by the risk assessment and the ISMS, or other IT security management methods recognized by a government or professional body, and that these controls are effectively integrated with the applicable procedural and physical security measures.

Guidance: Appropriate technical controls, suited to this Assurance Level, should be selected from [NIST800-63] or its equivalent, as established by a recognized national technical authority.

AL2_CO_OPN#020 Defined security roles

Define, by means of a job description, the roles and responsibilities for each service-related security-relevant task, relating it to specific procedures, (which shall be set out in the ISMS, or other IT security management methodology recognized by a government or professional body) and other service-related job descriptions. Where the role is security-critical or where special privileges or shared duties exist, these must be specifically identified as such, including the applicable access privileges relating to logical and physical parts of the service's operations.

AL2_CO_OPN#030 Personnel recruitment

Demonstrate that it has defined practices for the selection, evaluation, and contracting of all service-related personnel, both direct employees and those whose services are provided by third parties.

AL2_CO_OPN#040 Personnel skills

Ensure that employees are sufficiently trained, qualified, experienced, and current for the roles they fulfill. Such measures must be accomplished either by recruitment practices or through a specific training program. Where employees are undergoing on-the-job training, they must only do so under the guidance of a mentor possessing the defined service experiences for the training being provided.

AL2_CO_OPN#050 Adequacy of Personnel resources

Have sufficient staff to adequately operate and resource the specified service according to its policies and procedures.

AL2_CO_OPN#060 Physical access control

Apply physical access control mechanisms to ensure that:

a) access to sensitive areas is restricted to authorized personnel;

b) all removable media and paper documents containing sensitive information as plain-text are stored in secure containers.

Require a minimum of two person physical access control when accessing any cryptographic modules.

AL2_CO_OPN#070 Logical access control

Employ logical access control mechanisms that ensure access to sensitive system functions and controls is restricted to authorized personnel.

3.5.2.6 External Services and Components

These criteria apply to the relationships and obligations upon contracted parties both to apply the policies and procedures of the enterprise and also to be available for assessment as critical parts of the overall service provision.

An enterprise and its specified service must:

AL2_CO_ESC#010 Contracted policies and procedures

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.

AL2_CO_ESC#020 Visibility of contracted parties

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 the suppliers' compliance with contractually-stipulated policies and procedures, and thus with IAF Service Assessment Criteria, can be independently verified, and subsequently monitored if necessary.

3.5.2.7 Secure Communications

An enterprise and its specified service must:

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] Level 1-compliant encryption method or equivalent, as established by a recognized national technical authority.

AL2_CO_SCO#015 Verification / Authentication confirmation messages

Ensure that any verification or confirmation of authentication messages, which asserts either that a weakly bound credential is valid or that a strongly bound credential has not been subsequently revoked, is logically bound to the credential and that the message, the logical binding, and the credential are all transmitted within a single integrity-protected session between the service and the Verifier / Relying Party.

AL2_CO_SCO#016 Verification of Revoked Credential

When a verification / authentication request results in notification of a revoked credential one of the following measures shall be taken:

a) the confirmation message shall be time-stamped, or;

b) the session keys shall expire with an expiration time no longer than that of the applicable revocation list, or;

c) the time-stamped message, binding, and credential shall all be signed by the service.

AL2_CO_SCO#020 Limited access to shared secrets

Ensure that:

a) access to shared secrets shall be subject to discretionary controls that only permit access by those roles/applications requiring such access;

b) stored shared secrets are not held in their plaintext form unless given adequate physical or logical protection;

c) any long-term (i.e., not session) shared secrets are revealed only to the subscriber or to the CSP's direct agents (bearing in mind item "a" in this list).

These roles should be defined and documented by the CSP in accordance with AL2_CO_OPN#020 above.

AL2_CO_SCO#030 Logical protection of shared secrets

Ensure that one of the alternative methods (below) is used to protect shared secrets:

610 **a) concatenation of the password to a salt and/or username which is then hashed**
611 **with an Approved algorithm such that the computations used to conduct a**
612 **dictionary or exhaustion attack on a stolen password file are not useful to**
613 **attack other similar password files, or;**

614 **b) encryption using an Approved algorithm and modes, and the shared secret**
615 **decrypted only when immediately required for authentication, or;**

616 **c) any secure method allowed to protect shared secrets at Level 3 or 4.**

617
618

3.5.3 Assurance Level 3

Achieving AL3 requires meeting more stringent criteria in addition to all criteria required to achieve AL2.

3.5.3.1 Enterprise and Service Maturity

Criteria in this section address the establishment of the enterprise offering the service and its basic standing as a legal and operational business entity.

An enterprise and its specified service must:

AL3_CO_ESM#010 Established enterprise

Be a valid legal entity and a person with legal authority to commit the organization must submit the signed assessment package.

AL3_CO_ESM#020 Established service

Be fully operational in all areas described in the assessment package submitted for assessment.

AL3_CO_ESM#030 Legal & Contractual compliance

Demonstrate that it understands and complies with any legal requirements incumbent on it in connection with operation and delivery of the specified service, accounting for all jurisdictions within which its services may be offered. Any specific contractual requirements shall also be identified.

Guidance: Kantara Initiative will not recognize a service which is not fully released for the provision of services to its intended user/client community. Systems, or parts thereof, which are not fully proven and released shall not be considered in an assessment and therefore should not be included within the scope of the assessment package. Parts of systems still under development, or even still being planned, are therefore ineligible for inclusion within the scope of assessment.

AL3_CO_ESM#040 Financial Provisions

Provide documentation of financial resources that allow for the continued operation of the service and demonstrate appropriate liability processes and procedures that satisfy the degree of liability exposure being carried.

Guidance: The organization must show that it has a budgetary provision to operate the service for at least a twelve-month period, with a clear review of the budgetary planning within that period so as to keep the budgetary provisions extended. It must also show how it has determined the degree of liability protection required, in view of its exposure

per 'service' and the number of users it has. This criterion helps ensure that Kantara Initiative does not grant Recognition to services that are not likely to be sustainable over at least this minimum period of time.

AL3_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 private and identifiable information (personal and business) (i.e. its secure storage and protection against loss, accidental public exposure and/or improper destruction) and the protection of private information (against unlawful or unauthorized access, excepting that permitted by the information owner or required by due process).

AL3_CO_ESM#055 Termination provisions

Define the practices in place for the protection of subscribers' 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.

Guidance: Termination covers the cessation of the business activities, the service provider itself ceasing business operations altogether, change of ownership of the service-providing business, and other similar events which change the status and/or operations of the service provider in any way which interrupts the continued provision of the specific service.

AL3_CO_ESM#060 Ownership

If the enterprise named as the CSP is a part of a larger entity, the nature of the relationship with its parent organization shall be disclosed to the assessors and, on their request, to customers.

AL3_CO_ESM#070 Independent management and operations

Demonstrate that, for the purposes of providing the specified service, its management and operational structures are distinct, autonomous, have discrete legal accountability, and operate according to separate policies, procedures, and controls.

3.5.3.2 Notices and User Information

Criteria in this section address the publication of information describing the service and the manner of and any limitations upon its provision, and how users are required to accept those terms.

An enterprise and its specified service must:

AL3_CO_NUI#010 General Service Definition

Make available to the intended user community a Service Definition that includes all applicable Terms, Conditions, and Fees, including any limitations of its usage, and definitions of any terms having specific intention or interpretation. Specific provisions are stated in further criteria in this section.

Guidance: The intended user community encompasses potential and actual subscribers, subjects and relying parties.

AL3_CO_NUI#020 Service Definition inclusions

Make available a Service Definition for the specified service containing clauses that provide the following information:

a) Privacy, Identity Proofing & Verification, and Revocation and Termination Policies;
b) the country in or the legal jurisdiction under which the service is operated;
c) if different to the above, the legal jurisdiction under which subscriber and any relying party agreements are entered into;
d) applicable legislation with which the service complies;
e) obligations incumbent upon the CSP;
f) obligations incumbent upon the subscriber;
g) notifications and guidance for relying parties, especially in respect of actions they are expected to take should they choose to rely upon the service's product;
h) statement of warranties;
i) statement of liabilities toward both Subjects and Relying Parties;
j) procedures for notification of changes to terms and conditions;
k) steps the CSP will take in the event that it chooses or is obliged to terminate the service;
l) availability of the specified service *per se* and of its help desk facility.

AL3_CO_NUI#030 Due notification

Have in place and follow appropriate policy and procedures to ensure that it notifies subscribers and subjects in a timely and reliable fashion of any changes to the Service Definition and any applicable Terms, Conditions, Fees, and Privacy Policy for the specified service, and provide a clear means by which subscribers and subjects must indicate that they wish to accept the new terms or terminate their subscription.

AL3_CO_NUI#040 User Acceptance

Require subscribers and subjects to:

a) indicate, prior to receiving service, that they have read and accept the terms of service as defined in the Service Definition;
b) at periodic intervals, determined by significant service provision events (e.g. issuance, re-issuance, renewal) and otherwise at least once every five years, re-affirm their understanding and observance of the terms of service;
c) always provide full and correct responses to requests for information.

AL3_CO_NUI#050 Record of User Acceptance

Obtain a record (hard-copy or electronic) of the subscriber's and subject's acceptance of the terms and conditions of service, prior to initiating the service and thereafter reaffirm the agreement at periodic intervals, determined by significant service provision events (e.g. re-issuance, renewal) and otherwise at least once every five years.

AL3_CO_NUI#060 Withdrawn

Withdrawn.

AL3_CO_NUI#070 Change of Subscriber Information

Require and provide the mechanisms for subscribers and subjects to provide in a timely manner full and correct amendments should any of their recorded information change, as required under the terms of their use of the service, and only after the subscriber's and/or subject's identity has been authenticated.

AL3_CO_NUI#080 Withdrawn

Withdrawn.

3.5.3.3 Information Security Management

These criteria address the way in which the enterprise manages the security of its business, the specified service, and information it holds relating to its user community. This section focuses on the key components that make up a well-established and effective Information Security Management System (ISMS), or other IT security management methodology recognized by a government or professional body.

An enterprise and its specified service must:

AL3_CO_ISM#010 Documented policies and procedures

Have documented all security-relevant administrative management and technical policies and procedures. The enterprise must ensure that these are based upon recognized standards, published references or organizational guidelines, are adequate for the specified service, and are implemented in the manner intended.

AL3_CO_ISM#020 Policy Management and Responsibility

Have a clearly defined managerial role, at a senior level, where full responsibility for the business' security policies is vested and from which review, approval, and promulgation of policy and related procedures is applied and managed. The latest approved versions of these policies must be applied at all times.

AL3_CO_ISM#030 Risk Management

Demonstrate a risk management methodology that adequately identifies and mitigates risks related to the specified service and its user community **and must show that a risk assessment review is performed at least once every six months, such as adherence to SAS 70 or [IS27001] method**.

AL3_CO_ISM#040 Continuity of Operations Plan

Have and keep updated a continuity of operations plan that covers disaster recovery and the resilience of the specified service **and must show that a review of this plan is performed at least once every six months**.

AL3_CO_ISM#050 Configuration Management

Demonstrate that there is in place a configuration management system that at least includes:

a) version control for software system components;
b) timely identification and installation of all organizationally-approved patches for any software used in the provisioning of the specified service**;**
c) version control and managed distribution for all documentation associated with the specification, management, and operation of the system, covering both internal and publicly available materials.

AL3_CO_ISM#060 Quality Management

Demonstrate that there is in place a quality management system that is appropriate for the specified service.

AL3_CO_ISM#070 System Installation and Operation Controls

Apply controls during system development, procurement, installation, and operation that protect the security and integrity of the system environment, hardware, software, and communications **having particular regard to:**

a) the software and hardware development environments, for customized components;
b) the procurement process for commercial off-the-shelf (COTS) components;
c) contracted consultancy/support services;
d) shipment of system components;
e) storage of system components;
f) installation environment security;
g) system configuration;
h) transfer to operational status.

AL3_CO_ISM#080 Internal Service Audit

Be audited at least once every 12 months for effective provision of the specified service by independent internal audit functions of the enterprise responsible for the specified service, unless it can show that by reason of its organizational size or due to other **justifiable** operational restrictions it is unreasonable to be so audited.

AL3_CO_ISM#090 Independent Audit

Be audited by an independent auditor at least every 24 months to ensure the organization's security-related practices are consistent with the policies and procedures for the specified service.

Guidance: The appointed auditor should have appropriate accreditation or other acceptable experience and qualification, comparable to that required of Kantara-Accredited Assessors. It is expected that it will be cost-effective for the organization to use the same Kantara-Accredited Assessor for the purposes of fulfilling this criterion as they do for the maintenance of their grant of Kantara Recognition.

AL3_CO_ISM#100 Audit Records

Retain records of all audits, both internal and independent, for a period which, as a minimum, fulfills its legal obligations and otherwise for greater periods either as it may have committed to in its Service Definition or required by any other obligations it has with/to a subscriber, and which in any event is not less than 36 months. Such records must be held securely and be protected against unauthorized access, loss, alteration, public disclosure, or unapproved destruction.

AL3_CO_ISM#110 Termination provisions

This is now AL3_CO_ESM#055.

AL3_CO_ISM#120 Best Practice Security Management

Have in place an Information Security Management System (ISMS), or other IT security management methodology recognized by a government or professional body, that follows best practices as accepted by the information security industry and that applies and is appropriate to the CSP in question. All requirements expressed in preceding criteria in this section must *inter alia* fall wholly within the scope of this ISMS or selected recognized alternative.

3.5.3.4 Security-Relevant Event (Audit) Records

The criteria in this section are concerned with the need to provide an auditable log of all events that are pertinent to the correct and secure operation of the service.

An enterprise and its specified service must:

AL3_CO_SER#010 Security Event Logging

Maintain a log of all relevant security events concerning the operation of the service, together with an accurate record of the time at which the event occurred (time-stamp), and retain such records with appropriate protection and controls to ensure successful retrieval, accounting for Service Definition risk management requirements, applicable legislation, and organizational policy.

Guidance: It is sufficient that the accuracy of the time source is based upon an internal computer/system clock synchronized to an internet time source. The time source need not be authenticatable.

3.5.3.5 Operational Infrastructure

The criteria in this section address the infrastructure within which the delivery of the specified service takes place. It puts particular emphasis upon the personnel involved, and their selection, training, and duties.

An enterprise and its specified service must:

AL3_CO_OPN#010 Technical security

Demonstrate that the technical controls employed will provide the level of security protection required by the risk assessment and the ISMS, or other IT security management methods recognized by a government or professional body, and that these

controls are effectively integrated with the applicable procedural and physical security measures.

Guidance: Appropriate technical controls, suited to this Assurance Level, should be selected from [NIST800-63] or its equivalent, as established by a recognized national technical authority.

AL3_CO_OPN#020 Defined security roles

Define, by means of a job description, the roles and responsibilities for each service-related security-relevant task, relating it to specific procedures (which shall be set out in the ISMS, or other IT security management methodology recognized by a government or professional body) and other service-related job descriptions. Where the role is security-critical or where special privileges or shared duties exist, these must be specifically identified as such, including the applicable access privileges relating to logical and physical parts of the service's operations.

AL3_CO_OPN#030 Personnel recruitment

Demonstrate that it has defined practices for the selection, vetting, and contracting of all service-related personnel, both direct employees and those whose services are provided by third parties. **Full records of all searches and supporting evidence of qualifications and past employment must be kept for the duration of the individual's employment plus the longest lifespan of any credential issued under the Service Policy.**

AL3_CO_OPN#040 Personnel skills

Ensure that employees are sufficiently trained, qualified, experienced, and current for the roles they fulfill. Such measures must be accomplished either by recruitment practices or through a specific training program. Where employees are undergoing on-the-job training, they must only do so under the guidance of a mentor possessing the defined service experiences for the training being provided.

AL3_CO_OPN#050 Adequacy of Personnel resources

Have sufficient staff to adequately operate and resource the specified service according to its policies and procedures**.**

AL3_CO_OPN#060 Physical access control

Apply physical access control mechanisms to ensure that:

a) access to sensitive areas is restricted to authorized personnel;

b) all removable media and paper documents containing sensitive information as plain-text are stored in secure containers;

c) there is 24/7 monitoring for unauthorized intrusions.

AL3_CO_OPN#070 Logical access control

Employ logical access control mechanisms that ensure access to sensitive system functions and controls is restricted to authorized personnel.

3.5.3.6 External Services and Components

This section addresses the relationships and obligations upon contracted parties both to apply the policies and procedures of the enterprise and also to be available for assessment as critical parts of the overall service provision.

An enterprise and its specified service must:

AL3_CO_ESC#010 Contracted policies and procedures

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 those parties are engaged through reliable and appropriate contractual arrangements which stipulate which critical policies, procedures, and practices sub-contractors are required to fulfill.

AL3_CO_ESC#020 Visibility of contracted parties

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 controls, 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.

3.5.3.7 Secure Communications

An enterprise and its specified service must:

AL3_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 it services, the communications must be cryptographically authenticated, including long-term and session tokens, by an authentication protocol that meets, at a minimum, the requirements of AL**3** and encrypted using **either a FIPS 140-2 [FIPS140-2] Level 2 (or higher) validated hardware cryptographic module or any FIPS 140-2 Level 3 or 4 validated**

912 **cryptographic module,** or equivalent, as established by a recognized national technical
913 authority.

914 AL3_CO_SCO#020 Limited access to shared secrets

915 Ensure that:

916 a) access to shared secrets shall be subject to discretionary controls that permit
917 access to those roles/applications requiring such access;
918 **b)** stored shared secrets are **encrypted such that:**
919 **i** **the encryption key for the shared secret file is encrypted under a key**
920 **held in either a FIPS 140-2 [FIPS140-2] Level 2 (or higher) validated**
921 **hardware cryptographic module or any FIPS 140-2 Level 3 or 4**
922 **validated cryptographic module, or equivalent, as established by a**
923 **recognized national technical authority, and decrypted only as**
924 **immediately required for an authentication operation;**
925 **ii** **they are protected as a key within the boundary of either a FIPS 140-2**
926 **Level 2 (or higher) validated hardware cryptographic module or any**
927 **FIPS 140-2 Level 3 or 4 validated cryptographic module, or**
928 **equivalent, as established by a recognized national technical**
929 **authority, and are not exported from the module in plaintext;**
930 **iii** **they are split by an "*n from m*" cryptographic secret-sharing method;**
931 c) any long-term (i.e., not session) shared secrets are revealed only to the subscriber
932 and the CSP's direct agents (bearing in mind (a) above).
933
934 **These roles should be defined and documented by the CSP in accordance with**
935 **AL3_CO_OPN#020 above**.

936
937

3.5.4 Assurance Level 4

Achieving AL4 requires meeting even more stringent criteria in addition to the criteria required to achieve AL3.

3.5.4.1 Enterprise and Service Maturity

Criteria in this section address the establishment of the enterprise offering the service and its basic standing as a legal and operational business entity.

An enterprise and its specified service must:

AL4_CO_ESM#010 Established enterprise

Be a valid legal entity and a person with legal authority to commit the organization must submit the signed assessment package.

AL4_CO_ESM#020 Established service

Be fully operational in all areas described in the assessment package submitted for assessment.

AL4_CO_ESM#030 Legal & Contractual compliance

Demonstrate that it understands and complies with any legal requirements incumbent on it in connection with operation and delivery of the specified service, accounting for all jurisdictions within which its services may be offered. Any specific contractual requirements shall also be identified.

Guidance: Kantara Initiative will not recognize a service which is not fully released for the provision of services to its intended user/client community. Systems, or parts thereof, which are not fully proven and released shall not be considered in an assessment and therefore should not be included within the scope of the assessment package. Parts of systems still under development, or even still being planned, are therefore ineligible for inclusion within the scope of assessment.

AL4_CO_ESM#040 Financial Provisions

Provide documentation of financial resources that allow for the continued operation of the service and demonstrate appropriate liability processes and procedures that satisfy the degree of liability exposure being carried.

Guidance: The organization must show that it has a budgetary provision to operate the service for at least a twelve-month period, with a clear review of the budgetary planning within that period so as to keep the budgetary provisions extended. It must also show how it has determined the degree of liability protection required, in view of its exposure

per 'service' and the number of users it has. This criterion helps ensure that Kantara Initiative does not grant Recognition to services that are not likely to be sustainable over at least this minimum period of time.

AL4_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 private and identifiable information (personal and business) (i.e. its secure storage and protection against loss, accidental public exposure, and/or improper destruction) and the protection of private information (against unlawful or unauthorized access excepting that permitted by the information owner or required by due process).

Termination provisions

Define the practices in place for the protection of subscribers' 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.

Guidance: Termination covers the cessation of the business activities, the service provider itself ceasing business operations altogether, change of ownership of the service-providing business, and other similar events which change the status and/or operations of the service provider in any way which interrupts the continued provision of the specific service.

AL4_CO_ESM#060 Ownership

If the enterprise named as the CSP is a part of a larger entity, the nature of the relationship with its parent organization, shall be disclosed to the assessors and, on their request, to customers.

AL4_CO_ESM#070 Independent Management and Operations

Demonstrate that, for the purposes of providing the specified service, its management and operational structures are distinct, autonomous, have discrete legal accountability, and operate according to separate policies, procedures, and controls.

3.5.4.2 Notices and Subscriber Information/Agreements

Criteria in this section address the publication of information describing the service and the manner of and any limitations upon its provision, and how users are required to accept those terms.

An enterprise and its specified service must:

AL4_CO_NUI#010 General Service Definition

Make available to the intended user community a Service Definition that includes all applicable Terms, Conditions, and Fees, including any limitations of its usage, and definitions of any terms having specific intention or interpretation. Specific provisions are stated in further criteria in this section.

Guidance: The intended user community encompasses potential and actual subscribers, subjects, and relying parties.

AL4_CO_NUI#020 Service Definition inclusions

Make available a Service Definition for the specified service containing clauses that provide the following information:

a) Privacy, Identity Proofing & Verification, and Revocation and Termination Policies;
b) the country in or legal jurisdiction under which the service is operated;
c) if different to the above, the legal jurisdiction under which subscriber and any relying party agreements are entered into;
d) applicable legislation with which the service complies;
e) obligations incumbent upon the CSP;
f) obligations incumbent upon the subscriber;
g) notifications and guidance for relying parties, especially in respect of actions they are expected to take should they choose to rely upon the service's product;
h) statement of warranties;
i) statement of liabilities toward both Subjects and Relying Parties;
j) procedures for notification of changes to terms and conditions;
k) steps the CSP will take in the event that it chooses or is obliged to terminate the service;
l) availability of the specified service per se and of its help desk facility.

AL4_CO_NUI#030 Due Notification

Have in place and follow appropriate policy and procedures to ensure that it notifies subscribers and subjects in a timely and reliable fashion of any changes to the Service Definition and any applicable Terms, Conditions, Fees, and Privacy Policy for the specified service, and provide a clear means by which subscribers and subjects must indicate that they wish to accept the new terms or terminate their subscription.

AL4_CO_NUI#040 User Acceptance

Require subscribers and subjects to:

a) indicate, prior to receiving service, that they have read and accept the terms of service as defined in the Service Definition, thereby indicating their properly-informed opt-in;
b) at periodic intervals, determined by significant service provision events (e.g. issuance, re-issuance, renewal) and otherwise at least once every five years, re-affirm their understanding and observance of the terms of service;
c) always provide full and correct responses to requests for information.

AL4_CO_NUI#050 Record of User Acceptance

Obtain a record (hard-copy or electronic) of the subscriber's and subject's acceptance of the terms and conditions of service, prior to initiating the service and thereafter reaffirm the agreement at periodic intervals, determined by significant service provision events (e.g. issuance, re-issuance, renewal) and otherwise at least once every five years.

AL4_CO_NUI#060 Withdrawn

Withdrawn.

AL4_CO_NUI#070 Change of Subscriber Information

Require and provide the mechanisms for subscribers and subjects to provide in a timely manner full and correct amendments should any of their recorded information change, as required under the terms of their use of the service, and only after the subscriber's and/or subject's identity has been authenticated.

AL4_CO_NUI#080 Withdrawn

Withdrawn.

3.5.4.3 Information Security Management

These criteria address the way in which the enterprise manages the security of its business, the specified service, and information it holds relating to its user community. This section focuses on the key components that comprise a well-established and effective Information Security Management System (ISMS), or other IT security management methodology recognized by a government or professional body.

An enterprise and its specified service must:

AL4_CO_ISM#010 Documented policies and procedures

Have documented all security-relevant administrative, management, and technical policies and procedures. The enterprise must ensure that these are based upon recognized

standards, published references, or organizational guidelines, are adequate for the specified service, and are implemented in the manner intended.

AL4_CO_ISM#020 Policy Management and Responsibility

Have a clearly defined managerial role, at a senior level, where full responsibility for the business' security policies is vested and from which review, approval, and promulgation of policy and related procedures is applied and managed. The latest approved versions of these policies must be applied at all times.

AL4_CO_ISM#030 Risk Management

Demonstrate a risk management methodology that adequately identifies and mitigates risks related to the specified service and its user community and must show that on-going risk assessment review is conducted as a part of the business' procedures, such as adherence to SAS 70 or [IS27001] methods.

AL4_CO_ISM#040 Continuity of Operations Plan

Have and keep updated a continuity of operations plan that covers disaster recovery and the resilience of the specified service and must show that **on-going review of this plan is conducted as a part of the business' procedures**.

AL4_CO_ISM#050 Configuration Management

Demonstrate that there is in place a configuration management system that at least includes:

a) version control for software system components;
b) timely identification and installation of all organizationally-approved patches for any software used in the provisioning of the specified service;
c) version control and managed distribution for all documentation associated with the specification, management, and operation of the system, covering both internal and publicly available materials.

AL4_CO_ISM#060 Quality Management

Demonstrate that there is in place a quality management system that is appropriate for the specified service.

AL4_CO_ISM#070 System Installation and Operation Controls

Apply controls during system development, procurement, installation, and operation that protect the security and integrity of the system environment, hardware, software, and communications having particular regard to:

a) the software and hardware development environments, for customized components;
b) the procurement process for commercial off-the-shelf (COTS) components;
c) contracted consultancy/support services;
d) shipment of system components;
e) storage of system components;
f) installation environment security;
g) system configuration;
h) transfer to operational status.

AL4_CO_ISM#080 Internal Service Audit

Be audited at least once every 12 months for effective provision of the specified service by independent internal audit functions of the enterprise responsible for the specified service, unless it can show that by reason of its organizational size or due to other justifiable operational restrictions it is unreasonable to be so audited.

AL4_CO_ISM#090 Independent Audit

Be audited by an independent auditor at least every 24 months to ensure the organization's security-related practices are consistent with the policies and procedures for the specified service.

Guidance: The appointed auditor should have appropriate accreditation or other acceptable experience and qualification, comparable to that required of Kantara-Accredited Assessors. It is expected that it will be cost-effective for the organization to use the same Kantara-Accredited Assessor for the purposes of fulfilling this criterion as they do for the maintenance of their grant of Kantara Recognition.

AL4_CO_ISM#100 Audit Records

Retain records of all audits, both internal and independent, for a period which, as a minimum, fulfills its legal obligations and otherwise for greater periods either as it may have committed to in its Service Definition or required by any other obligations it has with/to a subscriber, and which in any event is not less than 36 months. Such records must be held securely and be protected against unauthorized access loss, alteration, public disclosure, or unapproved destruction.

AL4_CO_ISM#110 Termination provisions

This is now AL4_CO_ESM#055.

AL4_CO_ISM#120 Best Practice Security Management

Have in place a certified Information Security Management System (ISMS), or other IT security management methodology recognized by a government or professional body, that **has been assessed and found to be in compliance with the requirements of ISO/IEC 27001 [IS27001] and which applies and is appropriate to the CSP in question.** All requirements expressed in preceding criteria in this section must *inter alia* fall wholly within the scope of this ISMS, or the selected recognized alternative.

3.5.4.4 Security-Related (Audit) Records

The criteria in this section are concerned with the need to provide an auditable log of all events that are pertinent to the correct and secure operation of the service.

An enterprise and its specified service must:

AL4_CO_SER#010 Security Event Logging

Maintain a log of all relevant security events concerning the operation of the service, together with **a precise** record of the time at which the event occurred (time-stamp) **provided by a trusted time-source** and retain such records with appropriate protection and controls to ensure successful retrieval, accounting for service definition, risk management requirements, applicable legislation, and organizational policy.

Guidance: The trusted time source could be an external trusted service or a network time server or other hardware timing device. The time source must be not only precise but authenticatable as well.

3.5.4.5 Operational Infrastructure

The criteria in this section address the infrastructure within which the delivery of the specified service takes place. It puts particular emphasis upon the personnel involved, and their selection, training, and duties.

An enterprise and its specified service must:

AL4_CO_OPN#010 Technical Security

Demonstrate that the technical controls employed will provide the level of security protection required by the risk assessment and the ISMS, or other IT security management methods recognized by a government or professional body, and that these controls are effectively integrated with the applicable procedural and physical security measures.

Guidance: Appropriate technical controls, suited to this Assurance Level, should be selected from [NIST800-63] or its equivalent, as established by a recognized national technical authority.

AL4_CO_OPN#020 Defined Security Roles

Define, by means of a job description, the roles and responsibilities for each service-related security-relevant task, relating it to specific procedures (which shall be set out in the ISMS, or other IT security management methodology recognized by a government or professional body) and other service-related job descriptions. Where the role is security-critical or where special privileges or shared duties exist, these must be specifically identified as such, including the applicable access privileges relating to logical and physical parts of the service's operations.

AL4_CO_OPN#030 Personnel Recruitment

Demonstrate that it has defined practices for the selection, vetting, and contracting of all service-related personnel, both direct employees and those whose services are provided by third parties. Full records of all searches and supporting evidence of qualifications and past employment must be kept for the duration of the individual's employment plus the longest lifespan of any credential issued under the Service Policy.

AL4_CO_OPN#040 Personnel skills

Ensure that employees are sufficiently trained, qualified, experienced, and current for the roles they fulfill. Such measures must be accomplished either by recruitment practices or through a specific training program. Where employees are undergoing on-the-job training, they must only do so under the guidance of a mentor possessing the defined service experiences for the training being provided.

AL4_CO_OPN#050 Adequacy of Personnel resources

Have sufficient staff to adequately operate and resource the specified service according to its policies and procedures**.**

AL4_CO_OPN#060 Physical access control

Apply physical access control mechanisms to ensure that:

a) access to sensitive areas is restricted to authorized personnel;

b) all removable media and paper documents containing sensitive information as plain-text are stored in secure containers;

c) there is 24/7 monitoring for unauthorized intrusions.

AL4_CO_OPN#070 Logical access control

Employ logical access control mechanisms that ensure access to sensitive system functions and controls is restricted to authorized personnel.

3.5.4.6 External Services and Components

This section addresses the relationships and obligations upon contracted parties both to apply the policies and procedures of the enterprise and also to be available for assessment as critical parts of the overall service provision.

An enterprise and its specified service must:

AL4_CO_ESC#010 Contracted Policies and Procedures

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 those parties are engaged through reliable and appropriate contractual arrangements which stipulate which critical policies, procedures, and practices sub-contractors are required to fulfill.

AL4_CO_ESC#020 Visibility of Contracted Parties

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.

3.5.4.7 Secure Communications

An enterprise and its specified service must:

AL4_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 it services, the communications must be cryptographically authenticated, including long-term and session tokens, by an authentication protocol that meets the requirements of AL4 and encrypted using either a FIPS 140-2 [FIPS140-2] Level 2 (or higher) validated hardware cryptographic module or any FIPS 140-2 Level 3 or 4 validated cryptographic module, or equivalent, as established by a recognized national technical authority.

AL4_CO_SCO#020 Limited access to shared secrets

Ensure that:

a) access to shared secrets shall be subject to discretionary controls which permit access to those roles/applications which need such access;

b) stored shared secrets are encrypted such that:

i the encryption key for the shared secret file is encrypted under a key held in a FIPS 140-2 [FIPS140-2] Level 2 (or higher) validated hardware cryptographic module, or equivalent, as established by a recognized national technical authority, or any FIPS 140-2 Level 3 or 4 validated cryptographic module, or equivalent, as established by a recognized national technical authority, and decrypted only as immediately required for an authentication operation;

ii they are protected as a key within the boundary of a FIPS 140-2 Level 2 (or higher) validated hardware cryptographic module, or equivalent, as established by a recognized national technical authority, or any FIPS 140-2 Level 3 or 4 cryptographic module, or equivalent, as established by a recognized national technical authority, and are not exported in plaintext from the module;

iii they are split by an "*n from m*" cryptographic secret-sharing method;

c) any long-term (i.e., not session) shared secrets are revealed only to the subscriber and the CSP's direct agents (bearing in mind (a) above).

3.5.5 Compliance Tables

Use the following tables to correlate criteria for a particular Assurance Level (AL) and the evidence offered to support compliance.

Service providers preparing for an assessment can use the table appropriate to the AL at which they are seeking approval to correlate evidence with criteria or to justify non-applicability (e.g., "specific service types not offered").

Assessors can use the tables to record the steps in their assessment and their determination of compliance or failure.

Table 3-1. CO-SAC - AL1 Compliance

Clause	Description	Compliance
AL1_CO_ESM#010	Established enterprise	
AL1_CO_ESM#020	Established service	
AL1_CO_ESM#030	Legal & Contractual compliance	
AL1_CO_ESM#040	No stipulation	
AL1_CO_ESM#040	No stipulation	
AL1_CO_ESM#055	Termination provisions	
AL1_CO_NUI#010	General Service Definition	
AL1_CO_NUI#020	Service Definition inclusions	
AL1_CO_NUI#030	Due notification	
AL1_CO_NUI#040	User Acceptance	
AL1_CO_NUI#050	Record of User Acceptance	
AL1_CO_SCO#020	Limited access to shared secrets	

1267 **Table 3-2.** CO-SAC - AL2 Compliance

Clause	Description	Compliance
AL2_CO_ESM#010	Established enterprise	
AL2_CO_ESM#020	Established service	
AL2_CO_ESM#030	Legal & Contractual compliance	
AL2_CO_ESM#040	Financial Provisions	
AL2_CO_ESM#050	Data Retention and Protection	
AL2_CO_ESM#055	Termination provisions	
AL2_CO_NUI#010	General Service Definition	
AL2_CO_NUI#020	Service Definition inclusions	
AL2_CO_NUI#030	Due notification	
AL2_CO_NUI#040	User Acceptance	
AL2_CO_NUI#050	Record of User Acceptance	
AL2_CO_NUI#060	Withdrawn	No conformity requirement
AL2_CO_NUI#070	Change of Subscriber Information	
AL2_CO_NUI#080	Withdrawn	No conformity requirement
AL2_CO_ISM#010	Documented policies and procedures	
AL2_CO_ISM#020	Policy Management and Responsibility	
AL2_CO_ISM#030	Risk Management	
AL2_CO_ISM#040	Continuity of Operations Plan	
AL2_CO_ISM#050	Configuration Management	
AL2_CO_ISM#060	Quality Management	
AL2_CO_ISM#070	System Installation and Operation Controls	
AL2_CO_ISM#080	Internal Service Audit	
AL2_CO_ISM#090	Independent Audit	
AL2_CO_ISM#100	Audit Records	
AL2_CO_ISM#110	Termination provisions	Re-assigned as AL2_CO_ESM#055
AL2_CO_SER#010	Security event logging	
AL2_CO_OPN#010	Technical security	
AL2_CO_OPN#020	Defined security roles	
AL2_CO_OPN#030	Personnel recruitment	
AL2_CO_OPN#040	Personnel skills	
AL2_CO_OPN#050	Adequacy of Personnel resources	
AL2_CO_OPN#060	Physical access control	

AL2_CO_OPN#070	Logical access control	
AL2_CO_ESC#010	Contracted policies and procedures	
AL2_CO_ESC#020	Visibility of contracted parties	
AL2_CO_SCO#010	Secure remote communications	
AL2_CO_SCO#015	Verification / Authentication confirmation messages	
AL2_CO_SCO#016	Verification of Revoked Credential	
AL2_CO_SCO#020	Limited access to shared secrets	
AL2_CO_SCO#030	Logical protection of shared secrets	

1268

1269

1270 **Table 3-3.** CO-SAC - AL3 compliance

Clause	Description	Compliance
AL3_CO_ESM#010	Established enterprise	
AL3_CO_ESM#020	Established service	
AL3_CO_ESM#030	Legal & Contractual compliance	
AL3_CO_ESM#040	Financial Provisions	
AL3_CO_ESM#050	Data Retention and Protection	
AL3_CO_ESM#055	Termination provisions	
AL3_CO_ESM#060	Ownership	
AL3_CO_ESM#070	Independent management and operations	
AL3_CO_NUI#010	General Service Definition	
AL3_CO_NUI#020	Service Definition inclusions	
AL3_CO_NUI#030	Due notification	
AL3_CO_NUI#040	User Acceptance	
AL3_CO_NUI#050	Record of User Acceptance	
AL3_CO_NUI#060	Withdrawn	No conformity requirement
AL3_CO_NUI#070	Change of Subscriber Information	
AL3_CO_NUI#080	Withdrawn	No conformity requirement
AL3_CO_ISM#010	Documented policies and procedures	
AL3_CO_ISM#020	Policy Management and Responsibility	
AL3_CO_ISM#030	Risk Management	
AL3_CO_ISM#040	Continuity of Operations Plan	
AL3_CO_ISM#050	Configuration Management	
AL3_CO_ISM#060	Quality Management	
AL3_CO_ISM# 070	System Installation and Operation Controls	
AL3_CO_ISM#080	Internal Service Audit	
AL3_CO_ISM#090	Independent Audit	
AL3_CO_ISM#100	Audit Records	
AL3_CO_ISM#110	Termination provisions	Re-assigned as AL3_CO_ESM#055
AL3_CO_ISM#120	Best Practice Security Management	
AL3_CO_SER#010	Security Event Logging	
AL3_CO_OPN#010	Technical security	
AL3_CO_OPN#020	Defined security roles	
AL3_CO_OPN#030	Personnel recruitment	

AL3_CO_OPN#040	Personnel skills	
AL3_CO_OPN#050	Adequacy of Personnel resources	
AL3_CO_OPN#060	Physical access control	
AL3_CO_OPN#070	Logical access control	
AL3_CO_ESC#010	Contracted policies and procedures	
AL3_CO_ESC#020	Visibility of contracted parties	
AL3_CO_SCO#010	Secure remote communications	
AL3_CO_SCO#020	Limited access to shared secrets	

1271

1272

1273 **Table 3-4.** CO-SAC - AL4 compliance

Clause	Description	Compliance
AL4_CO_ESM#010	Established enterprise	
AL4_CO_ESM#020	Established service	
AL4_CO_ESM#030	Legal & Contractual compliance	
AL4_CO_ESM#040	Financial Provisions	
AL4_CO_ESM#050	Data Retention and Protection	
AL4_CO_ESM#055	Termination provisions	
AL4_CO_ESM#060	Ownership	
AL4_CO_ESM#070	Independent Management and Operations	
AL4_CO_NUI#010	General Service Definition	
AL4_CO_NUI#020	Service Definition inclusions	
AL4_CO_NUI#030	Due Notification	
AL4_CO_NUI#040	User Acceptance	
AL4_CO_NUI#050	Record of User Acceptance	
AL4_CO_NUI#060	Withdrawn	No conformity requirement
AL4_CO_NUI#070	Change of Subscriber Information	
AL4_CO_NUI#080	Withdrawn	No conformity requirement
AL4_CO_ISM#010	Documented policies and procedures	
AL4_CO_ISM#020	Policy Management and Responsibility	
AL4_CO_ISM#030	Risk Management	
AL4_CO_ISM#040	Continuity of Operations Plan	
AL4_CO_ISM#050	Configuration Management	
AL4_CO_ISM#060	Quality Management	
AL4_CO_ISM#070	System Installation and Operation Controls	
AL4_CO_ISM#080	Internal Service Audit	
AL4_CO_ISM#090	Independent Audit	
AL4_CO_ISM#100	Audit Records	
AL4_CO_ISM#110	Termination provisions	Re-assigned as AL4_CO_ESM#055
AL4_CO_ISM#120	Best Practice Security Management	
AL4_CO_SER#010	Security Event Logging	
AL4_CO_OPN#010	Technical Security	
AL4_CO_OPN#020	Defined Security Roles	
AL4_CO_OPN#030	Personnel Recruitment	

AL4_CO_OPN#040	Personnel skills	
AL4_CO_OPN#050	Adequacy of Personnel resources	
AL4_CO_OPN#060	Physical access control	
AL4_CO_OPN#070	Logical access control	
AL4_CO_ESC#010	Contracted Policies and Procedures	
AL4_CO_ESC#020	Visibility of Contracted Parties	
AL4_CO_SCO#010	Secure remote communications	
AL4_CO_SCO#020	Limited access to shared secrets	

1274
1275

3.6 Identity Proofing Service Assessment Criteria

The Service Assessment Criteria in this section establish the requirements for the technical conformity of identity proofing services at all ALs defined in Section 2 and in the Identity Assurance Framework: Levels of Assurance document. These criteria apply to a particular kind of electronic trust service (ETS) recognized by the IAWG and to the related credential service provider (CSP)—an identity proofing service for both individual identity and institutional identity credentials[1]. (For definitions of terms used in this section, see the Identity Assurance Framework: Glossary document). These criteria are generally referred to elsewhere within IAWG documentation as ID-SAC [ID-SAC].

These criteria do not address the delivery of a credential to the applicant/subscriber, which is dealt with by the Credential Management SAC (CM-SAC), described in Section 3.7.

These criteria may only be used in an assessment in one of the following circumstances:

- In conjunction with the Common Organizational SAC (CO-SAC), described in Section 3.5, for a standalone identity proofing service.
- In combination with one or more other SACs that must include the CO-SAC and where the identity proofing functions that these criteria address form part of a larger service offering.

3.6.1 Assurance Level 1

3.6.1.1 Policy

An enterprise or specified service must:

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 enterprise.

AL1_ID_POL#020 Unique subject identity

Ensure that each applicant's identity is unique within the service's community of subjects and uniquely associable with tokens and/or credentials issued to that identity.

[1] Identity proofing processes for entities that are not human persons will vary by assurance level and will utilize existing SSL and EV SSL issuance requirements from the CA Browser Forum for the appropriate level of assurance. Non-individual verification requirements will be attached as an appendix to this document.

3.6.1.2 Identity Verification

3.6.1.2.1 In-Person Public Verification

An enterprise or specified service must:

AL1_ID_IPV#010 Required evidence

Accept a self-assertion of identity.

AL1_ID_IPV#020 Evidence checks

Accept self-attestation of evidence.

3.6.1.2.2 Remote Public Verification

If the specific service offers remote identity proofing to applicants with whom it has no previous relationship, then it must comply with the criteria in this section.

An enterprise or specified service must:

AL1_ID_RPV#010 Required evidence

Require the applicant to provide a contact email address. In the case the user does not have email address or does not wish to provide an email address a telephone contact is required.

AL1_ID_RPV#020 Evidence checks

Verify the provided information by either:

a) confirming the request by calling the number;
b) successfully sending a confirmatory email and receiving a positive acknowledgement.

3.6.1.2.3 Secondary Verification

In each of the above cases, an enterprise or specified service must:

AL1_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).

1334

1335

3.6.2 Assurance Level 2

3.6.2.1 Policy

The specific service must show that it applies identity proofing policies and procedures and that it retains appropriate records of identity proofing activities and evidence.

The enterprise or specified service must:

AL2_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 enterprise.

AL2_ID_POL#020 Unique subject identity

Ensure that each applicant's identity is unique within the service's community of subjects and uniquely associable with tokens and/or credentials issued to that identity.

AL2_ID_POL#030 Published Proofing Policy

For each service it offers, make available the Identity Proofing Policy under which it verifies the identity of applicants[2] in form, language, and media accessible to the declared community of Users.

AL2_ID_POL#040 Adherence to Proofing Policy

Perform all identity proofing strictly in accordance with its published Identity Proofing Policy.

3.6.2.2 Identity Verification

The enterprise or specific service must:

[2] For an identity proofing service that is within the management scope of a credential management service provider, this should be the credential management service's definitive policy; for a stand-alone identity proofing service, the policy may be either that of a client who has imposed one through contract, the ID service's own policy, or a separate policy that explains how the client's policies will be complied with.

AL2_ID_IDV#000 Identity Proofing classes

a) include in its Service Definition at least one of the following classes of identity proofing service, and;

b) may offer any additional classes of identity proofing service it chooses, subject to the nature and the entitlement of the CSP concerned;

c) Fulfill the applicable assessment criteria according to its choice of identity proofing service, i.e. conform to at least one of the criteria sets defined in:

i) §3.6.2.2.1, "In-Person Public Verification";

ii) §3.6.2.2.2, "Remote Public Verification";

iii) §3.6.2.2.3, "Current Relationship Verification";

iv) §3.6.2.2.4, "Affiliation Verification".

3.6.2.2.1 In-Person Public Verification

If the specific service offers in-person identity proofing to applicants with whom it has no previous relationship, then it must comply with the criteria in this section.

The enterprise or specified service must:

AL2_ID_IPV#010 Required evidence

Ensure that the applicant is in possession of a primary Government Picture ID document that bears a photographic image of the holder.

AL2_ID_IPV#020 Evidence checks

Have in place and apply processes which ensure that the presented document:

a) appears to be a genuine document properly issued by the claimed issuing authority and valid at the time of application;

b) bears a photographic image of the holder that matches that of the applicant;

c) provides all reasonable certainty that the identity exists and that it uniquely identifies the applicant.

3.6.2.2.2 Remote Public Verification

If the specific service offers remote identity proofing to applicants with whom it has no previous relationship, then it must comply with the criteria in this section.

An enterprise or specified service must:

AL2_ID_RPV#010 Required evidence

Ensure that the applicant submits the references of and attests to current possession of a primary Government Picture ID document, and one of:

a) a second Government ID;
b) an employee or student ID number;
c) a financial account number (e.g., checking account, savings account, loan or credit card) or;
d) a utility service account number (e.g., electricity, gas, or water) for an address matching that in the primary document.

Ensure that the applicant provides additional verifiable personal information that at a minimum must include:

a) a name that matches the referenced photo-ID;
b) date of birth and;
c) current address or personal email address. In the case the user does not have email address or does not wish to provide an email address a telephone contact is required.

Additional information may be requested so as to ensure a unique identity, and alternative information may be sought where the enterprise can show that it leads to at least the same degree of certitude when verified.

AL2_ID_RPV#020 Evidence checks

Inspection and analysis of records against the provided identity references with the specified issuing authorities/institutions or through similar databases:

a) the existence of such records with matching name and reference numbers;
b) corroboration of date of birth, current address of record, and other personal information sufficient to ensure a unique identity.

Confirm address of record by at least one of the following means:

a) RA sends notice to an address of record confirmed in the records check and receives a mailed or telephonic reply from applicant;
b) RA issues credentials in a manner that confirms the address of record supplied by the applicant, for example by requiring applicant to enter on-line some information from a notice sent to the applicant;
c) RA issues credentials in a manner that confirms ability of the applicant to receive telephone communications at telephone number or email at email address associated with the applicant in records. Any secret sent over an unprotected channel shall be reset upon first use.

Additional checks should be performed so as to establish the uniqueness of the claimed identity.

Alternative checks may be performed where the enterprise can show that they lead to at least the same degree of certitude.

3.6.2.2.3 Current Relationship Verification

If the specific service offers identity proofing to applicants with whom it has a current relationship, then it must comply with the criteria in this section.

The enterprise or specified service must:

AL2_ID_CRV#010 Required evidence

Ensure that it has previously exchanged with the applicant a shared secret (e.g., a PIN or password) that meets AL2 (or higher) entropy requirements[3].

AL2_ID_CRV#020 Evidence checks

Ensure that it has:

a) only issued the shared secret after originally establishing the applicant's identity with a degree of rigor equivalent to that required under either the AL2 (or higher) requirements for in-person or remote public verification;

b) an ongoing business relationship sufficient to satisfy the enterprise of the applicant's continued personal possession of the shared secret.

3.6.2.2.4 Affiliation Verification

If the specific service offers identity proofing to applicants on the basis of some form of affiliation, then it must comply with the criteria in this section for the purposes of establishing that affiliation, in addition to the previously stated requirements for the verification of the individual's identity.

The enterprise or specified service must:

AL2_ID_AFV#000 Meet preceding criteria

Meet all the criteria set out above, under §3.6.2.2.3, "Current Relationship Verification".

[3] Refer to NIST SP 800-63 "Appendix A: Estimating Entropy and Strength" or similar recognized sources of such information.

AL2_ID_AFV#010 Required evidence

Ensure that the applicant possesses:

a) identification from the organization with which it is claiming affiliation;
b) agreement from the organization that the applicant may be issued a credential indicating that an affiliation exists.

AL2_ID_AFV#020 Evidence checks

Have in place and apply processes which ensure that the presented documents:

a) each appear to be a genuine document properly issued by the claimed issuing authorities and valid at the time of application;
b) refer to an existing organization with a contact address;
c) indicate that the applicant has some form of recognizable affiliation with the organization;
d) appear to grant the applicant an entitlement to obtain a credential indicating its affiliation with the organization.

3.6.2.2.5 Secondary Verification

In each of the above cases, the enterprise or specified service must:

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).

3.6.2.3 Verification Records

The specific service must retain records of the identity proofing (verification) that it undertakes and provide them to qualifying parties when so required.

An enterprise or specified service must:

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.

Guidance: The facts of the verification process should include the specific record information (source, unique reference, value/content) used in establishing the applicant's identity, and will be determined by the specific processes used and documents accepted

by the CSP. The CSP need not retain these records itself if it uses a third-party service which retains such records securely and to which the CSP has access when required, in which case it must retain a record of the identity of the third-party service providing the verification service or the location at which the (in-house) verification was performed.

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:

a) the subscriber's full name;
b) the subscriber's current address of record;
c) the subscriber's current telephone or email address of record;
d) the subscriber's acknowledgement for issuing the subject with a credential;
e) type, issuing authority, and reference number(s) of all documents checked in the identity proofing process.

AL2_ID_VRC#030 Record Retention

Either retain, securely, the record of the verification process for the duration of the subscriber account plus 7.5 years, or submit same record to a client CSP that has undertaken to retain the record for the requisite period or longer.

3.6.3 Assurance Level 3

3.6.3.1 Policy

The specific service must show that it applies identity proofing policies and procedures and that it retains appropriate records of identity proofing activities and evidence.

The enterprise or specified service must:

AL3_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 enterprise.

AL3_ID_POL#020 Unique subject identity

Ensure that each applicant's identity is unique within the service's community of subjects and uniquely associable with tokens and/or credentials issued to that identity.

AL3_ID_POL#030 Published Proofing Policy

Make available the Identity Proofing Policy under which it verifies the identity of applicants[4] in form, language, and media accessible to the declared community of Users.

AL3_ID_POL#040 Adherence to Proofing Policy

Perform all identity proofing strictly in accordance with its published Identity Proofing Policy, through application of the procedures and processes set out in its Identity Proofing Practice Statement.

3.6.3.2 Identity Verification

The enterprise or specific service must:

[4] For an identity proofing service that is within the management scope of a Credential Management service provider, this should be the Credential Management service's definitive policy; for a stand-alone identity proofing service, the policy may be either that of a client who has defined one through contract, the ID service's own policy or a separate policy that explains how the client's policies will be complied with.

AL3_ID_IDV#000 Identity Proofing classes

a) include in its Service Definition at least one of the following classes of identity proofing services, and;

b) may offer any additional classes of identity proofing service it chooses, subject to the nature and the entitlement of the CSP concerned;

c) Fulfill the applicable assessment criteria according to its choice of identity proofing service, i.e. conform to at least one of the criteria sets defined in:

i) §3.6.3.2.1, "In-Person Public Verification";

ii) §3.6.3.2.2, "Remote Public Verification";

iii) §3.6.3.2.4, "Affiliation Verification".

3.6.3.2.1 In-Person Public Verification

A specific service that offers identity proofing to applicants with whom it has no previous relationship must comply with the criteria in this section.

The enterprise or specified service must:

AL3_ID_IPV#010 Required evidence

Ensure that the applicant is in possession of a primary Government Picture ID document that bears a photographic image of the holder.

AL3_ID_IPV#020 Evidence checks

Have in place and apply processes which ensure that the presented document:

a) appears to be a genuine document properly issued by the claimed issuing authority and valid at the time of application;

b) bears a photographic image of the holder that matches that of the applicant;

c) **is electronically verified by a record check with the specified issuing authority or through similar databases that:**

i) establishes the existence of such records with matching name and reference numbers;

ii) corroborates date of birth, current address of record, and other personal information sufficient to ensure a unique identity;

d) provides all reasonable certainty that the identity exists and that it uniquely identifies the applicant**.**

3.6.3.2.2 Remote Public Verification

A specific service that offers remote identity proofing to applicants with whom it has no previous relationship must comply with the criteria in this section.

The enterprise or specified service must:

AL3_ID_RPV#010 Required evidence

Ensure that the applicant submits the references of and attests to current possession of a primary Government Picture ID document, and one of:

a) a second Government ID;
b) an employee or student ID number;
c) a financial account number (e.g., checking account, savings account, loan, or credit card), or;
d) a utility service account number (e.g., electricity, gas, or water) for an address matching that in the primary document.

Ensure that the applicant provides additional verifiable personal information that at a minimum must include:

e) a name that matches the referenced photo-ID;
f) date of birth;
g) current address or personal email address. In the case the user does not have email address or does not wish to provide an email address a telephone contact is required.

Additional information may be requested so as to ensure a unique identity, and alternative information may be sought where the enterprise can show that it leads to at least the same degree of certitude when verified.

AL3_ID_RPV#020 Evidence checks

Electronically verify by a record check against the provided identity references with the specified issuing authorities/institutions or through similar databases:

a) the existence of such records with matching name and reference numbers;
b) corroboration of date of birth, current address of record, **or personal email address or telephone number**, and other personal information sufficient to ensure a unique identity;
c) dynamic verification of personal information previously provided by or likely to be known only by the applicant.

Confirm address of record by at least one of the following means:

a) RA sends notice to an address of record confirmed in the records check and receives a mailed or telephonic reply from applicant;
b) RA issues credentials in a manner that confirms the address of record supplied by the applicant, for example by requiring applicant to enter on-line some information from a notice sent to the applicant;
c) RA issues credentials in a manner that confirms ability of the applicant to receive telephone communications at telephone number or email at email address associated with the applicant in records. Any secret sent over an unprotected channel shall be reset upon first use.

Additional checks may be performed so as to establish the uniqueness of the claimed identity, and alternative checks may be performed where the enterprise can show that they lead to at least the same degree of certitude.

3.6.3.2.3 Current Relationship Verification

No stipulation.

3.6.3.2.4 Affiliation Verification

A specific service that offers identity proofing to applicants on the basis of some form of affiliation must comply with the criteria in this section to establish that affiliation and with the previously stated requirements to verify the individual's identity.

The enterprise or specified service must:

AL3_ID_AFV#000 Meet preceding criteria

Meet all the criteria set out above, under §**3.6.3.2.2**, "**Remote Public Verification**".

AL3_ID_AFV#010 Required evidence

Ensure that the applicant possesses:

a) identification from the organization with which it is claiming affiliation;
b) agreement from the organization that the applicant may be issued a credential indicating that an affiliation exists.

AL3_ID_AFV#020 Evidence checks

Have in place and apply processes which ensure that the presented documents:

a) each appear to be a genuine document properly issued by the claimed issuing authorities and valid at the time of application;
b) refer to an existing organization with a contact address;

c) indicate that the applicant has some form of recognizable affiliation with the organization;
d) appear to grant the applicant an entitlement to obtain a credential indicating an affiliation with the organization.

3.6.3.2.5 Secondary Verification

In each of the above cases, the enterprise or specified service must also meet the following criteria:

AL3_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 circumstance 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).

3.6.3.3 Verification Records

The specific service must retain records of the identity proofing (verification) that it undertakes and provide them to qualifying parties when so required.

The enterprise or specified service must:

AL3_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 **and the identity of the registrar**, including a reference relating to the verification processes and the date and time of verification.

Guidance: The facts of the verification process should include the specific record information (source, unique reference, value/content) used in establishing the applicant's identity, and will be determined by the specific processes used and documents accepted by the CSP. The CSP need not retain these records itself if it uses a third-party service which retains such records securely and to which the CSP has access when required, in which case it must retain a record of the identity of the third-party service providing the verification service or the location at which the (in-house) verification was performed.

AL3_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:

a) the 'full name;
b) the subscriber's current address of record;
c) the subscriber's current telephone or email address of record;

d) the subscriber's acknowledgement of issuing the subject with a credential;
e) type, issuing authority, and reference number(s) of all documents checked in the identity proofing process;
f) where required, a telephone or email address for related contact and/or delivery of credentials/notifications.

AL3_ID_VRC#030 Record Retention

Either retain, securely, the record of the verification/revocation process for the duration of the subscriber account plus 7.5 years, or submit the same record to a client CSP that has undertaken to retain the record for the requisite period or longer.

3.6.4 Assurance Level 4

Identity proofing at Assurance Level 4 requires the physical presence of the applicant in front of the registration officer with photo ID or other readily verifiable biometric identity information, as well as the requirements set out by the following criteria.

3.6.4.1 Policy

The specific service must show that it applies identity proofing policies and procedures and that it retains appropriate records of identity proofing activities and evidence.

The enterprise or specified service must:

AL4_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 enterprise.

AL4_ID_POL#020 Unique subject identity

Ensure that each applicant's identity is unique within the service's community of subjects and uniquely associable with tokens and/or credentials issued to that identity.

AL4_ID_POL#030 Published Proofing Policy

Make available the Identity Proofing Policy under which it verifies the identity of applicants[5] in form, language, and media accessible to the declared community of users.

AL4_ID_POL#040 Adherence to Proofing Policy

Perform all identity proofing strictly in accordance with its published Identity Proofing Policy, through application of the procedures and processes set out in its Identity Proofing Practice Statement.

3.6.4.2 Identity Verification

The enterprise or specific service may:

[5] For an identity proofing service that is within the management scope of a credential management service provider, this should be the credential management service's definitive policy; for a stand-alone identity proofing service, the policy may be either that of a client which has defined one through contract, the ID service's own policy or a separate policy that explains how the client's policies will be complied with.

AL4_ID_IDV#000 Identity Proofing classes

[Omitted] offer **only face-to-face identity proofing service. Remote verification is not allowed at this assurance level**;

The enterprise or specified service must:

3.6.4.2.1 In-Person Public Verification

AL4_ID_IPV#010 Required evidence

Ensure that the applicant is in possession of:

a) a primary Government Picture ID document that bears a photographic image of the **holder and either:**
- **i) secondary Government Picture ID or an account number issued by a regulated financial institution or;**
- ii) **two items confirming name, and address or email address, such as: utility bill, professional license or membership, or other evidence of equivalent standing. In the case the user does not have email address or does not wish to provide an email address a telephone contact is required.**

AL4_ID_IPV#020 No stipulation

AL4_ID_IPV#030 Evidence checks – primary ID

Ensure that the presented document:

a) **appears to be a genuine document properly issued by the claimed issuing authority and valid at the time of application;**

b) **bears a photographic image of the holder which matches that of the applicant;**

c) **is electronically verified by a record check with the specified issuing authority or through similar databases that:**
- **i) establishes the existence of such records with matching name and reference numbers;**
- **ii) corroborates date of birth, current address of record, and other personal information sufficient to ensure a unique identity;**

d) **provides all reasonable certainty, at AL4, that the identity exists and that it uniquely identifies the applicant.**

AL4_ID_IPV#040 Evidence checks – secondary ID

Ensure that the presented document meets the following conditions:

a) If it is secondary Government Picture ID:
- **i) appears to be a genuine document properly issued by the claimed issuing authority and valid at the time of application;**
- **ii) bears a photographic image of the holder which matches that of the applicant;**
- **iii) states an address at which the applicant can be contacted.**

b) If it is a financial institution account number, is verified by a record check with the specified issuing authority or through similar databases that:
- **i) establishes the existence of such records with matching name and reference numbers;**
- **ii) corroborates date of birth, current address of record, and other personal information sufficient to ensure a unique identity.**

c) If it is two utility bills or equivalent documents:
- **i) each appears to be a genuine document properly issued by the claimed issuing authority;**
- **ii) corroborates current address of record or telephone number sufficient to ensure a unique identity.**

AL4_ID_IPV#050 Applicant knowledge checks

Where the applicant is unable to satisfy any of the above requirements, that the applicant can provide a unique identifier, such as a Social Security Number (SSN), that matches the claimed identity.

3.6.4.2.2 Remote Public Verification

Not permitted

3.6.4.2.3 Affiliation Verification

A specific service that offers identity proofing to applicants on the basis of some form of affiliation must comply with the criteria in this section to establish that affiliation, in addition to complying with the previously stated requirements for verifying the individual's identity.

The enterprise or specified service must:

AL4_ID_AFV#000 Meet preceding criteria

Meet all the criteria set out above, under §**3.6.4.2.1**, "**In-Person Public Verification**".

AL4_ID_AFV#010 Required evidence

Ensure that the applicant possesses:

a) identification from the organization with which it is claiming affiliation;

b) agreement from the organization that the applicant may be issued a credential indicating that an affiliation exists.

AL4_ID_AFV#020 Evidence checks

Have in place and apply processes which ensure that the presented documents:

a) each appear to be a genuine document properly issued by the claimed issuing authorities and valid at the time of application;
b) refer to an existing organization with a contact address;
c) indicate that the applicant has some form of recognizable affiliation with the organization;
d) appear to grant the applicant an entitlement to obtain a credential indicating an affiliation with the organization.

3.6.4.2.4 Secondary Verification

In each of the above cases, the enterprise or specified service must also meet the following criteria:

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).

3.6.4.3 Verification Records

The specific service must retain records of the identity proofing (verification) that it undertakes and provide them to qualifying parties when so required.

The enterprise or specified service must:

AL4_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 and the identity of the registrar, including a reference relating to the verification processes and the date and time of verification **issued by a trusted time-source**.

Guidance: The facts of the verification process should include the specific record information (source, unique reference, value/content) used in establishing the applicant's identity, and will be determined by the specific processes used and documents accepted by the CSP. The CSP need not retain these records itself if it uses a third-party service

which retains such records securely and to which the CSP has access when required, in which case it must retain a record of the identity of the third-party service providing the verification service or the location at which the (in-house) verification was performed.

AL4_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:

a) the subscriber's full name;
b) the subscriber's current address of record;
c) the subscriber's current telephone or email address of record;
d) the subscriber's authorization for issuing the subject a credential;
e) type, issuing authority, and reference number(s) of all documents checked in the identity proofing process;
f) a biometric record of each required representative of the affiliating organization (e.g., a photograph, fingerprint, voice recording), as determined by that organization's governance rules/charter.

AL4_ID_VRC#030 Record Retention

Either retain, securely, the record of the verification/revocation process for the duration of the subscriber account plus **10.5** years, or submit the record to a client CSP that has undertaken to retain the record for the requisite period or longer.

3.6.5 Compliance Tables

Use the following tables to correlate criteria for a particular Assurance Level (AL) and the evidence offered to support compliance.

Service providers preparing for an assessment can use the table appropriate to the AL at which they are seeking approval to correlate evidence with criteria or to justify non-applicability (e.g., "specific service types not offered").

Assessors can use the tables to record the steps in their assessment and their determination of compliance or failure.

Table 3-5. ID-SAC - AL1 Compliance

Clause	Description	Compliance
AL1_ID_POL#010	Unique service identity	
AL1_ID_POL#020	Unique subject identity	
AL1_ID_IPV#010	Required evidence	
AL1_ID_IPV#020	Evidence checks	
AL1_ID_RPV#010	Required evidence	
AL1_ID_RPV#020	Evidence checks	
AL1_ID_SCV#010	Secondary checks	

1838 **Table 3-6.** ID-SAC - AL2 Compliance

Clause	Description	Compliance
AL2_ID_POL#010	Unique service identity	
AL2_ID_POL#020	Unique subject identity	
AL2_ID_POL#030	Published Proofing Policy	
AL2_ID_POL#040	Adherence to Proofing Policy	
AL2_ID_IDV#000	Identity Proofing classes	
AL2_ID_IPV#010	Required evidence	
AL2_ID_IPV#020	Evidence checks	
AL2_ID_RPV#010	Required evidence	
AL2_ID_RPV#020	Evidence checks	
AL2_ID_CRV#010	Required evidence	
AL2_ID_CRV#020	Evidence checks	
AL2_ID_AFV#000	Meet preceding criteria	
AL2_ID_AFV#010	Required evidence	
AL2_ID_AFV#020	Evidence checks	
AL2_ID_SCV#010	Secondary checks	
AL2_ID_VRC#010	Verification Records for Personal Applicants	
AL2_ID_VRC#020	Verification Records for Affiliated Applicants	
AL2_ID_VRC#030	Record Retention	

1839

1840

1841 **Table 3-7.** ID-SAC - AL3 compliance

Clause	Description	Compliance
AL3_ID_POL#010	Unique service identity	
AL3_ID_POL#020	Unique subject identity	
AL3_ID_POL#030	Published Proofing Policy	
AL3_ID_POL#040	Adherence to Proofing Policy	
AL3_ID_IDV#000	Identity Proofing classes	
AL3_ID_IPV#010	Required evidence	
AL3_ID_IPV#020	Evidence checks	
AL3_ID_RPV#010	Required evidence	
AL3_ID_RPV#020	Evidence checks	
AL3_ID_AFV#000	Meet preceding criteria	
AL3_ID_AFV#010	Required evidence	
AL3_ID_AFV#020	Evidence checks	
AL3_ID_SCV#010	Secondary checks	
AL3_ID_VRC#010	Verification Records for Personal Applicants	
AL3_ID_VRC#020	Verification Records for Affiliated Applicants	
AL3_ID_VRC#030	Record Retention	

1842

1843

1844 **Table 3-8.** ID-SAC - AL4 compliance

Clause	Description	Compliance
AL4_ID_POL#010	Unique service identity	
AL4_ID_POL#020	Unique subject identity	
AL4_ID_POL#030	Published Proofing Policy	
AL4_ID_POL#040	Adherence to Proofing Policy	
AL3_ID_IDV#000	Identity Proofing classes	
AL4_ID_IPV#010	Required evidence	
AL4_ID_IPV#020	No stipulation	No conformity requirement
AL4_ID_IPV#030	Evidence checks – primary ID	
AL4_ID_IPV#040	Evidence checks – secondary ID	
AL4_ID_IPV#050	Applicant knowledge checks	
AL4_ID_AFV#000	Meet preceding criteria	
AL4_ID_AFV#010	Required evidence	
AL4_ID_AFV#020	Evidence checks	
AL4_ID_SCV#010	Secondary checks	
AL4_ID_VRC#010	Verification Records for Personal Applicants	
AL4_ID_VRC#020	Verification Records for Affiliated Applicants	
AL4_ID_VRC#030	Record Retention	

1845

1846

3.7 Credential Management Service Assessment Criteria

The Service Assessment Criteria in this section establish requirements for the functional conformity of credential management services and their providers at all ALs defined in Section 2 and in the Identity Assurance Framework: Levels of Assurance document. These criteria are generally referred to elsewhere within IAF documentation as CM-SAC.

The criteria are divided into five parts. Each part deals with a specific functional aspect of the overall credential management process.

This SAC must be used in conjunction with the Common Organizational SAC (CO-SAC), described in Section 3.5, and, in addition, must either:

- explicitly include the criteria of the Identity Proofing SAC ([ID-SAC]) described in Section 3.6, or
- rely upon the criteria of the ID-SAC [ID-SAC] being fulfilled by the use of a Kantara-approved ID-proofing service.

3.7.1 Part A - Credential Operating Environment

The criteria in this part deal with the overall operational environment in which the credential life-cycle management is conducted. The credential management service assessment criteria must be used in conjunction with the Common Organizational criteria described in Section 3.5. In addition, they must either explicitly include the identity proofing service assessment criteria described in Section 3.6 or rely upon those criteria being fulfilled by the use of a Kantara-approved identity proofing service.

These criteria describe requirements for the overall operational environment in which credential lifecycle management is conducted. The common organizational criteria describe broad requirements. The criteria in this section describe implementation specifics. Implementation depends on the AL. The procedures and processes required to create a secure environment for management of credentials and the particular technologies that are considered strong enough to meet the assurance requirements differ considerably from level to level.

3.7.1.1 Assurance Level 1

These criteria apply to PINs and passwords, as well as SAML assertions.

3.7.1.1.1 Not used

No stipulation.

3.7.1.1.2 Security Controls

An enterprise and its specified service must:

AL1_CM_CTR#010 No stipulation

AL1_CM_CTR#020 Protocol threat risk assessment and controls

Account for at least the following protocol threats and apply appropriate controls:

a) password guessing, such that the resistance to an on-line guessing attack against a selected user/password is at least 1 in 2^{10} (1,024);
b) message replay.

AL1_CM_CTR#025 No stipulation

AL1_CM_CTR#030 System threat risk assessment and controls

Account for the following system threats and apply appropriate controls:

a) the introduction of malicious code;
b) compromised authentication arising from insider action;
c) out-of-band attacks by other users and system operators (e.g., the ubiquitous shoulder-surfing);
d) spoofing of system elements/applications;
e) malfeasance on the part of subscribers and subjects.

3.7.1.1.3 Storage of Long-term Secrets

AL1_CM_STS#010 Withdrawn

Withdrawn (AL1_CO_SCO#020 (a) & (b) enforce this requirement)

3.7.1.1.4 Not used

3.7.1.1.5 Subject Options

AL1_CM_OPN#010 Withdrawn

Withdrawn – see AL1_CM_RNR#010.

3.7.1.2 Assurance Level 2

These criteria apply to passwords, as well as acceptable SAML assertions.

3.7.1.2.1 Credential Policy and Practices

These criteria apply to the policy and practices under which credentials are managed.

An enterprise and its specified service must:

AL2_CM_CPP#010 Credential Policy and Practice Statement

Include in its Service Definition a description of the policy against which it issues credentials and the corresponding practices it applies in their management. At a minimum, the Credential Policy and Practice Statement must specify:

a) if applicable, any OIDs related to the Practice and Policy Statement;
b) how users may subscribe to the service/apply for credentials and how users' credentials will be delivered to them;
c) how subscribers acknowledge receipt of tokens and credentials and what obligations they accept in so doing (including whether they consent to publication of their details in credential status directories);
d) how credentials may be renewed, modified, revoked, and suspended, including how requestors are authenticated or their identity re-proven;
e) what actions a subscriber must take to terminate a subscription;
f) how records are retained and archived.

AL2_CM_CPP#020 No stipulation

AL2_CM_CPP#030 Management Authority

Have a nominated management body with authority and responsibility for approving the Credential Policy and Practice Statement and for its implementation.

3.7.1.2.2 Security Controls

An enterprise and its specified service must:

AL2_CM_CTR#010 Secret revelation

Withdrawn.

AL2_CM_CTR#020 Protocol threat risk assessment and controls

Account for at least the following protocol threats **in its risk assessment** and apply **[omitted]** controls **that reduce them to acceptable risk levels**:

a) password guessing, such that the resistance to an on-line guessing attack against a selected user/password is at least 1 in 2^{14} **(16,384)**;
b) message replay**, showing that it is impractical**;
c) eavesdropping, showing that it is impractical.

AL2_CM_CTR#025 Permitted authentication protocols

Permit only the following authentication protocols:

a) tunneled password;
b) zero knowledge-base password;
c) SAML assertions.

AL2_CM_CTR#028 One-time passwords

Use only one-time passwords which:

a) are generated using an approved block-cipher or hash function to combine a symmetric key, stored on the device, with a nonce;
b) derive the nonce from a date and time, or a counter generated on the device;
c) have a limited lifetime, in the order of minutes.

AL2_CM_CTR#030 System threat risk assessment and controls

Account for the following system threats **in its risk assessment** and apply **[omitted]** controls **that reduce them to acceptable risk levels**:

a) the introduction of malicious code;
b) compromised authentication arising from insider action;
c) out-of-band attacks by both users and system operators (e.g., the ubiquitous shoulder-surfing);
d) spoofing of system elements/applications;
e) malfeasance on the part of subscribers and subjects;
f) intrusions leading to information theft.

AL2_CM_CTR#040 Specified Service's Key Management

Specify and observe procedures and processes for the generation, storage, and destruction of its own cryptographic keys used for securing the specific service's assertions and other publicized information. At a minimum, these should address:

a) the physical security of the environment;
b) access control procedures limiting access to the minimum number of authorized personnel;
c) public-key publication mechanisms;
d) application of controls deemed necessary as a result of the service's risk assessment;

e) destruction of expired or compromised private keys in a manner that prohibits their retrieval, or their archival in a manner that prohibits their reuse;

f) applicable cryptographic module security requirements, quoting FIPS 140-2 [FIPS140-2] or equivalent, as established by a recognized national technical authority.

3.7.1.2.3 Storage of Long-term Secrets

AL2_CM_STS#010 Withdrawn

Withdrawn (AL2_CO_SCO#020 (a) & (b) enforce this requirement).

3.7.1.2.4 Security-Relevant Event (Audit) Records

3.7.1.2.5 No stipulation

AL2_CM_OPN#010 Withdrawn

Withdrawn – see AL2_CM_RNR#010.

3.7.1.3 Assurance Level 3

These criteria apply to one-time password devices and soft crypto applications protected by passwords or biometric controls, as well as cryptographically-signed SAML assertions.

3.7.1.3.1 Credential Policy and Practices

These criteria apply to the policy and practices under which credentials are managed.

An enterprise and its specified service must:

AL3_CM_CPP#010 Credential Policy and Practice Statement

Include in its Service Definition a full description of the policy against which it issues credentials and the corresponding practices it applies in their issuance. At a minimum, the Credential Policy and Practice Statement must specify:

a) if applicable, any OIDs related to the Credential Policy and Practice Statement;
b) how users may subscribe to the service/apply for credentials and how the users' credentials will be delivered to them;
c) how subscribers acknowledge receipt of tokens and credentials and what obligations they accept in so doing (including whether they consent to publication of their details in credential status directories);
d) how credentials may be renewed, modified, revoked, and suspended, including how requestors are authenticated or their identity proven;
e) what actions a subscriber must take to terminate a subscription;
f) how records are retained and archived.

AL3_CM_CPP#020 No stipulation

AL3_CM_CPP#030 Management Authority

Have a nominated or appointed high-level management body with authority and responsibility for approving the Certificate Policy and Certification Practice Statement, including ultimate responsibility for their proper implementation.

3.7.1.3.2 Security Controls

AL3_CM_CTR#010 No stipulation

AL3_CM_CTR#020 Protocol threat risk assessment and controls

Account for at least the following protocol threats in its risk assessment and apply controls that reduce them to acceptable risk levels:

a) password guessing, such that the resistance to an on-line guessing attack against a selected user/password is at least 1 in 2^{14} **(16,384)**;
b) message replay, showing that it is impractical;
c) eavesdropping, showing that it is impractical;
d) relying party (verifier) impersonation, showing that it is impractical;
e) man-in-the-middle attack, showing that it is impractical.

The above list shall not be considered to be a complete list of threats to be addressed by the risk assessment.

AL3_CM_CTR#025 Permitted authentication protocols

For non-PKI credentials, permit only the following authentication protocols:

a) tunneled password;
b) zero knowledge-base password;
c) SAML assertions.

AL3_CM_CTR#030 System threat risk assessment and controls

Account for the following system threats in its risk assessment and apply controls that reduce them to acceptable risk levels:

a) the introduction of malicious code;
b) compromised authentication arising from insider action;
c) out-of-band attacks by both users and system operators (e.g., shoulder-surfing);
d) spoofing of system elements/applications;
e) malfeasance on the part of subscribers and subjects;
f) intrusions leading to information theft.

The above list shall not be considered to be a complete list of threats to be addressed by the risk assessment.

AL3_CM_CTR#040 Specified Service's Key Management

Specify and observe procedures and processes for the generation, storage, and destruction of its own cryptographic keys used for securing the specific service's assertions and other publicized information. At a minimum, these should address:

a) the physical security of the environment;
b) access control procedures limiting access to the minimum number of authorized personnel;
c) public-key publication mechanisms;
d) application of controls deemed necessary as a result of the service's risk assessment;
e) destruction of expired or compromised private keys in a manner that prohibits their retrieval or their archival in a manner that prohibits their reuse;

f) applicable cryptographic module security requirements, quoting FIPS 140-2 [FIPS140-2] or equivalent, as established by a recognized national technical authority.

3.7.1.3.3 Storage of Long-term Secrets

An enterprise and its specified service must:

AL3_CM_STS#010 Withdrawn

Withdrawn (AL3_CO_SCO#020 (a) & (b) enforce this requirement).

AL3_CM_STS#020 Stored Secret Encryption

Encrypt such shared secret files so that:

a) the encryption key for the shared secret file is encrypted under a key held in a FIPS 140-2 [FIPS140-2] Level 2 or higher validated hardware or software cryptographic module or any FIPS 140-2 Level 3 or 4 cryptographic module, or equivalent, as established by a recognized national technical authority;
b) the shared secret file is decrypted only as immediately required for an authentication operation;
c) shared secrets are protected as a key within the boundary of a FIPS 140-2 Level 2 or higher validated hardware cryptographic module or any FIPS 140-2 Level 3 or 4 cryptographic module and are not exported from the module in plain text, or equivalent, as established by a recognized national technical authority;
d) shared secrets are split by an "*n from m*" cryptographic secret sharing method.

3.7.1.3.4 Security-relevant Event (Audit) Records

These criteria describe the need to provide an auditable log of all events that are pertinent to the correct and secure operation of the service. The common organizational criteria applying to provision of an auditable log of all security-related events pertinent to the correct and secure operation of the service must also be considered carefully. These criteria carry implications for credential management operations.

In the specific context of a certificate management service, an enterprise and its specified service must:

AL3_CM_SER#010 Security event logs

Ensure that such audit records include:

a) the identity of the point of registration (irrespective of whether internal or outsourced);

b) generation of the subscriber's keys or the evidence that the subscriber was in possession of both parts of their own key-pair;
c) generation of the subscriber's certificate;
d) dissemination of the subscriber's certificate;
e) any revocation or suspension associated with the subscriber's certificate.

3.7.1.3.5 Subject options

AL3_CM_OPN#010 Changeable PIN/Password

Withdrawn – see AL3_CM_RNR#010.

3.7.1.4 Assurance Level 4

These criteria apply exclusively to cryptographic technology deployed through a Public Key Infrastructure. This technology requires hardware tokens protected by password or biometric controls. No other forms of credential are permitted at AL4.

3.7.1.4.1 Certification Policy and Practices

These criteria apply to the policy and practices under which certificates are managed.

An enterprise and its specified service must:

AL4_CM_CPP#010 No stipulation

AL4_CM_CPP#020 Certificate Policy/Certification Practice Statement

Include in its Service Definition its full Certificate Policy and the corresponding Certification and Practice Statement. The Certificate Policy and Certification Practice Statement must conform to IETF RFC 3647 (2003-11) [RFC 3647] in their content and scope or be demonstrably consistent with the content or scope of that RFC. At a minimum, the Certificate Policy must specify:

a) applicable OIDs for each certificate type issued;
b) how users may subscribe to the service/apply for certificates, and how certificates will be issued to them;
c) if users present their own keys, how they will be required to demonstrate possession of the private key;
d) if users' keys are generated for them, how the private keys will be delivered to them;
e) how subscribers acknowledge receipt of tokens and credentials and what obligations they accept in so doing (including whether they consent to publication of their details in certificate status directories);
f) how certificates may be renewed, re-keyed, modified, revoked, and suspended, including how requestors are authenticated or their identity proven;
g) what actions a subscriber must take to terminate their subscription.

AL4_CM_CPP#030 Management Authority

Have a nominated or appointed high-level management body with authority and responsibility for approving the Certificate Policy and Certification Practice Statement, including ultimate responsibility for their proper implementation.

3.7.1.4.2 Security Controls

An enterprise and its specified service must:

2137 AL4_CM_CTR#010 No stipulation

2138 AL4_CM_CTR#020 Protocol threat risk assessment and controls

2139 Account for at least the following protocol threats in its risk assessment and apply
2140 controls that reduce them to acceptable risk levels:

2141 a) password guessing, showing that there is sufficient entropy;
2142 b) message replay, showing that it is impractical;
2143 c) eavesdropping, showing that it is impractical;
2144 d) relying party (verifier) impersonation, showing that it is impractical;
2145 e) man-in-the-middle attack, showing that it is impractical;
2146 **f) session hijacking, showing that it is impractical.**

2147 The above list shall not be considered to be a complete list of threats to be addressed by
2148 the risk assessment.

2149 AL4_CM_CTR#025 No stipulation

2150 AL4_CM_CTR#030 System threat risk assessment and controls

2151 Account for the following system threats in its risk assessment and apply controls that
2152 reduce them to acceptable risk levels:

2153 a) the introduction of malicious code;
2154 b) compromised authentication arising from insider action;
2155 c) out-of-band attacks by both users and system operators (e.g., shoulder-surfing);
2156 d) spoofing of system elements/applications;
2157 e) malfeasance on the part of subscribers and subjects;
2158 f) intrusions leading to information theft.

2159 The above list shall not be considered to be a complete list of threats to be addressed by
2160 the risk assessment.

2161 AL4_CM_CTR#040 Specified Service's Key Management

2162 Specify and observe procedures and processes for the generation, storage, and destruction
2163 of its own cryptographic keys used for securing the specific service's assertions and other
2164 publicized information. At a minimum, these should address:

2165 a) the physical security of the environment;
2166 b) access control procedures limiting access to the minimum number of authorized
2167 personnel;
2168 c) public-key publication mechanisms;
2169 d) application of controls deemed necessary as a result of the service's risk
2170 assessment;

e) destruction of expired or compromised private keys in a manner that prohibits their retrieval, or their archival in a manner which prohibits their reuse;
f) applicable cryptographic module security requirements, quoting FIPS 140-2 [FIPS140-2] or equivalent, as established by a recognized national technical authority.

3.7.1.4.3 Storage of Long-term Secrets

The enterprise and its specified service must meet the following criteria:

AL4_CM_STS#010 Stored Secrets

a) Withdrawn (AL4_CO_SCO#020 (a) & (b) enforce this requirement)

b) apply discretionary access controls that limit access to trusted administrators and to those applications that require access.

AL4_CM_STS#020 Stored Secret Encryption

Encrypt such **[omitted]** secret files so that:

a) the encryption key for the **[omitted]** secret file is encrypted under a key held in a FIPS 140-2 [FIPS140-2] Level 2 or higher validated hardware cryptographic module or any FIPS 140-2 Level 3 or 4 cryptographic module, or equivalent, as established by a recognized national technical authority;
b) the **[omitted]** secret file is decrypted only as immediately required for a key recovery operation;
c) **[omitted]** secrets are protected as a key within the boundary of a FIPS 140-2 Level 2 or higher validated hardware cryptographic module or any FIPS 140-2 Level 3 or 4 cryptographic module and are not exported from the module in plaintext, or equivalent, as established by a recognized national technical authority;
d) escrowed secrets are split by an "*n from m*" cryptographic secret **storing** method.

3.7.1.4.4 Security-relevant Event (Audit) Records

These criteria describe the need to provide an auditable log of all events that are pertinent to the correct and secure operation of the service. The common organizational criteria relating to the recording of all security-related events must also be considered carefully. These criteria carry implications for credential management operations.

In the specific context of a certificate management service, an enterprise and its specified service must:

AL4_CM_SER#010 Security event logs

Ensure that such audit records include:

a) the identity of the point of registration (irrespective of whether internal or outsourced);
b) generation of the subscriber's keys or evidence that the subscriber was in possession of both parts of the key-pair;
c) generation of the subscriber's certificate;
d) dissemination of the subscriber's certificate;
e) any revocation or suspension associated with the subscriber's credential.

3.7.1.4.5 Subject Options

AL4_CM_OPN#010 Changeable PIN/Password

Withdrawn – see AL4_CM_RNR#010.

3.7.2 Part B - Credential Issuing

These criteria apply to the verification of the identity of the subject of a credential and with token strength and credential delivery mechanisms. They address requirements levied by the use of various technologies to achieve the appropriate AL[6]. These criteria include by reference all applicable criteria in Section 3.6.

3.7.2.1 Assurance Level 1

3.7.2.1.1 Identity Proofing

These criteria determine how the enterprise shows compliance with the criteria for fulfilling identity proofing functions.

The enterprise and its specified service must:

AL1_CM_IDP#010 Self-managed Identity Proofing

If the enterprise assumes direct responsibility for identity proofing functions, show, by direct inclusion, compliance with all applicable identity proofing service assessment criteria[7] ([ID-SAC]) for AL1 or higher.

AL1_CM_IDP#020 Kantara-Recognized outsourced service

If the enterprise outsources responsibility for identity proofing functions and uses a service already Kantara-Recognized, show that the service in question has been approved at AL1 or higher.

AL1_CM_IDP#030 Non-recognized outsourced service

If the enterprise outsources responsibility for identity proofing functions, ensure that each provider of such a service demonstrates compliance with all applicable identity proofing service assessment criteria for AL1 or higher, and that the enterprise, itself, has in place controls to ensure the continued fulfillment of those criteria by the provider to which the functions have been outsourced.

AL1_CM_IDP#040 Revision to subscriber information

Provide a means for subscribers to amend their stored information after registration.

[6] Largely driven by the guidance in NIST SP 800-63 [NIST800-63].

[7] Not all criteria may be applicable – the precise scope (definition) of the identity proofing performed by a particular service may exclude certain functionality and therefore certain criteria.

3.7.2.1.2 Credential Creation

These criteria address the requirements for creation of credentials that can only be used at AL1. Any credentials/tokens that comply with the criteria stipulated for AL2 and higher are acceptable at AL1.

An enterprise and its specified service must:

AL1_CM_CRN#010 Authenticated Request

Only accept a request to generate a credential and bind it to an identity if the source of the request can be authenticated as being authorized to perform identity proofing at AL1 or higher.

AL1_CM_CRN#020 No stipulation

AL1_CM_CRN#030 Credential uniqueness

Allow the subscriber 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.

3.7.2.1.3 Not used

3.7.2.1.4 Not used

3.7.2.2 Assurance Level 2

3.7.2.2.1 Identity Proofing

These criteria determine how the enterprise shows compliance with the criteria for fulfilling identity proofing functions.

The enterprise and its specified service must:

AL2_CM_IDP#010 Self-managed Identity Proofing

If the enterprise assumes direct responsibility for identity proofing functions, show, by direct inclusion, compliance with all applicable identity proofing service assessment criteria ([ID-SAC]) for AL**2** or higher.

AL2_CM_IDP#020 Kantara-Recognized outsourced service

If the enterprise outsources responsibility for identity proofing functions and uses a service already Kantara-Recognized, show that the service in question has been approved at AL**2** or higher **and that its approval has at least six months of remaining validity**.

AL2_CM_IDP#030 Non- Kantara-Recognized outsourced service

If the enterprise outsources responsibility for identity proofing functions, ensure that each provider of such a service demonstrates compliance with all applicable identity proofing service assessment criteria for AL2 or higher, and that the enterprise, itself, has in place controls to ensure the continued fulfillment of those criteria by the provider to which the functions have been outsourced.

AL2_CM_IDP#040 Revision to subscriber information

Provide a means for subscribers to **securely** amend their stored information after registration**, either by re-proving their identity, as in the initial registration process, or by using their credentials to authenticate their revision**.

3.7.2.2.2 Credential Creation

These criteria define the requirements for creation of credentials whose highest use is at AL2. Credentials/tokens that comply with the criteria stipulated at AL3 and higher are also acceptable at AL2 and below.

Note, however, that a token and credential required by a higher AL but created according to these criteria may not necessarily provide that higher level of assurance for the claimed identity of the subscriber. Authentication can only be provided at the assurance level at which the identity is proven.

An enterprise and its specified service must:

AL2_CM_CRN#010 Authenticated Request

Only accept a request to generate a credential and bind it to an identity if the source of the request can be authenticated**, i.e., Registration Authority (RA), as being authorized to perform identity proofing at AL2 or higher**.

AL2_CM_CRN#020 Unique identity

Ensure that the identity which relates to a specific applicant is unique within the specified service, including identities previously used and that are now cancelled, other than its re-assignment to the same applicant.

Guidance: This requirement is intended to prevent identities that may exist in a Relying Party's access control list from possibly representing a different physical person.

AL2_CM_CRN#030 Credential uniqueness

Allow the subscriber 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.

AL2_CM_CRN#035 Convey credential

Be capable of conveying the unique identity information associated with a credential to Verifiers and Relying Parties.

AL2_CM_CRN#040 Password strength

Only allow passwords that, over the life of the password, have resistance to an on-line guessing attack against a selected user/password of at least 1 in 2^{14} (16,384), accounting for state-of-the-art attack strategies, and at least 10 bits of min-entropy[8].

AL2_CM_CRN#050 One-time password strength

Only allow password tokens that have a resistance to online guessing attack against a selected user/password of at least 1 in 2^{14} (16,384), accounting for state-of-the-art attack strategies, and at least 10 bits of min-entropy[8].

[8] Refer to NIST SP 800-63 "Appendix A: Estimating Entropy and Strength" or similar recognized sources of such information.

AL2_CM_CRN#060 Software cryptographic token strength

Ensure that software cryptographic keys stored on general-purpose devices:

a) are protected by a key and cryptographic protocol that are evaluated against FIPS 140-2 [FIPS140-2] Level 2, or equivalent, as established by a recognized national technical authority;
b) require password or biometric activation by the subscriber or employ a password protocol when being used for authentication.

AL2_CM_CRN#070 Hardware token strength

Ensure that hardware tokens used to store cryptographic keys:

a) employ a cryptographic module that is evaluated against FIPS 140-2 [FIPS140-2] Level 1 or higher, or equivalent, as established by a recognized national technical authority;
b) require password or biometric activation by the subscriber or also employ a password when being used for authentication.

AL2_CM_CRN#080 No stipulation

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.

3.7.2.2.3 Subject Key Pair Generation

No stipulation.

3.7.2.2.4 Credential Delivery

An enterprise and its specified service must:

AL2_CM_CRD#010 Notify Subject of Credential Issuance

Notify the subject of the credential's issuance and, if necessary, confirm the Subject's contact information by:

a) sending notice to the address of record confirmed during identity proofing or;
b) issuing the credential(s) in a manner that confirms the address of record supplied by the applicant during identity proofing or;

c) issuing the credential(s) in a manner that confirms the ability of the applicant to receive telephone communications at a fixed-line telephone number or postal address supplied by the applicant during identity proofing.

AL2_CM_CRD#015 Confirm Applicant's identity (in person)

Prior to delivering the credential, require the Applicant to identify themselves in person in any new electronic transaction (beyond the first transaction or encounter) by either:

(a) using a 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, or;

(b) through the use of a biometric that was recorded during a prior encounter.

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.

3.7.2.3 Assurance Level 3

3.7.2.3.1 Identity Proofing

These criteria in this section determine how the enterprise shows compliance with the criteria for fulfilling identity proofing functions.

The enterprise and its specified service must:

AL3_CM_IDP#010 Self-managed Identity Proofing

If the enterprise assumes direct responsibility for identity proofing functions, show, by direct inclusion, compliance with all applicable identity proofing service assessment criteria for AL**3 or AL4**.

AL3_CM_IDP#020 Kantara-Recognized outsourced service

If the enterprise outsources responsibility for identity proofing functions and uses a service already Kantara-Recognized, show that the service in question has been certified at AL**3 or AL4** and that its approval has at least six months of remaining validity.

AL3_CM_IDP#030 Non- Kantara-Recognized outsourced service

***Not* use any non- Kantara-Recognized services for identity proofing unless they can be demonstrated to have satisfied equivalently rigorous requirements established by another scheme recognized by IAWG.**

AL3_CM_IDP#040 Revision to subscriber information

Provide a means for subscribers to securely amend their stored information after registration, either by re-proving their identity as in the initial registration process or by using their credentials to authenticate their revision. **Successful revision must, where necessary, instigate the re-issuance of the credential.**

3.7.2.3.2 Credential Creation

These criteria define the requirements for creation of credentials whose highest use is AL3. Any credentials/tokens that comply with the criteria stipulated at AL4 are also acceptable at AL3 and below.

Note, however, that a token and credential type required by a higher AL but created according to these criteria may not necessarily provide that higher level of assurance for the claimed identity of the subscriber. Authentication can only be provided at the assurance level at which the identity is proven.

An enterprise and its specified service must:

AL3_CM_CRN#010 Authenticated Request

Only accept a request to generate a credential and bind it to an identity if the source of the request, i.e., Registration Authority (RA), can be authenticated as being authorized to perform identity proofing at AL**3** or higher.

AL3_CM_CRN#020 Unique identity

Ensure that the identity which relates to a specific applicant is unique within the specified service, including identities previously used and that are now cancelled other than its re-assignment to the same applicant.

Guidance: This requirement is intended to prevent identities that may exist in a Relying Party's access control lists from possibly representing a different physical person.

AL3_CM_CRN#030 Credential uniqueness

Allow the subscriber 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.

AL3_CM_CRN#035 Convey credential

Be capable of conveying the unique identity information associated with a credential to Verifiers and Relying Parties.

AL3_CM_CRN#040 PIN/Password strength

Not use PIN/password tokens.

AL3_CM_CRN#050 One-time password strength

Only allow one-time password tokens that:

a) depend on a symmetric key stored on a personal hardware device evaluated against FIPS 140-2 [FIPS140-2] Level 1 or higher, or equivalent, as established by a recognized national technical authority;
b) permit at least 10^6 possible password values;
c) require password or biometric activation by the subscriber.

AL3_CM_CRN#060 Software cryptographic token strength

Ensure that software cryptographic keys stored on general-purpose devices:

a) are protected by a key and cryptographic protocol that are evaluated against FIPS 14-2 [FIPS140-2] Level 2, or equivalent, as established by a recognized national technical authority;
b) require password or biometric activation by the subscriber or employ a password protocol when being used for authentication.

AL3_CM_CRN#070 Hardware token strength

Ensure that hardware tokens used to store cryptographic keys:

a) employ a cryptographic module that is evaluated against FIPS 140-2 [FIPS140-2] Level 1 or higher, or equivalent, as established by a recognized national technical authority;
b) require password or biometric activation by the subscriber or also employ a password when being used for authentication.

AL3_CM_CRN#080 Binding of key

If the specified service generates the subject's key pair, that the key generation process securely and uniquely binds that process to the certificate generation and maintains at all times the secrecy of the private key, until it is accepted by the subject.

AL3_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., private 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. **[Omitted]**

3.7.2.3.3 Subject Key Pair Generation

An enterprise and its specified service must:

AL3_CM_SKP#010 Key generation by Specified Service

If the specified service generates the subject's keys:

a) use a FIPS 140-2 [FIPS140-2] compliant algorithm, or equivalent, as established by a recognized national technical authority, that is recognized as being fit for the purposes of the service;
b) only create keys of a key length and for use with a FIPS 140-2 [FIPS140-2] compliant public key algorithm, or equivalent, as established by a recognized

national technical authority, recognized as being fit for the purposes of the service;

c) generate and store the keys securely until delivery to and acceptance by the subject;

d) deliver the subject's private key in a manner that ensures that the privacy of the key is not compromised and only the subject has access to the private key.

AL3_CM_SKP#020 Key generation by Subject

If the subject generates and presents its own keys, obtain the subject's written confirmation that it has:

a) used a FIPS 140-2 [FIPS140-2] compliant algorithm, or equivalent, as established by a recognized national technical authority, that is recognized as being fit for the purposes of the service;

b) created keys of a key length and for use with a FIPS 140-2 [FIPS140-2] compliant public key algorithm, or equivalent, as established by a recognized national technical authority, recognized as being fit for the purposes of the service.

3.7.2.3.4 Credential Delivery

An enterprise and its specified service must:

AL3_CM_CRD#010, Notify Subject of Credential Issuance

Notify the subject of the credential's issuance and, if necessary, confirm Subject's contact information by:

a) sending notice to the address of record confirmed during identity proofing**, and either:**

i) issuing the credential(s) in a manner that confirms the address of record supplied by the applicant during identity proofing, or;

ii) issuing the credential(s) in a manner that confirms the ability of the applicant to receive telephone communications at a phone number supplied by the applicant during identity proofing, while recording the applicant's voice.

AL3_CM_CRD#020 Subject's acknowledgement

Receive acknowledgement of receipt of the credential before it is activated and its directory status record is published (and thereby the subscription becomes active or re-activated, depending upon the circumstances of issue).

3.7.2.4 Assurance Level 4

3.7.2.4.1 Identity Proofing

These criteria determine how the enterprise shows compliance with the criteria for fulfilling identity proofing functions.

An enterprise and its specified service must:

AL4_CM_IDP#010 Self-managed Identity Proofing

If the enterprise assumes direct responsibility for identity proofing functions, show, by direct inclusion, compliance with all applicable identity proofing service assessment criteria for **[omitted]** AL4.

AL4_CM_IDP#020 Kantara-Recognized outsourced service

If the enterprise outsources responsibility for identity proofing functions and uses a service already Kantara-Recognized, show that the service in question has been certified at **[omitted]** AL4 and that its approval has at least **12** months of remaining validity.

AL4_CM_IDP#030 Non- Kantara-Recognized outsourced service

Not use any non- Kantara-Recognized outsourced services for identity proofing unless they can be demonstrated to have satisfied equivalently rigorous requirements established by another scheme recognized by IAWG.

AL4_CM_IDP#040 Revision to subscriber information

Provide a means for subscribers to securely amend their stored information after registration, either by re-proving their identity as in the initial registration process or by using their credentials to authenticate their revision. Successful revision must, where necessary, instigate the re-issuance of the credential.

3.7.2.4.2 Credential Creation

These criteria define the requirements for creation of credentials whose highest use is AL4.

Note, however, that a token and credential created according to these criteria may not necessarily provide that level of assurance for the claimed identity of the subscriber. Authentication can only be provided at the assurance level at which the identity is proven.

An enterprise and its specified service must:

AL4_CM_CRN#010 Authenticated Request

Only accept a request to generate a credential and bind it to an identity if the source of the request, i.e., Registration Authority (RA), can be authenticated as being authorized to perform identity proofing at AL**4**.

AL4_CM_CRN#020 Unique identity

Ensure that the identity which relates to a specific applicant is unique within the specified service, including identities previously used and that are now cancelled, other than its re-assignment to the same applicant.

Guidance: This requirement is intended to prevent identities that may exist in a Relying Party's access control lists from possibly representing a different physical person.

AL4_CM_CRN#030 Credential uniqueness

Allow the subscriber 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.

AL4_CM_CRN#035 Convey credential

Be capable of conveying the unique identity information associated with a credential to Verifiers and Relying Parties.

AL4_CM_CRN#040 PIN/Password strength

Not use PIN/password tokens.

AL4_CM_CRN#050 One-time password strength

***Not* use one-time password tokens.**

AL4_CM_CRN#060 Software cryptographic token strength

***Not* use software cryptographic tokens.**

AL4_CM_CRN#070 Hardware token strength

Ensure that hardware tokens used to store cryptographic keys:

a) employ a cryptographic module that is validated against FIPS 140-2 [FIPS140-2] Level **2** or higher, or equivalent, as determined by a recognized national technical authority;

b) are evaluated against FIPS 140-2 Level 3 or higher, or equivalent, as determined by a recognized national technical authority, for their physical security;

c) require password or biometric activation by the subscriber **[omitted]**.

AL4_CM_CRN#080 Binding of key

If the specified service generates the subject's key pair, that the key generation process securely and uniquely binds that process to the certificate generation and maintains at all times the secrecy of the private key, until it is accepted by the subject.

AL4_CM_CRN#090 Nature of subject

Record the nature of the subject of the credential **[omitted]**, i.e., private 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.

3.7.2.4.3 Subject Key Pair Generation

An enterprise and its specified service must:

AL4_CM_SKP#010 Key generation by Specified Service

If the specified service generates the subject's keys:

a) use a FIPS 140-2 [FIPS140-2] compliant algorithm, or equivalent, as established by a recognized national technical authority, that is recognized as being fit for the purposes of the service;

b) only create keys of a key length and for use with a FIPS 140-2 [FIPS140-2] compliant public key algorithm, or equivalent, as established by a recognized national technical authority, recognized as being fit for the purposes of the service;

c) generate and store the keys securely until delivery to and acceptance by the subject;

d) deliver the subject's private key in a manner that ensures that the privacy of the key is not compromised and only the subject has access to the private key.

AL4_CM_SKP#020 Key generation by Subject

If the subject generates and presents its own keys, obtain the subject's written confirmation that it has:

a) used a FIPS 140-2 [FIPS140-2] compliant algorithm, or equivalent, as established by a recognized national technical authority, that is recognized as being fit for the purposes of the service;
b) created keys of a key length and for use with a FIPS 140-2 [FIPS140-2] compliant public key algorithm, or equivalent, as established by a recognized national technical authority, recognized as being fit for the purposes of the service.

3.7.2.4.4 Credential Delivery

An enterprise and its specified service must:

AL4_CM_CRD#010 Notify Subject of Credential Issuance

Notify the subject of the credential's issuance and, if necessary, confirm Subject's contact information by:

a) sending notice to the address of record confirmed during identity proofing**;**
b) unless the subject presented with a private key, issuing the hardware token to the subject in a manner that confirms the address of record supplied by the applicant during identity proofing;
c) issuing the certificate to the subject over a separate channel in a manner that confirms either the address of record or the email address supplied by the applicant during identity proofing.

AL4_CM_CRD#020 Subject's acknowledgement

Receive acknowledgement of receipt of the **hardware token** before it is activated and **the corresponding certificate and** its directory status record are published (and thereby the subscription becomes active or re-activated, depending upon the circumstances of issue).

3.7.3 Part C - Credential Renewal and Re-issuing

These criteria apply to the renewal and re-issuing of credentials. They address requirements levied by the use of various technologies to achieve the appropriate AL[9]. These criteria include by reference all applicable criteria in Section 3.6 and the renewal and re-issuing processes shall comply in all practical senses with the applicable criteria set forth in Part B of this section.

3.7.3.1 Assurance Level 1

3.7.3.1.1 Renewal/Re-issuance Procedures

These criteria address general renewal and re-issuance functions, to be exercised as specific controls in these circumstances while continuing to observe the general requirements established for initial credential issuance.

An enterprise and its specified service must:

AL1_CM_RNR#010 Changeable PIN/Password

Permit subjects to change their PINs/passwords.

[9] Largely driven by the guidance in NIST SP 800-63 [NIST800-63].

3.7.3.2 Assurance Level 2

3.7.3.2.1 Renewal/Re-issuance Procedures

These criteria address general renewal and re-issuance functions, to be exercised as specific controls in these circumstances while continuing to observe the general requirements established for initial credential issuance.

An enterprise and its specified service must:

AL2_CM_RNR#010 Changeable PIN/Password

Permit subjects to change their **[omitted]** passwords**, but employ reasonable practices with respect to password resets and repeated password failures**.

AL2_CM_RNR#020 Proof-of-possession on Renewal/Re-issuance

Subjects wishing to change their passwords must demonstrate that they are in possession of the unexpired current token prior to the CSP proceeding to renew or re-issue it.

AL2_CM_RNR#030 Renewal/Re-issuance limitations

a. not renew but may re-issue Passwords;

b. neither renew nor re-issue expired tokens;

c. conduct all renewal / re-issuance interactions with the Subject over a protected channel such as SSL/TLS.

Guidance: Renewal is considered as an extension of usability, whereas re-issuance requires a change.

3.7.3.3 Assurance Level 3

3.7.3.3.1 Renewal/Re-issuance Procedures

These criteria address general renewal and re-issuance functions, to be exercised as specific controls in these circumstances while continuing to observe the general requirements established for initial credential issuance.

An enterprise and its specified service must:

AL3_CM_RNR#010 Changeable PIN/Password

Permit subjects to change **the** passwords **used to activate their credentials**.

Further criteria may be determined after AL3 comparability assessment against Federal CAF and NIST SP 800-63.

3.7.3.4 Assurance Level 4

3.7.3.4.1 Renewal/Re-issuance Procedures

These criteria address general renewal and re-issuance functions, to be exercised as specific controls in these circumstances while continuing to observe the general requirements established for initial credential issuance.

An enterprise and its specified service must:

AL4_CM_RNR#010 Changeable PIN/Password

Permit subjects to change the passwords used to activate their credentials.

Further criteria may be determined after AL4 comparability assessment against Federal CAF and NIST SP 800-63.

3.7.4 Part D - Credential Revocation

These criteria deal with credential revocation and the determination of the legitimacy of a revocation request.

3.7.4.1 Assurance Level 1

An enterprise and its specified service must:

3.7.4.1.1 Not used

3.7.4.1.2 Not used

3.7.4.1.3 Secure Revocation Request

This criterion applies when revocation requests between remote components of a service are made over a secured communication.

An enterprise and its specified service must:

AL1_CM_SRR#010 Submit Request

Submit a request for revocation to the Credential Issuer service (function), using a secured network communication, if necessary.

3.7.4.2 Assurance Level 2

3.7.4.2.1 Revocation Procedures

These criteria address general revocation functions, such as the processes involved and the basic requirements for publication.

An enterprise and its specified service must:

AL2_CM_RVP#010 Revocation procedures

a) State the conditions under which revocation of an issued credential may occur;

b) State the processes by which a revocation request may be submitted;

c) State the persons and organizations from which a revocation request will be accepted;

d) State the validation steps that will be applied to ensure the validity (identity) of the Revocant, and;

e) State the response time between a revocation request being accepted and the publication of revised certificate status.

AL2_CM_ RVP#020 Secure status notification

Ensure that published credential status notification information can be relied upon in terms of the enterprise of its origin (i.e., its authenticity) and its correctness (i.e., its integrity).

AL2_CM_ RVP#030 Revocation publication

Unless the credential will expire automatically within 72 hours:

Ensure that published credential status notification is revised within 72 hours of the receipt of a valid revocation request, such that any subsequent attempts to use that credential in an authentication shall be unsuccessful.

AL2_CM_RVP#040 Verify revocation identity

Establish that the identity for which a revocation request is received is one that was issued by the specified service.

AL2_CM_RVP#050 Revocation Records

Retain a record of any revocation of a credential that is related to a specific identity previously verified, solely in connection to the stated credential. At a minimum, records of revocation must include:

a) the Revocant's full name;
b) the Revocant's authority to revoke (e.g., subscriber themselves, someone acting with the subscriber's power of attorney, the credential issuer, law enforcement, or other legal due process);
c) the Credential Issuer's identity (if not directly responsible for the identity proofing service);
d) the identity associated with the credential (whether the subscriber's name or a pseudonym);
e) the reason for revocation.

AL2_CM_RVP#060 Record Retention

Retain, securely, the record of the revocation process for the duration of the subscriber's account plus 7.5 years.

3.7.4.2.2 Verify Revocant's Identity

Revocation of a credential requires that the requestor and the nature of the request be verified as rigorously as the original identity proofing. The enterprise should not act on a request for revocation without first establishing the validity of the request (if it does not, itself, determine the need for revocation).

In order to do so, the enterprise and its specified service must:

AL2_CM_RVR#010 Verify revocation identity

Establish that the credential for which a revocation request is received was one that was issued by the specified service, applying the same process and criteria as would be applied to an original identity proofing.

AL2_CM_RVR#020 Revocation reason

Establish the reason for the revocation request as being sound and well founded, in combination with verification of the Revocant, according to AL2_ID_RVR#030, AL2_ID_RVR#040, or AL2_ID_RVR#050.

AL2_CM_RVR#030 Verify Subscriber as Revocant

When the subscriber seeks revocation of the subscriber's own credential, the enterprise must:

a) if in person, require presentation of a primary Government Picture ID document that shall be electronically verified by a record check against the provided identity with the specified issuing authority's records;
b) if remote:
i. electronically verify a signature against records (if available), confirmed with a call to a telephone number of record, or;
ii. authenticate an electronic request as being from the same subscriber, supported by a credential at Assurance Level 2 or higher.

AL2_CM_RVR#040 CSP as Revocant

Where a CSP seeks revocation of a subscriber's credential, the enterprise must establish that the request is either:

a) from the specified service itself, with authorization as determined by established procedures, or;
b) from the client Credential Issuer, by authentication of a formalized request over the established secure communications network.

AL2_CM_RVR#050 Verify Legal Representative as Revocant

Where the request for revocation is made by a law enforcement officer or presentation of a legal document, the enterprise must:

a) if in-person, verify the identity of the person presenting the request;
b) if remote:
i. **in paper/facsimile form, verify the origin of the legal document by a database check or by telephone with the issuing authority, or;**
ii. **as an electronic request, authenticate it as being from a recognized legal office, supported by a credential at Assurance Level 2 or higher.**

3.7.4.2.3 Secure Revocation Request

This criterion applies when revocation requests must be communicated between remote components of the service organization.

An enterprise and its specified service must:

AL2_CM_SRR#010 Submit Request

Submit a request for the revocation to the Credential Issuer service (function), using a secured network communication.

3.7.4.3 Assurance Level 3

3.7.4.3.1 Revocation Procedures

These criteria address general revocation functions, such as the processes involved and the basic requirements for publication.

An enterprise and its specified service must:

AL3_CM_RVP#010 Revocation procedures

a) State the conditions under which revocation of an issued credential may occur;

b) State the processes by which a revocation request may be submitted;

c) State the persons and organizations from which a revocation request will be accepted;

d) State the validation steps that will be applied to ensure the validity (identity) of the Revocant, and;

e) State the response time between a revocation request being accepted and the publication of revised certificate status.

AL3_CM_ RVP#020 Secure status notification

Ensure that published credential status notification information can be relied upon in terms of the enterprise being its origin (i.e., its authenticity) and its correctness (i.e., its integrity).

AL3_CM_ RVP#030 Revocation publication

[Omitted] Ensure that published credential status notification is revised within **24** hours of the receipt of a valid revocation request, such that any subsequent attempts to use that credential in an authentication shall be unsuccessful. **The nature of the revocation mechanism shall be in accord with the technologies supported by the service.**

AL3_CM_RVP_#040 Verify Revocation Identity

Establish that the identity for which a revocation request is received is one that was issued by the specified service.

AL3_CM_RVP#050 Revocation Records

Retain a record of any revocation of a credential that is related to a specific identity previously verified, solely in connection to the stated credential. At a minimum, records of revocation must include:

a) the Revocant's full name;
b) the Revocant's authority to revoke (e.g., subscriber themselves, someone acting with the subscriber's power of attorney, the credential issuer, law enforcement, or other legal due process);
c) the Credential Issuer's identity (if not directly responsible for the identity proofing service);
d) the identity associated with the credential (whether the subscriber's name or a pseudonym);
e) the reason for revocation.

AL3_CM_RVP#060 Record Retention

Retain, securely, the record of the revocation process for a period which is in compliance with:

a) the records retention policy required by AL2_CM_CPP#010, and;

b) applicable legislation;

and which, in addition, must be not less than the duration of the subscriber's account plus 7.5 years.

3.7.4.3.2 Verify Revocant's Identity

Revocation of a credential requires that the requestor and the nature of the request be verified as rigorously as the original identity proofing. The enterprise should not act on a request for revocation without first establishing the validity of the request (if it does not, itself, determine the need for revocation).

In order to do so, the enterprise and its specified service must:

AL3_CM_RVR#010 Verify revocation identity

Establish that the credential for which a revocation request is received is one that was initially issued by the specified service, applying the same process and criteria as would be applied to an original identity proofing.

AL3_CM_RVR#020 Revocation reason

Establish the reason for the revocation request as being sound and well founded, in combination with verification of the Revocant, according to AL**3**_ID_RVR#030, AL**3**_ID_RVR#040, or AL**3**_ID_RVR#050.

AL3_CM_RVR#030 Verify Subscriber as Revocant

When the subscriber seeks revocation of the subscriber's own credential:

a) if in-person, require presentation of a primary Government Picture ID document that shall be electronically verified by a record check against the provided identity with the specified issuing authority's records;
b) if remote:
   i. electronically verify a signature against records (if available), confirmed with a call to a telephone number of record, or;
   ii. as an electronic request, authenticate it as being from the same subscriber**,** supported by a credential at Assurance Level **3** or higher.

AL3_CM_RVR#040 Verify CSP as Revocant

Where a CSP seeks revocation of a subscriber's credential, establish that the request is either:

a) from the specified service itself, with authorization as determined by established procedures, or;
b) from the client Credential Issuer, by authentication of a formalized request over the established secure communications network.

AL3_CM_RVR#050 Verify Legal Representative as Revocant

Where the request for revocation is made by a law enforcement officer or presentation of a legal document:

a) if in person, verify the identity of the person presenting the request, or;
b) if remote:
   i. in paper/facsimile form, verify the origin of the legal document by a database check or by telephone with the issuing authority, or;
   ii. as an electronic request, authenticate it as being from a recognized legal office**,** supported by a credential at Assurance Level **3** or higher.

3.7.4.3.3 Secure Revocation Request

This criterion applies when revocation requests must be communicated between remote components of the service organization.

An enterprise and its specified service must:

AL3_CM_SRR#010 Submit Request

Submit a request for the revocation to the Credential Issuer service (function), using a secured network communication.

3.7.4.4 Assurance Level 4

3.7.4.4.1 Revocation Procedures

These criteria address general revocation functions, such as the processes involved and the basic requirements for publication.

An enterprise and its specified service must:

AL4_CM_RVP#010 Revocation procedures

a) State the conditions under which revocation of an issued certificate may occur;

b) State the processes by which a revocation request may be submitted;

c) State the persons and organizations from which a revocation request will be accepted;

d) State the validation steps that will be applied to ensure the validity (identity) of the Revocant, and;

e) State the response time between a revocation request being accepted and the publication of revised certificate status.

AL4_CM_ RVP#020 Secure status notification

Ensure that published credential status notification information can be relied upon in terms of the enterprise of its origin (i.e., its authenticity) and its correctness (i.e., its integrity).

AL4_CM_ RVP#030 Revocation publication

Ensure that published credential status notification is revised within **18** hours of the receipt of a valid revocation request, such that any subsequent attempts to use that credential in an authentication shall be unsuccessful. The nature of the revocation mechanism shall be in accordance with the technologies supported by the service.

AL4_CM_RVP#040 No stipulation

AL4_CM_RVP#050 Revocation Records

Retain a record of any revocation of a credential that is related to a specific identity previously verified, solely in connection to the stated credential. At a minimum, records of revocation must include:

a) the Revocant's full name;

b) the Revocant's authority to revoke (e.g., subscriber themselves, someone acting with the subscriber's power of attorney, the credential issuer, law enforcement, or other legal due process);
c) the Credential Issuer's identity (if not directly responsible for the identity proofing service);
d) the identity associated with the credential (whether the subscriber's name or a pseudonym);
e) the reason for revocation.

AL4_CM_RVP#060 Record Retention

Retain, securely, the record of the revocation process for a period which is in compliance with:

c) the records retention policy required by AL2_CM_CPP#010, and;

d) applicable legislation;

and which, in addition, must be not less than the duration of the subscriber's account plus 7.5 years.

3.7.4.4.2 Verify Revocant's Identity

Revocation of a credential requires that the requestor and the nature of the request be verified as rigorously as the original identity proofing. The enterprise should not act on a request for revocation without first establishing the validity of the request (if it does not, itself, determine the need for revocation).

In order to do so, the enterprise and its specified service must:

AL4_CM_RVR#010 Verify revocation identity

Establish that the credential for which a revocation request is received is one that was initially issued by the specified service, applying the same process and criteria as would apply to an original identity proofing.

AL4_CM_RVR#020 Revocation reason

Establish the reason for the revocation request as being sound and well founded, in combination with verification of the Revocant, according to AL4_CM_RVR#030, AL4_CM_RVR#040, or AL4_CM_RVR#050.

AL4_CM_RVR#030 Verify Subscriber as Revocant

Where the subscriber seeks revocation of the subscriber's own credential:

a) if in person, require presentation of a primary Government Picture ID document that shall be **[Omitted]** verified by a record check against the provided identity with the specified issuing authority's records;
b) if remote:
   i. verify a signature against records (if available), confirmed with a call to a telephone number of record, or;
   ii. as an electronic request, authenticate it as being from the same subscriber, supported by a **different** credential at **Assurance Level 4**.

AL4_CM_RVR#040 Verify CSP as Revocant

Where a CSP seeks revocation of a subscriber's credential, establish that the request is either:

a) from the specified service itself, with authorization as determined by established procedures, or;
b) from the client Credential Issuer, by authentication of a formalized request over the established secure communications network.

AL4_CM_RVR#050 Verify Legal Representative as Revocant

Where the request for revocation is made by a law enforcement officer or presentation of a legal document:

a) if in-person, verify the identity of the person presenting the request, or;
b) if remote:
   i. in paper/facsimile form, verify the origin of the legal document by a database check or by telephone with the issuing authority;
   ii. as an electronic request, authenticate it as being from a recognized legal office, supported by a different credential at **Assurance Level 4**.

3.7.4.4.3 Re-keying a credential

Re-keying of a credential requires that the requestor be verified as the subject with as much rigor as was applied to the original identity proofing. The enterprise should not act on a request for re-key without first establishing that the requestor is identical to the subject.

In order to do so, the enterprise and its specified service must:

AL4_CM_RKY#010 Verify Requestor as Subscriber

Where the subscriber seeks a re-key for the subscriber's own credential:

a) if in-person, require presentation of a primary Government Picture ID document that shall be verified by a record check against the provided identity with the specified issuing authority's records;
b) if remote:

i. verify a signature against records (if available), confirmed with a call to a telephone number of record, or;

ii. authenticate an electronic request as being from the same subscriber, supported by a different credential at Assurance Level 4.

AL4_CM_RKY#020 Re-key requests other than subscriber

Re-key requests from any parties other than the subscriber must not be accepted.

3.7.4.4.4 Secure Revocation/Re-key Request

This criterion applies when revocation **or re-key** requests must be communicated between remote components of the service organization.

The enterprise and its specified service must:

AL4_CM_SRR#010 Submit Request

Submit a request for the revocation to the Credential Issuer service (function), using a secured network communication.

3.7.5 Part E - Credential Status Management

These criteria deal with credential status management, such as the receipt of requests for new status information arising from a new credential being issued or a revocation or other change to the credential that requires notification. They also deal with the provision of status information to requesting parties (Verifiers, Relying Parties, courts and others having regulatory authority, etc.) having the right to access such information.

3.7.5.1 Assurance Level 1

3.7.5.1.1 Status Maintenance

An enterprise and its specified service must:

AL1_CM_CSM#010 Maintain Status Record

Maintain a record of the status of all credentials issued.

AL1_CM_CSM#020 No stipulation

AL1_CM_CSM#030 No stipulation

AL1_CM_CSM#040 Status Information Availability

Provide, with 95% availability, a secure automated mechanism to allow relying parties to determine credential status and authenticate the subject's identity.

3.7.5.2 Assurance Level 2

3.7.5.2.1 Status Maintenance

An enterprise and its specified service must:

AL2_CM_CSM#010 Maintain Status Record

Maintain a record of the status of all credentials issued.

AL2_CM_CSM#020 Validation of Status Change Requests

Authenticate all requestors seeking to have a change of status recorded and published and validate the requested change before considering processing the request. Such validation should include:

a) the requesting source as one from which the specified service expects to receive such requests;
b) if the request is not for a new status, the credential or identity as being one for which a status is already held.

AL2_CM_CSM#030 Revision to Published Status

Process authenticated requests for revised status information and have the revised information available for access within a period of 72 hours.

AL2_CM_CSM#040 Status Information Availability

Provide, with 95% availability, a secure automated mechanism to allow relying parties to determine credential status and authenticate the subject's identity.

AL2_CM_CSM#050 Inactive Credentials

Disable any credential that has not been successfully used for authentication during a period of 18 months.

3.7.5.3 Assurance Level 3

3.7.5.3.1 Status Maintenance

An enterprise and its specified service must:

AL3_CM_CSM#010 Maintain Status Record

Maintain a record of the status of all credentials issued.

AL3_CM_CSM#020 Validation of Status Change Requests

Authenticate all requestors seeking to have a change of status recorded and published and validate the requested change before considering processing the request. Such validation should include:

a) the requesting source as one from which the specified service expects to receive such requests;
b) if the request is not for a new status, the credential or identity as being one for which a status is already held.

AL3_CM_CSM#030 Revision to Published Status

Process authenticated requests for revised status information and have the revised information available for access within a period of 72 hours.

AL3_CM_CSM#040 Status Information Availability

Provide, with **99**% availability, a secure automated mechanism to allow relying parties to determine credential status and authenticate the subject's identity.

AL3_CM_CSM#050 Inactive Credentials

Disable any credential that has not been successfully used for authentication during a period of 18 months.

3.7.5.4 Assurance Level 4

3.7.5.4.1 Status Maintenance

An enterprise and its specified service must:

AL4_CM_CSM#010 Maintain Status Record

Maintain a record of the status of all credentials issued.

AL4_CM_CSM#020 Validation of Status Change Requests

Authenticate all requestors seeking to have a change of status recorded and published and validate the requested change before considering processing the request. Such validation should include:

a) the requesting source as one from which the specified service expects to receive such requests;
b) if the request is not for a new status, the credential or identity as being one for which a status is already held.

AL4_CM_CSM#030 Revision to Published Status

Process authenticated requests for revised status information and have the revised information available for access within a period of 72 hours.

AL4_CM_CSM#040 Status Information Availability

Provide, with 99% availability, a secure automated mechanism to allow relying parties to determine credential status and authenticate the subject's identity.

AL4_CM_CSM#050 Inactive Credentials

Disable any credential that has not been successfully used for authentication during a period of 18 months.

3.7.6 Part F - Credential Validation/Authentication

These criteria apply to credential validation and identity authentication.

3.7.6.1 Assurance Level 1

3.7.6.1.1 Assertion Security

An enterprise and its specified service must:

AL1_CM_ASS#010 Validation and Assertion Security

Provide validation of credentials to a Relying Party using a protocol that:

a) requires authentication of the specified service or of the validation source;
b) ensures the integrity of the authentication assertion;
c) protects assertions against manufacture, modification and substitution, and secondary authenticators from manufacture;

and which, specifically:

d) creates assertions which are specific to a single transaction;
e) where assertion references are used, generates a new reference whenever a new assertion is created;
f) when an assertion is provided indirectly, either signs the assertion or sends it via a protected channel, using a strong binding mechanism between the secondary authenticator and the referenced assertion;
g) requires the secondary authenticator to:
    i) be signed when provided directly to Relying Party, or;
    ii) have a minimum of 64 bits of entropy when provision is indirect (i.e. through the credential user).

AL1_CM_ASS#015 No stipulation

AL1_CM_ASS#020 No Post Authentication

Not authenticate credentials that have been revoked.

AL1_CM_ASS#030 Proof of Possession

Use an authentication protocol that requires the claimant to prove possession and control of the authentication token.

AL1_CM_ASS#040 Assertion Lifetime

Generate assertions so as to indicate and effect their expiration within:

a) 12 hours after their creation, where the service shares a common internet domain with the Relying Party;

b) five minutes after their creation, where the service does not share a common internet domain with the Relying Party.

3.7.6.2 Assurance Level 2

3.7.6.2.1 Assertion Security

An enterprise and its specified service must:

AL2_CM_ASS#010 Validation and Assertion Security

Provide validation of credentials to a Relying Party using a protocol that:

a) requires authentication of the specified service, itself, or of the validation source;
b) ensures the integrity of the authentication assertion;
c) protects assertions against manufacture, modification**, substitution and disclosure**, and secondary authenticators from manufacture**, capture and replay**;
d) uses approved cryptography techniques;

and which, specifically:

e) creates assertions which are specific to a single transaction;
f) where assertion references are used, generates a new reference whenever a new assertion is created;
g) when an assertion is provided indirectly, either signs the assertion or sends it via a protected channel, using a strong binding mechanism between the secondary authenticator and the referenced assertion;
h) send assertions either via a channel mutually-authenticated with the Relying Party, or signed and encrypted for the Relying Party;
i) requires the secondary authenticator to:
    i) be signed when provided directly to Relying Party, or;
    ii) have a minimum of 64 bits of entropy when provision is indirect (i.e. through the credential user);
    iii) be transmitted to the Subject through a protected channel which is linked to the primary authentication process in such a way that session hijacking attacks are resisted;
    iv) not be subsequently transmitted over an unprotected channel or to an unauthenticated party while it remains valid.

AL2_CM_ASS#015 No False Authentication

Employ techniques which ensure that system failures do not result in 'false positive authentication' errors.

AL2_CM_ASS#020 No Post Authentication

Not authenticate credentials that have been revoked **unless the time of the transaction for which verification is sought preceeds the time of revocation of the credential**.

3162 AL2_CM_ASS#030 Proof of Possession

3163 Use an authentication protocol that requires the claimant to prove possession and control
3164 of the authentication token.

3165 AL2_CM_ASS#040 Assertion Lifetime

3166 Generate assertions so as to indicate and effect their expiration:

3167 a) 12 hours after their creation, where the service shares a common internet domain
3168 with the Relying Party;

3169 b) five minutes after their creation, where the service does not share a common
3170 internet domain with the Relying Party.

3171

3172

3.7.6.3 Assurance Level 3

3.7.6.3.1 Assertion Security

An enterprise and its specified service must:

AL3_CM_ASS#010 Validation and Assertion Security

Provide validation of credentials to a Relying Party using a protocol that:

a) requires authentication of the specified service, itself, or of the validation source;
b) ensures the integrity of the authentication assertion.

AL3_CM_ASS#015 No False Authentication

Employ techniques which ensure that system failures do not result in 'false positive authentication' errors.

AL3_CM_ASS#020 Post Authentication

Not authenticate credentials that have been revoked unless the time of the transaction for which verification is sought preceeds the time of revocation of the credential.

AL3_CM_ASS#030 Proof of Possession

Use an authentication protocol that requires the claimant to prove possession and control of the authentication token.

AL3_CM_ASS#040 Assertion Lifetime

For non-cryptographic credentials, generate assertions so as to indicate and effect their expiration 12 hours after their creation**; otherwise, notify the relying party of how often the revocation status sources are updated**.

3.7.6.4 Assurance Level 4

3.7.6.4.1 Assertion Security

An enterprise and its specified service must:

AL4_CM_ASS#010 Validation and Assertion Security

Provide validation of credentials to a Relying Party using a protocol that:

a) requires authentication of the specified service, itself, or of the validation source;
b) ensures the integrity of the authentication assertion.

AL4_CM_ASS#015 No False Authentication

Employ techniques which ensure that system failures do not result in 'false positive authentication' errors.

AL4_CM_ASS#020 Post Authentication

Not authenticate credentials that have been revoked unless the time of the transaction for which verification is sought preceeds the time of revocation of the credential.

AL4_CM_ASS#030 Proof of Possession

Use an authentication protocol that requires the claimant to prove possession and control of the authentication token.

AL4_CM_ASS#040 Assertion Lifetime

[Omitted] Notify the relying party of how often the revocation status sources are updated.

3.7.7 Compliance Tables

Use the following tables to correlate criteria for a particular Assurance Level (AL) and the evidence offered to support compliance.

Service providers preparing for an assessment can use the table appropriate to the AL at which they are seeking approval to correlate evidence with criteria or to justify non-applicability (e.g., "specific service types not offered").

Assessors can use the tables to record the steps in their assessment and their determination of compliance or failure.

Table 3-9 CM-SAC - AL1 Compliance

Clause	Description	Compliance
Part A – Credential Operating Environment		
AL1_CM_CTR#010	No stipulation	No conformity requirement
AL1_CM_CTR#020	Protocol threat risk assessment and controls	
AL1_CM_CTR#025	No stipulation	No conformity requirement
AL1_CM_CTR#030	System threat risk assessment and controls	
AL1_CM_STS#010	Withdrawn	No conformity requirement
AL1_CM_OPN#010	Changeable PIN/Password	
Part B – Credential Issuing		
AL1_CM_IDP#010	Self-managed Identity Proofing	
AL1_CM_IDP#020	Kantara-Recognized outsourced service	
AL1_CM_IDP#030	Non-recognized outsourced service	
AL1_CM_IDP#040	Revision to subscriber information	
AL1_CM_CRN#010	Authenticated Request	
AL1_CM_CRN#020	No stipulation	No conformity requirement
AL1_CM_CRN#030	Credential uniqueness	
Part C – Credential Renewal and Re-issuing		
AL1_CM_RNR#010	Changeable PIN/Password	
Part D – Credential Revocation		
AL1_CM_SRR#010	Submit Request	
Part E – Credential Status Management		
AL1_CM_CSM#010	Maintain Status Record	
AL1_CM_CSM#020	No stipulation	No conformity requirement
AL1_CM_CSM#030	No stipulation	No conformity requirement

AL1_CM_CSM#040	Status Information Availability	
Part F – Credential Validation / Authentication		
AL1_CM_ASS#010	Validation and Assertion Security	
AL1_CM_ASS#015	No stipulation	No conformity requirement
AL1_CM_ASS#020	No Post Authentication	
AL1_CM_ASS#030	Proof of Possession	
AL1_CM_ASS#040	Assertion Lifetime	

3225

3226

3227 **Table 3-10 CM-SAC - AL2 Compliance**

Clause	Description	Compliance
Part A - Credential Operating Environment		
AL2_CM_CPP#010	Credential Policy and Practice Statement	
AL2_CM_CPP#020	No stipulation	No conformity requirement
AL2_CM_CPP#030	Management Authority	
AL2_CM_CTR#010	Withdrawn	No conformity requirement
AL2_CM_CTR#020	Protocol threat risk assessment and controls	
AL2_CM_CTR#025	Permitted authentication protocols	
AL2_CM_CTR#028	One-time passwords	
AL2_CM_CTR#030	System threat risk assessment and controls	
AL2_CM_CTR#040	Specified Service's Key Management	
AL2_CM_STS#010	Withdrawn	No conformity requirement
AL2_CM_OPN#010	Withdrawn	No conformity requirement
Part B – Credential Issuing		
AL2_CM_IDP#010	Self-managed identity proofing	
AL2_CM_IDP#020	Kantara-Recognized outsourced service	
AL2_CM_IDP#030	Non- Kantara-Recognized outsourced service	
AL2_CM_IDP#040	Revision to subscriber information	
AL2_CM_CRN#010	Authenticated Request	
AL2_CM_CRN#020	Unique identity	
AL2_CM_CRN#030	Credential uniqueness	
AL2_CM_CRN#035	Convey credential	
AL2_CM_CRN#040	Password strength	
AL2_CM_CRN#050	One-time password strength	
AL2_CM_CRN#060	Software cryptographic token strength	
AL2_CM_CRN#070	Hardware token strength	
AL2_CM_CRN#080	No stipulation	No conformity requirement
AL2_CM_CRN#090	Nature of subject	
AL2_CM_CRD#010	Notify Subject of Credential Issuance	
AL2_CM_CRD#015	Confirm Applicant's identity (in person)	
AL2_CM_CRD#016	Confirm Applicant's identity (remotely)	
Part C – Credential Renewal and Re-issuing		

AL2_CM_RNR#010	Changeable PIN/Password	
AL2_CM_RNR#020	Proof-of-possession on Renewal/Re-issuance	
AL2_CM_RNR#030	Renewal/Re-issuance limitations	
Part D – Credential Revocation		
AL2_CM_RVP#010	Revocation procedures	
AL2_CM_ RVP#020	Secure status notification	
AL2_CM_ RVP#030	Revocation publication	
AL2_CM_RVP#040	Verify revocation identity	
AL2_CM_RVP#050	Revocation Records	
AL2_CM_RVP#060	Record Retention	
AL2_CM_RVR#010	Verify revocation identity	
AL2_CM_RVR#020	Revocation reason	
AL2_CM_RVR#030	Verify Subscriber as Revocant	
AL2_CM_RVR#040	CSP as Revocant	
AL2_CM_RVR#050	Verify Legal Representative as Revocant	
AL2_CM_SRR#010	Submit Request	
Part E – Credential Status Management		
AL2_CM_CSM#010	Maintain Status Record	
AL2_CM_CSM#020	Validation of Status Change Requests	
AL2_CM_CSM#030	Revision to Published Status	
AL2_CM_CSM#040	Status Information Availability	
AL2_CM_CSM#050	Inactive Credentials	
Part F – Credential Validation / Authentication		
AL2_CM_ASS#010	Validation and Assertion Security	
AL2_CM_ASS#015	No False Authentication	
AL2_CM_ASS#020	No Post Authentication	
AL2_CM_ASS#030	Proof of Possession	
AL2_CM_ASS#040	Assertion Lifetime	

3228

3229

3230 **Table 3-11 CM-SAC - AL3 Compliance**

Clause	Description	Compliance
Part A – Credential Operating Environment		
AL3_CM_CPP#010	Credential Policy and Practice Statement	
AL3_CM_CPP#020	No stipulation	No conformity requirement
AL3_CM_CPP#030	Management Authority	
AL3_CM_CTR#010	No stipulation	No conformity requirement
AL3_CM_CTR#020	Protocol threat risk assessment and controls	
AL3_CM_CTR#025	Permitted authentication protocols	
AL3_CM_CTR#030	System threat risk assessment and controls	
AL3_CM_CTR#040	Specified Service's Key Management	
AL3_CM_STS#010	Withdrawn	No conformity requirement
AL3_CM_STS#020	Stored Secret Encryption	
AL3_CM_SER#010	Security event logs	
AL3_CM_OPN#010	Changeable PIN/Password	
Part B – Credential Issuing		
AL3_CM_IDP#010	Self-managed Identity Proofing	
AL3_CM_IDP#020	Kantara-Recognized outsourced service	
AL3_CM_IDP#030	Non- Kantara-Recognized outsourced service	
AL3_CM_IDP#040	Revision to subscriber information	
AL3_CM_CRN#010	Authenticated Request	
AL3_CM_CRN#020	Unique identity	
AL3_CM_CRN#030	Credential uniqueness	
AL3_CM_CRN#035	Convey credential	
AL3_CM_CRN#040	PIN/Password strength	
AL3_CM_CRN#050	One-time password strength	
AL3_CM_CRN#060	Software cryptographic token strength	
AL3_CM_CRN#070	Hardware token strength	
AL3_CM_CRN#080	Binding of key	
AL3_CM_CRN#090	Nature of subject	
AL3_CM_SKP#010	Key generation by Specified Service	
AL3_CM_SKP#020	Key generation by Subject	
AL3_CM_CRD#010	Notify Subject of Credential Issuance	

AL3_CM_CRD#020	Subject's acknowledgement	
Part C – Credential Renewal and Re-issuing		
AL3_CM_RNR#010	Changeable PIN/Password	
Part D – Credential Revocation		
AL3_CM_RVP#010	Revocation procedures	
AL3_CM_ RVP#020	Secure status notification	
AL3_CM_ RVP#030	Revocation publication	
AL3_CM_RVP#040	Verify Revocation Identity	
AL3_CM_RVP#050	Revocation Records	
AL3_CM_RVP#060	Record Retention	
AL3_CM_RVR#010	Verify revocation identity	
AL3_CM_RVR#020	Revocation reason	
AL3_CM_RVR#030	Verify Subscriber as Revocant	
AL3_CM_RVR#040	Verify CSP as Revocant	
AL3_CM_RVR#050	Verify Legal Representative as Revocant	
AL3_CM_SRR#010	Submit Request	
Part E – Credential Status Management		
AL3_CM_CSM#010	Maintain Status Record	
AL3_CM_CSM#020	Validation of Status Change Requests	
AL3_CM_CSM#030	Revision to Published Status	
AL3_CM_CSM#040	Status Information Availability	
AL3_CM_CSM#050	Inactive Credentials	
Part F – Credential Validation / Authentication		
AL3_CM_ASS#010	Validation and Assertion Security	
AL3_CM_ASS#015	No False Authentication	
AL3_CM_ASS#020	Post Authentication	
AL3_CM_ASS#030	Proof of Possession	
AL3_CM_ASS#040	Assertion Lifetime	

3231

3232 **Table 3-12 CM-SAC - AL4 Compliance**

Clause	Description	Compliance
Part A - Credential Operating Environment		
AL4_CM_CPP#010	No stipulation	No conformity requirement
AL4_CM_CPP#020	Certificate Policy/Certification Practice Statement	
AL4_CM_CPP#030	Management Authority	
AL4_CM_CTR#010	No stipulation	No conformity requirement
AL4_CM_CTR#020	Protocol threat risk assessment and controls	
AL4_CM_CTR#025	No stipulation	No conformity requirement
AL4_CM_CTR#030	System threat risk assessment and controls	
AL4_CM_CTR#040	Specified Service's Key Management	
AL4_CM_STS#010	Stored Secrets	
AL4_CM_STS#020	Stored Secret Encryption	
AL4_CM_SER#010	Security event logs	
AL4_CM_OPN#010	Withdrawn	No conformity requirement
Part B – Credential Issuing		
AL4_CM_IDP#010	Self-managed Identity Proofing	
AL4_CM_IDP#020	Kantara-Recognized outsourced service	
AL4_CM_IDP#030	Non- Kantara-Recognized outsourced service	
AL4_CM_IDP#040	Revision to subscriber information	
AL4_CM_CRN#010	Authenticated Request	
AL4_CM_CRN#020	Unique identity	
AL4_CM_CRN#030	Credential uniqueness	
AL4_CM_CRN#035	Convey credential	
AL4_CM_CRN#040	PIN/Password strength	
AL4_CM_CRN#050	One-time password strength	
AL4_CM_CRN#060	Software cryptographic token strength	
AL4_CM_CRN#070	Hardware token strength	
AL4_CM_CRN#080	Binding of key	
AL4_CM_CRN#090	Nature of subject	
AL4_CM_SKP#010	Key generation by Specified Service	
AL4_CM_SKP#020	Key generation by Subject	
AL4_CM_CRD#010	Notify Subject of Credential Issuance	

AL4_CM_CRD#020	Subject's acknowledgement	
Part C – Credential Renewal and Re-issuing		
AL4_CM_RNR#010	Changeable PIN/Password	
Part D – Credential Revocation		
AL4_CM_RVP#010	Revocation procedures	
AL4_CM_ RVP#020	Secure status notification	
AL4_CM_ RVP#030	Revocation publication	
AL4_CM_RVP#040	No stipulation	No conformity requirement
AL4_CM_RVP#050	Revocation Records	
AL4_CM_RVP#060	Record Retention	
AL4_CM_RVR#010	Verify revocation identity	
AL4_CM_RVR#020	Revocation reason	
AL4_CM_RVR#030	Verify Subscriber as Revocant	
AL4_CM_RVR#040	Verify CSP as Revocant	
AL4_CM_RVR#050	Verify Legal Representative as Revocant	
AL4_CM_RKY#010	Verify Requestor as Subscriber	
AL4_CM_RKY#020	Re-key requests other than subscriber	
AL4_CM_SRR#010	Submit Request	
Part E – Credential Status Management		
AL4_CM_CSM#010	Maintain Status Record	
AL4_CM_CSM#020	Validation of Status Change Requests	
AL4_CM_CSM#030	Revision to Published Status	
AL4_CM_CSM#040	Status Information Availability	
AL4_CM_CSM#050	Inactive Credentials	
Part F – Credential Validation / Authentication		
AL4_CM_ASS#010	Validation and Assertion Security	
AL4_CM_ASS#015	No False Authentication	
AL4_CM_ASS#020	Post Authentication	
AL4_CM_ASS#030	Proof of Possession	
AL4_CM_ASS#040	Assertion Lifetime	

3233

4 REFERENCES

[CAF] Louden, Chris, Spencer, Judy, Burr, Bill, Hawkins, Kevin, Temoshok, David, Cornell, John, Wilsher, Richard G., Timchak, Steve, Sill, Stephen, Silver, Dave, Harrison, Von, eds., "E-Authentication Credential Assessment Framework (CAF)," E-Authentication Initiative, Version 2.0.0 (March 16, 2005). http://www.cio.gov/eauthentication/documents/CAF.pdf

[EAP CSAC 04011] "EAP working paper: Identity Proofing Service Assessment Criteria (ID-SAC)," Electronic Authentication Partnership, Draft 0.1.3 (July 20, 2004) http://eap.projectliberty.org/docs/Jul2004/EAP_CSAC_04011_0-1-3_ID-SAC.doc

[EAPTrustFramework] "Electronic Authentication Partnership Trust Framework" Electronic Authentication Partnership, Version 1.0. (January 6, 2005) http://eap.projectliberty.org/docs/Trust_Framework_010605_final.pdf

[FIPS140-2] "Security Requirements for Cryptographic Modules" Federal Information Processing Standards. (May 25, 2001) http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

[IS27001] ISO/IEC 27001:2005 "Information technology - Security techniques - Requirements for information security management systems" International Organization for Standardization. http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103

[M-04-04] Bolton, Joshua B., eds., "E-Authentication Guidance for Federal Agencies," Office of Management and Budget, (December 16, 2003). http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf

[NIST800-63] Burr, William E., Dodson, Donna F., Polk, W. Timothy, eds., "Electronic Authentication Guideline: : Recommendations of the National Institute of Standards and Technology," Version 1.0.2, National Institute of Standards and Technology, (April, 2006). http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

[RFC 3647] Chokhani, S., Ford, W., Sabett, R., Merrill, C., Wu, S., eds., "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework," The Internet Engineering Task Force (November, 2003). http://www.ietf.org/rfc/rfc3647.txt