Identity Assurance Framework:
Service Assessment Criteria

Version: 4.0*bis*

Date: 2014-05-12

Status: Final Recommendation

Approval: KIR20140512

Editor: Richard G. Wilsher
Zygma LLC

Contributors: https://kantarainitiative.org/confluence/x/k4PEAw

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 set of documents 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 these *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 latest versions of each of these documents can be found on Kantara's Identity Assurance Framework - General Information web page.

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.

Contents

1 INTRODUCTION

Kantara Initiative formed the Identity Assurance Work Group (IAWG) to foster adoption of consistently managed identity trust services. 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 specifies 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. It 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 supported by *Rules governing Assurance Assessments (RAA)*, which encompasses the associated assessment and certification program, as well as several subordinate documents. The present document, subordinate to the AAS, describes the Service Assessment Criteria component of the IAF.

The latest versions of each of these documents can be found on Kantara's Identity Assurance Framework - General Information web page.

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.

1.1 Changes in this revision

The principal reason for changes in this revision is to capture results of a mapping between version 3.0 of the SAC and NIST SP 800-63-2. Historically, AL1 and AL2 were aligned against SP 800-63-1 but no formalized mapping had been conducted at ALs 3 & 4.

Additionally, the mapping between v2.0 and v3.0 found in §8 of v3.0 has been removed – at the time of formal publication of the revisions in the present version of the document SAC v3.0 had been published for over twelve months.

In the course of these revisions the opportunity has been taken to perform incidental tidy-up where the originally-drafted language no longer reflects practice or terminology.

Excepting where text has been moved within the document and is otherwise unchanged, all revisions between v3.0 and v4.0 are shown with a grey background.

Additionally, the Compliance Tables now indicate the revision status for each criterion (italicized and right-justified), indicating whether it has:

i) been introduced as a NEW requirement;

ii) had its requirement AMENDED in any way;

iii) had merely an EDITorial change (i.e. no change to the requirement);

iv) been supplemented with GUIDANCE;

v) been RE-NUMBERED;

or any combination of the above. If a criterion has not changed, nothing is indicated

A reference to the formal approval ballot results has been included on the cover page (*bis* release).

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 *Identity Assurance Framework: Levels of Assurance* document, which can be found on Kantara's Identity Assurance Framework - General Information page.

3 SERVICE ASSESSMENT CRITERIA - GENERAL

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, at each Assurance Level (AL), against which Services must be assessed by Kantara-Accredited Assessors. They are divided into two parts:

1) **Organizational Criteria**:
These criteria address the general business and organizational conformity of services and their providers. They are generally referred-to as the 'CO-SAC';

2) **Operational Criteria**:
These criteria address operational conformity of credential management services and the necessary functions which they embrace. They are generally referred-to as the 'OP-SAC'.

3.2 Criteria Applicability

All criteria (i.e. CO-SAC and OP-SAC, at the applicable level) must be complied-with by all Full Service Provisions that are submitted for Approval under the Identity Assurance Framework (IAF).

Each Service Component within a Full Service Provision must comply with the CO-SAC and a defined sub-set of OP-SAC clauses which fall within the component's scope.

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 credentialing services for which a CSP is seeking Kantara Approval.

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

This document describes the specific criteria that must be met to achieve each of the four ALs under the IAF. To be Approved under the IAF Identity Assurance Program and be granted the right to use Kantara Initiative Trust Mark, credential services must conform to all applicable criteria at the appropriate level.

3.3 Status and Readership

This document sets out **normative** Kantara requirements and is required reading for Kantara-Accredited Assessors and applicant Service Providers. It will also be of interest to those wishing to gain a detailed knowledge of the workings of the Kantara Initiative's Identity Assurance Framework. It sets out the Service Assessment Criteria to which credential services must conform in order to be granted Kantara Approval.

The description of criteria in this document is required reading for all organizations wishing to become Kantara-Approved credential services, 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.

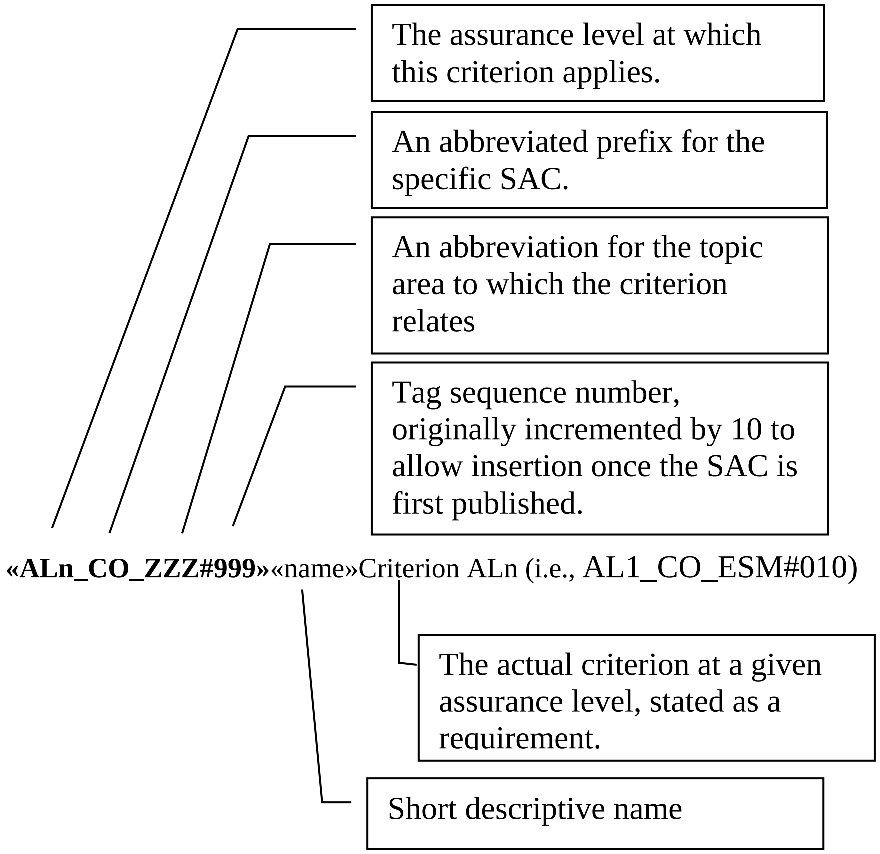
This document will also be of interest to those seeking a detailed understanding of the operation of the Identity Assurance Framework but who are not actively involved in its operations or in services that may fall within the scope of the Framework.

3.4 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:


The assurance level at which this criterion applies.
An abbreviated prefix for the specific SAC.
An abbreviation for the topic area to which the criterion relates
Tag sequence number, originally incremented by 10 to allow insertion once the SAC is first published.
«ALn_CO_ZZZ#999»«name»Criterion ALn (i.e., AL1_CO_ESM#010)
The actual criterion at a given assurance level, stated as a requirement.
Short descriptive name

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.

3.5 Terminology

All special terms used in this document are defined in the *IAF Glossary*, which can be found on Kantara's Identity Assurance Framework - General Information page.

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.

4 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 Assurance Levels (AL) – refer to Section 2. These criteria are generally referred to elsewhere within IAWG documentation as CO-SAC and can be identified by their tag "ALn_CO_ xxxx".

These criteria must be conformed-to by all applicants for Approval, whether for Service Components or Full Service Provision.

4.1 Assurance Level 1

4.1.1 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 Withdrawn
Withdrawn

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 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 Subjects’ private information (against unlawful or unauthorized access, excepting that permitted by the information owner or required by due process).

AL1_CO_ESM#055 Termination provisions
Define the practices in place for the protection of Subjects' private and secret information related to their use of the service which must ensure the ongoing secure preservation and protection of legally required records and for the secure destruction and disposal of any such information whose retention is no longer legally required. Specific details of these practices must be made available.

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.

4.1.2 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).

4.1.3 No stipulation

4.1.4 No stipulation

4.1.5 No stipulation

4.1.6 No stipulation

4.1.7 Secure Communications

AL1_CO_SCO#010 No stipulation

AL1_CO_SCO#015 No stipulation

AL1_CO_SCO#016 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.

4.2 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.

4.2.1 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 Withdrawn
Withdrawn

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 Subjects' 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 Subject, 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 Subjects' private and secret information related to their use of the service which must ensure the ongoing secure preservation and protection of legally required records and for the secure destruction and disposal of any such information whose retention is no longer legally required. Specific details of these practices must be made available.

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.

4.2.2 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, Renewal/Re-issuance, 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 each class of user of the service, e.g. Relying Parties, Subscribers and Subjects;**
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 Subscribers, 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#025 AL2 Configuration Specification

Make available a detailed specification (accounting for the service specification and architecture) which defines how a user of the service can configure it so as to be assured of receiving at least an AL2 baseline service.

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.

4.2.3 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 subjected to a first-party audit at least once every 12 months for the effective provision of the specified service by 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.

Guidance: ‘First-party’ audits are those undertaken by an independent part of the same organization which offers the service. The auditors cannot be involved in the specification, development or operation of the service.
Using a ‘third-party’ (i.e. independent) auditor (i.e. one having no relationship with the Service Provider nor any vested interests in the outcome of the assessment other than their professional obligations to perform the assessment objectively and independently) should be considered when the organization cannot easily provide truly independent internal resources but wishes to benefit from the value which audits can provide, and for the purposes of fulfilling Kantara’s needs, a formal Kantara Assessment performed by an Accredited Assessor should be considered as such.

AL2_CO_ISM#090 Withdrawn

Withdrawn.

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 or Subject, 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 Withdrawn

Withdrawn.

4.2.4 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 authenticable.

4.2.5 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;

c) a minimum of two persons is required to enable access to 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.

4.2.6 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.

4.2.7 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 it services, or parties requiring access to the CSP's services, each transaction must be cryptographically protected using an encryption method approved by a national technical authority or other generally-recognized authoritative body, by either:

a) implementing mutually-authenticated protected sessions; or

b) time-stamped or sequenced messages signed by their source and encrypted for their recipient.

Guidance: The reference to "parties requiring access to the CSP's services" is intended to cover SP 800-63-2's reference to RPs (see cross-mapped EZP 63-2 clause).

AL2_CO_SCO#015 Verification / Authentication confirmation messages
Ensure that any verification or confirmation of authentication messages, which assert either that a weakly bound credential is valid or that a strongly bound credential has not been subsequently revoked, are 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 Withdrawn
Now AL2_CM_RVP#045

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 Subject or to the CSP's direct agents (bearing in mind (a) above).

In addition, 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:

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

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

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

4.3 Assurance Level 3

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

4.3.1 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 Withdrawn
Withdrawn

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 Subjects' private and secret information related to their use of the service which must ensure the ongoing secure preservation and protection of legally required records and for the secure destruction and disposal of any such information whose retention is no longer legally required. Specific details of these practices must be made available.

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.

4.3.2 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, Renewal/Re-issuance, 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 each class of user of the service, e.g. Relying Parties, Subscribers and Subjects, ...;
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#025 AL3 Configuration Specification

Make available a detailed specification (accounting for the service specification and architecture) which defines how a user of the service can configure it so as to be assured of receiving at least an **AL3** baseline service.

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.

4.3.3 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 CobIT or [IS27001] practices**.

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 subjected to a first-party audit at least once every 12 months for the effective provision of the specified service by 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.

Guidance: ‘First-party’ audits are those undertaken by an independent part of the same organization which offers the service. The auditors cannot be involved in the specification, development or operation of the service.

Management systems require that there be internal audit conducted as an inherent part of management review processes. Any third-party (i.e. independent) audit of the management system is intended to show that the internal management system controls are being appropriately applied, and for the purposes of fulfilling Kantara's needs, a formal Kantara Assessment performed by an Accredited Assessor should be considered as such.

AL3_CO_ISM#090 Withdrawn
Withdrawn.

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 or Subject, 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 Withdrawn
Withdrawn.

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.

Guidance: The auditors determining that this ISMS meets the above requirement must be appropriately qualified in assessing the specific management system or methodology applied.

4.3.4 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.

4.3.5 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) a minimum of two persons are required to enable access to any cryptographic modules;
d) 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.

4.3.6 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.

4.3.7 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, or parties requiring access to the CSP's services, each transaction must be cryptographically protected using an encryption method approved by a recognized national technical authority or other generally-recognized authoritative body, by either:
a) implementing mutually-authenticated protected sessions; or
b) time-stamped or sequenced messages signed by their source and encrypted for their recipient.

Guidance: The reference to “parties requiring access to the CSP’s services” is intended to cover SP 800-63-2’s reference to RPs (see cross-mapped EZP 63-2 clause).

AL3_CO_SCO#015 Verification / Authentication confirmation messages

Ensure that any verification or confirmation of authentication messages, which assert 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.

AL3_CO_SCO#016 Withdrawn

AL3_CO_SCO#020 Limited access to shared secrets

Ensure that:

a) access to shared secrets shall be subject to discretionary controls that permit access to those roles/applications requiring 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 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, and decrypted only as immediately required for an authentication operation;

ii they are protected as a key within the boundary of either a FIPS 140-2 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, and are not exported from the module in plaintext;

iii Omitted;

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

These roles should be defined and documented by the CSP in accordance with AL3_CO_OPN#020 above.

4.4 Assurance Level 4

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

4.4.1 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 Withdrawn
Withdrawn

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).

AL4_CO_ESM#055 Termination provisions
Define the practices in place for the protection of Subjects' private and secret information related to their use of the service which must ensure the ongoing secure preservation and protection of legally required records and for the secure destruction and disposal of any such information whose retention is no longer legally required. Specific details of these practices must be made available.

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.

4.4.2 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, Renewal/Re-issuance, 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 and Subject;
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#025 AL4 Configuration Specification

Make available a detailed specification (accounting for the service specification and architecture) which defines how a user of the service can configure it so as to be assured of receiving at least an **AL4** baseline service.

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.

4.4.3 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 CobIT 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 subjected to a first-party audit at least once every 12 months for the effective provision of the specified service by 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.

Guidance: 'First-party' audits are those undertaken by an independent part of the same organization which offers the service. The auditors cannot be involved in the specification, development or operation of the service.

Management systems require that there be internal audit conducted as an inherent part of management review processes. Any third-party (i.e. independent) audit of the management system is intended to show that the internal management system controls are being appropriately applied, and for the purposes of fulfilling Kantara's needs, a formal Kantara Assessment performed by an Accredited Assessor should be considered as such.

AL4_CO_ISM#090 Withdrawn
Withdrawn.

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 or Subject, 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 Withdrawn
Withdrawn.

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.

4.4.4 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.

4.4.5 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) a minimum of two persons are required to enable access to any cryptographic modules;
d) 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.

4.4.6 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.

4.4.7 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, or parties requiring access to the CSP's services, each transaction must be cryptographically protected using an encryption method approved by a recognized national technical authority or other generally-recognized authoritative body, by either:
a) implementing mutually-authenticated protected sessions; or
b) time-stamped or sequenced messages signed by their source and encrypted for their recipient.

Guidance: The reference to “parties requiring access to the CSP’s services” is intended to cover SP 800-63-2’s reference to RPs (see cross-mapped EZP 63-2 clause).

AL4_CO_SCO#015 Verification / Authentication confirmation messages
Ensure that any verification or confirmation of authentication messages, which assert 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.

AL4_CO_SCO#016 No stipulation

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 from the module in plaintext;
   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 Subject and the CSP's direct agents (bearing in mind (a) above).

These roles should be defined and documented by the CSP in accordance with AL4_CO_OPN#020 above.

4.5 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.

These tables also provide an overview of any revisions made to criteria in comparison to v3.0 of this document (see §1.1).

Table 3-1. CO-SAC - AL1 Compliance

Clause	Description	Compliance
AL1_CO_ESM#010	Established enterprise	
AL1_CO_ESM#020	Withdrawn	No conformity requirement
AL1_CO_ESM#030	Legal & Contractual compliance	
AL1_CO_ESM#040	No stipulation	
AL1_CO_ESM#050	Data Retention and Protection	*New*
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#010	No stipulation	No conformity requirement
AL1_CO_SCO#015	No stipulation	No conformity requirement
AL1_CO_SCO#016	No stipulation	No conformity requirement
AL1_CO_SCO#020	Limited access to shared secrets	*Editorial*

1358 **Table 3-2.** CO-SAC - AL2 Compliance

Clause	Description	Compliance
AL2_CO_ESM#010	Established enterprise	
AL2_CO_ESM#020	Data Retention and Protection	*Added*
AL2_CO_ESM#030	Legal & Contractual compliance	
AL2_CO_ESM#040	Financial Provisions	
AL2_CO_ESM#050	Data Retention and Protection	*Editorial*
AL2_CO_ESM#055	Termination provisions	
AL2_CO_NUI#010	General Service Definition	
AL2_CO_NUI#020	Service Definition inclusions	*Amended*
AL2_CO_NUI#025	AL2 Configuration Specification	*New*
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	*Guidance*
AL2_CO_ISM#090	Withdrawn	No conformity requirement
AL2_CO_ISM#100	Audit Records	
AL2_CO_ISM#110	Withdrawn	No conformity requirement
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	*Amended*

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	*Amended; Guidance*
AL2_CO_SCO#015	Verification / Authentication confirmation messages	*Amended*
AL2_CO_SCO#016	Withdrawn	*Re-numbered as AL2_CM_RVP#045*
AL2_CO_SCO#020	Limited access to shared secrets	*Amended*
AL2_CO_SCO#030	Logical protection of shared secrets	

1361 **Table 3-3.** CO-SAC - AL3 compliance

Clause	Description	Compliance
AL3_CO_ESM#010	Established enterprise	
AL3_CO_ESM#020	Withdrawn	No conformity requirement
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	*Amended*
AL3_CO_NUI#025	AL3 Configuration Specification	*New*
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	*Guidance*
AL3_CO_ISM#090	Withdrawn	No conformity requirement
AL3_CO_ISM#100	Audit Records	
AL3_CO_ISM#110	Withdrawn	No conformity requirement
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	*Amended*
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	*Amended; Guidance*
AL3_CO_SCO#015	Verification / Authentication confirmation messages	*New*
AL3_CO_SCO#016	Withdrawn	*Re-numbered as AL2_CM_RVP#045*
AL3_CO_SCO#020	Limited access to shared secrets	*Amended*

1364 **Table 3-4.** CO-SAC - AL4 compliance

Clause	Description	Compliance
AL4_CO_ESM#010	Established enterprise	
AL4_CO_ESM#020	Withdrawn	No conformity requirement
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	*Editorial*
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	*Amended*
AL4_CO_NUI#025	AL4 Configuration Specification	*New*
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	*Amended*
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	*Guidance*
AL4_CO_ISM#090	Withdrawn	No conformity requirement
AL4_CO_ISM#100	Audit Records	
AL4_CO_ISM#110	Withdrawn	No conformity requirement
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	*Amended*
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	*Amended; Guidance*
AL4_CO_SCO#015	Verification / Authentication confirmation messages	*New*
AL4_CO_SCO#016	No stipulation	No conformity requirement
AL4_CO_SCO#020	Limited access to shared secrets	*Amended*

5 OPERATIONAL SERVICE ASSESSMENT CRITERIA

The Service Assessment Criteria in this section establish requirements for the operational conformity of credential management services and their providers at all Assurance Levels (AL) – refer to Section 2. These criteria are generally referred to elsewhere within IAF documentation as OP-SAC.

Previous editions of this document have these criteria set out in two distinct sections and have used the terms CM-SAC and ID-SAC: the OP-SAC is the combination of those two previous SAC sections, with optimizations necessary for their integration. To ensure backwards compatibility with assessments already performed against previous editions of this document the criteria within the OP-SAC continue to be identified either by a tag “ALn_ID_ xxxx” or “ALn_CM_ xxxx”.

Within each Assurance Level the criteria are divided into six Parts. Each part deals with a specific functional aspect of the overall credential management process, including identity proofing services (see Parts B, at each Assurance Level).

Full Service Provision requires conformity to all of the following operational criteria at the chosen Assurance Level. This may be demonstrated either by the Full Service Provider fulfilling all of these criteria itself or by its service being a composition of Service Components which must, collectively, fulfill all of these criteria, under the overall management of the Full Service Provider. Providers of Service Components may conform to a defined sub-set of these criteria (although, within Part A at each Assurance Level, there is a small number of criteria which are mandatory for Component Services, which are marked as such).

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.

5.1 Assurance Level 1

5.1.1 Part A - Credential Operating Environment

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 Part describe operational implementation specifics

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

The criterion AL1_CM_CTR#030 is marked as **MANDATORY** for all Component Services.

5.1.1.1 Not used

No stipulation.

5.1.1.2 Security Controls

An enterprise and its specified service must:

AL1_CM_CTR#010 Withdrawn

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 there are at least 14 bits of entropy to resist an on-line guessing attack against a selected user/password;
b) message replay.

Guidance: Organizations should consider potential protocol threats identified in other sources, e.g. ISO/IEC 29115:2013 “Information technology -- Security techniques – Entity authentication assurance framework”.

AL1_CM_CTR#025 No stipulation

AL1_CM_CTR#028 No stipulation

AL1_CM_CTR#030 System threat risk assessment and controls
MANDATORY.

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.

Guidance: the risk assessment should address these threats from any perspective in which they might adversely affect the operation of the service, whether they be from within the organization (e.g. in its development environment, the hosting environment) or without (e.g. network attacks, hackers).

5.1.1.3 Storage of Long-term Secrets

AL1_CM_STS#010 Withdrawn
Withdrawn (AL1_CO_SCO#020 (a) & (b) enforce this requirement)

5.1.1.4 No stipulation

5.1.1.5 Subject Options

AL1_CM_OPN#010 Withdrawn
Withdrawn – see AL1_CM_RNR#010.

5.1.2 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 Assurance Level 1.

5.1.2.1 Identity Proofing 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 and its 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.

5.1.2.2 Identity Verification

The enterprise or specific service:

AL1_ID_IDV#000 Identity Proofing classes

a) must 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) must 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) §**Error! Reference source not found.**, "In-Person Public Identity Proofing";

ii) §**Error! Reference source not found.**, "Remote Public Identity Proofing".

5.1.2.3 In-Person Public Identity 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.

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.

5.1.2.4 Remote Public Identity 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 telephone number or email address.

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.

5.1.2.5 No stipulation

5.1.2.6 No stipulation

5.1.2.7 Issuing Derived Credentials

Where the Applicant already possesses recognized original credentials the CSP may choose to accept the verified identity of the Applicant as a substitute for identity proofing, subject to the following specific provisions. All other requirements of Assurance Level 1 identity proofing must also be observed.

AL1_ID_IDC#010 Authenticate Original Credential

Prior to issuing any derived credential the original credential on which the identity-proofing relies must be proven to be in the possession and under the control of the Applicant.

Guidance: This is the equivalent of recording the details of idebtity-proofing documents provided during (e.g.) face-face id-proofing. It is not required that the original credential be issued by a Kantara-Approved CSP.

5.1.2.8 Secondary Identity 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:

a) any reasonably 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);

b) any use of processes and/or technologies which may not fully meet the preceding applicable requirements but which are deemed to be comparable and thus able to support AL1.

5.1.2.9 Identity-proofing Records

AL1_ID_VRC#010 No stipulation
AL1_ID_VRC#020 No stipulation

AL1_ID_VRC#025 Provide Subject Identity Records
If required, provide to qualifying parties a unique identity for each Subscriber and their associated tokens and credentials to the extent permitted by applicable legislation and/or agreed by the Subscriber.

Guidance: the qualifier ‘if required’ is intended to account for circumstances where conditions such as whether a contract or a federation policy permits or is required or jurisdiction / legal injunction demand such provision. A qualifying party is any party to which provision of such info can justified according to circumstance: by contract/policy; with Subject’s agreement; with due authority (Court Order, e.g.). The CSP needs to make the case, according to their service’s characteristics and operating environment**.**

AL1_ID_VRC#030 No stipulation

AL1_CM_IDP#010 Revision to Subject Information
Provide a means for Subjects to amend their stored information after registration.

Guidance: The necessity for re-issuance will be determined by, *inter alia*, policy, the technology and practices in use, the nature of change (e.g. registration data not bound into the credential) and the nature of the proofing processes.

AL1_CM_IDP#020 Authenticate Subject Information Changes
Permit only changes which are supported by appropriate and sufficient authentication of the legitimacy of change according, to its type.

Guidance: The requirement to authenticate the legitimacy of a change will depend upon what is retained by the CSP and what is being changed: whereas a change of address may require less demanding authentication than may a change of name, a change of date-of-birth would be very unlikely and therefore would require substantial supporting authentication.

5.1.2.10 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 Subject to select a credential (e.g., UserID) that is verified to be unique within the specified service's community and assigned uniquely to a single identity Subject.

AL1_CM_CRN#035 Convey credential
Be capable of conveying the unique identity information associated with a credential to Verifiers and Relying Parties.

AL1_CM_CRN#040 Token strength

Ensure that the single-factor token associated with the credential has one of the following set of characteristics:

c) For a memorized secret, apply a rule-set such that there shall be a minimum of 14 bits of entropy in the pin or pass-phrase;

d) For a knowledge-based question, apply a rule-set such that there shall be:

    i) a minimum of 14 bits of entropy in the pin or pass-phrase OR;

    ii) a set of knowledge-based questions created by the user OR;

iii) a set of knowledge-based questions selected by the user from a service-generated list of at least five questions.

Note – null or empty answers in any case above shall not be permitted.

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**Error! Bookmark not defined.**.

5.1.2.11 No stipulation

5.1.2.12 No stipulation

5.1.3 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 Assurance Level 1.

5.1.3.1 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:

AL1_CM_RNR#010 Changeable PIN/Password
Permit Subjects to change their PINs/passwords.

5.1.4 Part D - Credential Revocation

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

An enterprise and its specified service must:

5.1.4.1 No stipulation

5.1.4.2 No stipulation

5.1.4.3 No stipulation

5.1.4.4 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.

5.1.5 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.

5.1.5.1 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 Claimant's identity.

5.1.6 Part F - Credential Verification/Authentication

These criteria apply to credential validation and identity authentication.

5.1.6.1 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#018 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#035 Limit authentication attempts

Limit the number of failed authentication attempts to no more than 100 in any 30-day period.

AL1_CM_ASS#040 Assertion Lifetime
Set assertions to expire such that:

a) those used outside of the internet domain of the Verifier become invalid 5 minutes after their creation; or

b) those used within a single internet domain become invalid 12 hours after their creation (including assertions contained in or referenced by cookies).

5.1.6.2 Authenticator-generated challenges

No stipulation.

5.1.6.3 Multi-factor authentication

No stipulation.

5.1.6.4 Verifier's assertion schema

Note: Since assertions and related schema can be complex and may be modeled directly on the needs and preferences of the participants, the details of such schema fall outside the scope of the SAC's herein, which are expressed observing, insofar as is feasible, a technology-agnostic policy. The following criteria, therefore, are perhaps more open to variable conformity through their final implementation than are others in this document.

These criteria are derived directly from NIST SP 800-63-2 and have been expressed in as generic a manner as they can be.

An enterprise and its specified service must:

AL1_CM_VAS#010 No stipulation
No stipulation**.**

AL1_CM_VAS#020 No stipulation
No stipulation**.**

AL1_CM_VAS#030 Assertion assurance level
Create assertions which, either explicitly or implicitly (using a mutually-agreed mechanism), indicate the assurance level at which the <u>initial</u> authentication of the Subject was made.

AL1_CM_VAS#040 No stipulation
No stipulation.

AL1_CM_VAS#050 No stipulation
No stipulation.

AL1_CM_VAS#060 No assertion manufacture/modification
Ensure that it is impractical to manufacture an assertion or assertion reference by using at least one of the following techniques:

a) Signing the assertion;

b) Encrypting the assertion using a secret key shared with the RP;

c) Creating an assertion reference which has a minimum of 64 bits of entropy;

d) Sending the assertion over a protected channel during a mutually-authenticated session.

AL1_CM_VAS#070 No stipulation

No stipulation.

AL1_CM_VAS#080 Single-use assertions

Limit to a single transaction the use of assertions which do not support proof of ownership.

AL1_CM_VAS#090 Single-use assertion references

Limit to a single transaction the use of assertion references.

AL1_CM_VAS#100 Bind reference to assertion

Provide a strong binding between the assertion reference and the corresponding assertion, based on integrity-protected (or signed) communications over which the Verifier has been authenticated.

5.2 Assurance Level 2

5.2.1 Part A - Credential Operating Environment

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 Part describe operational implementation specifics.

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

The following three criteria are **MANDATORY** for all Services, Full or Component, and are individually marked as such:
AL2_CM_CPP#010, AL2_CM_CPP#030, AL2_CM_CTR#030.

5.2.1.1 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
MANDATORY.

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 Subjects 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 Subject 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
MANDATORY.

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

5.2.1.2 Security Controls

An enterprise and its specified service must:

AL2_CM_CTR#010 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 there are at least 24 bits of entropy to resist an on-line guessing attack against a selected user/password

b) message replay**, showing that it is impractical**;

c) eavesdropping, showing that it is impractical;

d) no stipulation;

e) man-in-the-middle attack;

f) session hijacking.

Guidance: Organizations should consider potential protocol threats identified in other sources, e.g. ISO/IEC 29115:2013 “Information technology -- Security techniques – Entity authentication assurance framework”.

AL2_CM_CTR#025 Authentication protocols

Apply only authentication protocols which, through a comparative risk assessment which takes into account the target Assurance Level, are shown to have resistance to attack at least as strong as that provided by commonly-recognized protocols such as:

a) tunneling;

b) zero knowledge-based;

c) signed SAML [Omitted].

Guidance: Whilst many authentication protocols are well-established and may be mandated or strongly-recommended by specific jurisdictions or sectors (e.g. standards published by national SDOs or applicable to government-specific usage) this criterion gives flexibility to advanced and innovative authentication protocols for which adequate strength can be shown to be provided by the protocol applied with the specific service.

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; or

b) derive the nonce from a date and time, or a counter, which is generated on the device; or

c) have a limited lifetime, in the order of minutes.

AL2_CM_CTR#030 System threat risk assessment and controls

MANDATORY.

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.

Guidance: the risk assessment should address these threats from any perspective in which they might adversely affect the operation of the service, whether they be from within the organization (e.g. in its development environment, the hosting environment) or without (e.g. network attacks, hackers).

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.

5.2.1.3 Storage of Long-term Secrets

AL2_CM_STS#010 Withdrawn

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

5.2.1.4 No stipulation

5.2.1.5 No stipulation

AL2_CM_OPN#010 Withdrawn

Withdrawn – see AL2_CM_RNR#010.

5.2.2 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 Assurance Level 2.

5.2.2.1 Identity Proofing 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 and its 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.

Guidance: Cf. AL2_CM_CRN#020 which expresses a very similar requirement. Although presenting repetition for a single provider, if the identity-proofing functions and credential management functions are provided by separate CSPs, each needs to fulfill this requirement.

AL2_ID_POL#030 Published Proofing Policy
Make available the Identity Proofing Policy under which it verifies the identity of applicants[1] 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.

5.2.2.2 Identity Verification

The enterprise or specific service:

AL2_ID_IDV#000 Identity Proofing classes

[1] 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.

a) must include in its Service Definition <u>at least one</u> 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) must 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) §0, "In-Person Public Identity Verification";

ii) §5.2.2.4, "Remote Public Identity Verification"**;**

iii) §5.2.2.5, "Current Relationship Identity Verification";

iv) §5.2.2.6, "Affiliation Identity Verification";

although, in any of the above cases, the criteria defined in §5.2.2.7 may be substituted for identity proofing where the Applicant already possesses a recognized credential at Level 3 or 4.

AL2_ID_IDV#010 - Identity Verification Measures

For each identity proofing service offered (see above [*i.e. AL2_ID_IDV#000*]) justify the identity verification measures applied by describing how these meet or exceed the requirements of applicable policies, regulations, adopted standards and other relevant conditions in order to maintain a level of rigour consistent with the applicable Assurance Level.

Guidance: Although strict requirements for identity proofing and verification can be defined, a real-world approach must account for instances where there is not 100% certitude. To cope with this CSPs need to have a set of prescribed (through policy – see AL2_ID_POL#030) and applied measures (see AL2_ID_POL#040) which observe policy, identify the measures taken according to the degree of certitude determined by each step in the verification process and what additional measures are taken. The CSP must present a case which shows that their solution is sufficient to ensure that the basic requirements of the applicable AL are met or exceeded.

Note that in each set of proofing service criteria below there are criteria with specific requirements for evidence checks and an additional criterion for 'secondary' checks, all of which have an interplay with these overall requirements to have a policy and practice statement and to demonstrate processes which sustain confidence that AL2 is being achieved.

Even though a CSP may use the services of a component service for the performance of the identity-proofing within its own service, it still needs to ensure that its policy is both justified and upheld. Where another service provider is used appropriate stipulations in contracts should be established, but any internal adherence to (e.g.) 'POL#040 should be determined by the fact that the component service is already Kantara Approved.

5.2.2.3 In-Person Public Identity Proofing

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.

5.2.2.4 Remote Public Identity Proofing

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 [omitted] **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;

e) a telephone service account.

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

f) a name that matches the referenced photo-ID;
g) date of birth and;
h) current address [omitted];
i) for a telephone service account, the demonstrable ability to send or receive messages at the phone number.

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

Perform inspection and analysis of records against the provided identity references with the specified issuing authorities/institutions or through similar databases, according to the inspection rules set by the issuing authorities:

a) the existence of such records with matching name and reference numbers;
b) corroboration of date of birth, current contact information of record, 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;
d) for a telephone service account, confirmation that the phone number is associated in Records with the Applicant's name and address of record and by having the applicant demonstrate that they are able to send or receive messages at the phone number.

Confirm contact information of record by at least one of the following means, ensuring that any secret sent over an unprotected channel shall be reset upon first use and shall be valid for a maximum lifetime of seven days:

e) RA sends notice to an address of record confirmed in the records check and receives a mailed or telephonic reply from applicant;
f) 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;
g) 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.
h) [Omitted]

Additional checks may be performed so as to establish the uniqueness of the claimed identity (see AL2_ID_SCV#010).

Alternative checks may be performed where the enterprise can show that they lead to a comparable degree of certitude (see AL2_ID_SCV#010).

5.2.2.5 Current Relationship Identity Proofing

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[2].

AL2_ID_CRV#020 Evidence checks

Ensure that it has:

a) only issued the shared secret after originally establishing the applicant's identity:
  i) with a degree of rigor equivalent to that required under either the AL2 (or higher) requirements for in-person or remote public verification; or
  ii) by complying with regulatory requirements effective within the applicable jurisdiction which set forth explicit proofing requirements which include a prior in-person appearance by the applicant and are defined as meeting AL2 (or higher) requirements;

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

5.2.2.6 Affiliation Identity Proofing

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 §5.2.2.5, "Current Relationship Verification".

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;

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

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.

5.2.2.7 Identity-proofing based on Recognized Credentials

Where the Applicant already possesses recognized original credentials the CSP may choose to accept the verified identity of the Applicant as a substitute for identity proofing, subject to the following specific provisions. All other requirements of **Assurance Level 2** identity proofing must also be observed.

AL2_ID_IDC#010 Authenticate Original Credential
Prior to issuing any derived credential the original credential on which the identity-proofing relies must be:

a) authenticated by a source trusted by the CSP as being valid and un-revoked;
b) issued at Assurance Level 3 or 4;
c) issued in the same name as that which the Applicant is claiming;
d) proven to be in the possession and under the control of the Applicant.

Guidance: This is the equivalent of recording the details of id documents provided during (e.g.) face-face id-proofing. It is not required that the original credential be issued by a Kantara-Approved CSP.

AL2_ID_IDC#020 Record Original Credential
Record the details of the original credential.

AL2_ID_IDC#030 Issue Derived Credential
Before issuing the derived credential ensure that:

a) for in-person issuance, the claimant is the Applicant;

b) for remote issuance, token activation requires proof of possession of both the derived token and the original Level 3 or Level 4 token.

5.2.2.8 Secondary Identity-proofing

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:

a) any reasonably 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);

b) any use of processes and/or technologies which may not fully meet the preceding applicable requirements but which are deemed to be comparable and thus able to support **AL2**.

5.2.2.9 Identity-proofing Records

The specific service must retain s 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, the date and time of verification and the identity of the registrar (person, or entity if remote or automatic) performing the proofing functions.

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 [omitted].

Guidance: Although there is no specific stipulation as to what should be recorded the list below suggests facts which would typically be captured:

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

AL2_ID_VRC#025 Provide Subject identity records
If required, provide to qualifying parties **records of identity proofing** to the extent permitted by applicable legislation and/or agreed by the Subscriber**.**

Guidance: the qualifier 'if required' is intended to account for circumstances where conditions such as whether a contract or a federation policy permits or is required or jurisdiction / legal injunction demand such provision. A qualifying party is any party to which provision of such info can justified according to circumstance: by contract/policy;

with Subject's agreement; with due authority (Court Order, e.g.). The CSP needs to make the case, according to their service's characteristics and operating environment**.**

AL2_ID_VRC#030 Record Retention
Either retain, securely, the record of the verification process for the duration of the Subject account plus a further period sufficient to allow fulfillment of any period required legally, contractually or by any other form of binding agreement or obligation, or submit same record to a client CSP that has undertaken to retain the record for the requisite period or longer.

AL2_CM_IDP#010 Revision to Subject information
Provide a means for Subjects 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 instigate the re-issuance of the credential when the data being revised are bound into the credential**.

Guidance: The necessity for re-issuance will be determined by, *inter alia*, policy, the technology and practices in use, the nature of change (e.g. registration data not bound into the credential) and the nature of the proofing processes.

AL2_CM_IDP#020 Authenticate Subject Information Changes
Permit only changes which are supported by appropriate and sufficient authentication of the legitimacy of change according, to its type.

Guidance: The requirement to authenticate the legitimacy of a change will depend upon what is retained by the CSP and what is being changed: whereas a change of address may require less demanding authentication than may a change of name, a change of date-of-birth would be very unlikely and therefore would require substantial supporting authentication.

5.2.2.10 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 Subject. 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, 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. Cf. AL2_CM_POL#020 which expresses a very similar requirement. Although presenting repetition for a single provider, if the identity-proofing functions and credential management functions are provided by separate CSPs, each needs to fulfill this requirement.

AL2_CM_CRN#030 Credential uniqueness

Allow the Subject to select a credential (e.g., UserID) that is verified to be unique within the specified service's community and assigned uniquely to a single identity Subject.

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 Token strength

Ensure that the single-factor token associated with the credential has one of the following set of characteristics:

a) For a memorized secret, apply a rule-set such that there shall be a minimum of **24** bits of entropy in the pin or pass-phrase;

b) For a knowledge-based question, apply a rule-set such that there shall be:

   i) a minimum of **20** bits of entropy in the pin or pass-phrase OR;

   ii) a set of knowledge-based questions created by the user OR;

   iii) a set of knowledge-based questions selected by the user from a service-generated list of at least **seven** questions.

   Note – null or empty answers in either case above shall not be permitted.

c) For a look-up token, apply a rule-set such that there shall be a minimum of 20 bits of entropy in the secret phrase(s);

d) For an out-of-band token, ensure that the token is uniquely addressable and supports communication over a channel that is separate from the primary channel for e-authentication;

e) For a one-time-password device, generate one-time passwords using an approved block cipher or hash function to combine a nonce and a symmetric key;

f) Use a cryptographic device validated at FIPS 140-2 Level 1 or higher or equivalent, as established by a recognized national technical authority.

[Omitted]

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 Error! Bookmark not defined.**.**

AL2_CM_CRN#055 One-time password lifetime

Set the minimum valid lifetime for the one-time password to a value commensurate with service usage and in no case greater than fifteen minutes.

AL2_CM_CRN#060 Software cryptographic token strength

Ensure that software cryptographic keys stored on general-purpose devices are protected by a key and cryptographic protocol that are evaluated against FIPS 140-2 [FIPS140-2] Level 1, or equivalent, as established by a recognized national technical authority.

[**Omitted**]

AL2_CM_CRN#070 Hardware token strength

Ensure that hardware tokens used to store cryptographic keys 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.

[**Omitted**]

AL2_CM_CRN#075 No stipulation

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. [Omitted]

AL2_CM_CRN#095 Pseudonym's Real Identity

If the credential is based upon a pseudonym this must be indicated in the credential and a record of the real identity retained.

5.2.2.11 Subject Key Pair Generation

No stipulation.

5.2.2.12 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.

Guidance: The nature of issuance could mean that the Subject is fully aware and therefore no notification is necessary. If any other such circumstances prevailed, the CSP should identify them.

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 transaction (beyond the first transaction or encounter) by either:

(a) using 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, or;

(b) matching a biometric sample against a reference sample 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.

5.2.3 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 Assurance Level 2.

5.2.3.1 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:

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) neither set to default nor re-use any token secrets;

d) 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.

AL2_CM_RNR#040 No stipulation
No stipulation.

AL2_CM_RNR#050 Record Retention
Retain, securely, the record of any renewal/re-issuance process for the duration of the Subscriber's account plus a further period sufficient to allow fulfillment of any period required legally, contractually or by any other form of binding agreement or obligation, or submit same record to a client CSP that has undertaken to retain the record for the requisite period or longer.

5.2.4 Part D - Credential Revocation

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

5.2.4.1 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:

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#045 Notification 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_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, the Subject themselves, someone acting with the Subscriber's or the Subject'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 Subject'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 a period which is the maximum of:

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

b) applicable legislation, regulation, contract or standards.

5.2.4.2 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:

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 or Subject seeks revocation of the Subject's 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 or Subject, supported by a credential at Assurance Level 2 or higher.

AL2_CM_RVR#040 CSP as Revocant

Where a CSP seeks revocation of a Subject'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.**

5.2.4.3 No stipulation

5.2.4.4 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.

5.2.5 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.

5.2.5.1 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 Claimant'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.

5.2.6 Part F - Credential Verification/Authentication

These criteria apply to credential validation and identity authentication.

5.2.6.1 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#013 No Stipulation

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#018 No stipulation

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 precedes the time of revocation of the credential**.

Guidance: The purpose in this criterion is that, if a verification is intended to refer to the status of a credential at a specific historical point in time, e.g. to determine whether the Claimant was entitled to act as a signatory in a specific capacity at the time of the transaction, this may be done. It is implicit in this thinking that both the request and the response indicate the historical nature of the query and response; otherwise the default time is 'now'. If no such service is offered then this criterion may simply be 'Inapplicable', for that reason.

AL2_CM_ASS#030 Proof of Possession

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

AL2_CM_ASS#035 Limit authentication attempts

Unless the token authenticator has at least 64 bits of entropy, limit the number of failed authentication attempts to no more than 100 in any 30-day period.

AL2_CM_ASS#040 Assertion Lifetime

Set assertions to expire such that:

a) those used outside of the internet domain of the Verifier become invalid 5 minutes after their creation; or

b) those used within a single internet domain become invalid 12 hours after their creation (including assertions contained in or referenced by cookies).

5.2.6.2 Authenticator-generated challenges

An enterprise and its specified service must:

AL2_CM_AGC#010 Entropy level
Create authentication secrets to be used during the authentication exchange (i.e. with out-of-band or cryptographic device tokens) with a degree of entropy appropriate to the token type in question.

5.2.6.3 Multi-factor authentication

An enterprise and its specified service must:

AL2_CM_MFA#010 Permitted multi-factor tokens
Require two tokens which, when used in combination within a single authentication exchange, are acknowledged as providing an equivalence of AL2, as determined by a recognized national technical authority.

5.2.6.4 Verifier's assertion schema

Note: Since assertions and related schema can be complex and may be modeled directly on the needs and preferences of the participants, the details of such schema fall outside the scope of the SAC's herein, which are expressed observing, insofar as is feasible, a technology-agnostic policy. The following criteria, therefore, are perhaps more open to variable conformity through their final implementation than are others in this document.

These criteria are derived directly from NIST SP 800-63-2 and have been expressed in as generic a manner as they can be.

Editor's note: I have avoided reference to the RP here – I am concerned as to what the SAC requires services to do, not who might be using their products. SAC do not refer to RPs.

An enterprise and its specified service must:

AL2_CM_VAS#010 Approved cryptography
Apply assertion protocols which use cryptographic techniques approved by a national authority or other generally-recognized authoritative body.

AL2_CM_VAS#020 No stipulation
No stipulation.

AL2_CM_VAS#030 Assertion assurance level

Create assertions which, either explicitly or implicitly (using a mutually-agreed mechanism), indicate the assurance level at which the initial authentication of the Subject was made.

AL2_CM_VAS#040 Notify pseudonyms

Create assertions which indicate whether the Subscriber name in the credential subject to verification is a pseudonym.

AL2_CM_VAS#050 Specify recipient

Create assertions which identify the intended recipient of the verification such that the recipient may validate that it is intended for them.

AL2_CM_VAS#060 No assertion manufacture/modification

Ensure that it is impractical to manufacture an assertion or assertion reference by using at least one of the following techniques:

a) Signing the assertion;
b) Encrypting the assertion using a secret key shared with the RP;
c) Creating an assertion reference which has a minimum of 64 bits of entropy;
d) Sending the assertion over a protected channel during a mutually-authenticated session.

AL2_CM_VAS#070 Assertion protections

Provide protection of assertion-related data such that:

a) both assertions and assertion references are protected against capture and re-use;
b) assertions are also protected against redirection;
[US / EZP800-63-2: §9.3.2.2.2]
c) assertions, assertion references and session cookies used for authentication purposes, including any which are re-directed, are protected against session hijacking, for at least the duration of their validity (see AL2_CM_VAS#110).

AL2_CM_VAS#080 Single-use assertions

Limit to a single transaction the use of assertions which do not support proof of ownership.

AL2_CM_VAS#090 Single-use assertion references

Limit to a single transaction the use of assertion references.

AL2_CM_VAS#100 Bind reference to assertion

Provide a strong binding between the assertion reference and the corresponding assertion, based on integrity-protected (or signed) communications over which the Verifier has been authenticated.

5.3 Assurance Level 3

5.3.1 Part A - Credential Operating Environment

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 Part describe operational implementation specifics.

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.

The following four criteria are **MANDATORY** for all Services, Full or Component, and are individually marked as such:
AL3_CM_CPP#010, AL3_CM_CPP#030, AL3_CM_CTR#030, AL3_CM_SER#010.

5.3.1.1 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
MANDATORY.

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 and/or Subjects 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 or Subject 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
MANDATORY.

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.

5.3.1.2 Security Controls

AL3_CM_CTR#010 Withdrawn

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;
f) session hijacking, 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.

Guidance: Organizations should consider potential protocol threats identified in other sources, e.g. ISO/IEC 29115:2013 “Information technology -- Security techniques – Entity authentication assurance framework”.

AL3_CM_CTR#025 Permitted authentication protocols

For non-PKI credentials, apply only authentication protocols which, through a comparative risk assessment which takes into account the target Assurance Level, are shown to have resistance to attack at least as strong as that provided by commonly-recognized protocols such as:

d) tunneling;
e) zero knowledge-based;
f) signed SAML [Omitted].

AL3_CM_CTR#028 No Stipulation

AL3_CM_CTR#030 System threat risk assessment and controls

MANDATORY.

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.

Guidance: the risk assessment should address these threats from any perspective in which they might adversely affect the operation of the service, whether they be from within the organization (e.g. in its development environment, the hosting environment) or without (e.g. network attacks, hackers).

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.

5.3.1.3 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.

5.3.1.4 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

MANDATORY, to the extent that the sub-items relate to the scope of service.

Ensure that such audit records include:

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

b) generation of the Subject’s keys or the evidence that the Subject was in possession of both parts of their own key-pair;

c) generation of the Subject’s certificate;

d) dissemination of the Subject’s certificate;

e) any revocation or suspension associated with the Subject’s certificate.

5.3.1.5 Subject options

AL3_CM_OPN#010 Changeable PIN/Password

Withdrawn – see AL3_CM_RNR#010.

5.3.2 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 Assurance Level 3.

5.3.2.1 Identity Proofing 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 and its 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.

Guidance: Cf. AL3_CM_CRN#020 which expresses a very similar requirement. Although presenting repetition for a single provider, if the identity-proofing functions and credential management functions are provided by separate CSPs, each needs to fulfill this requirement.

AL3_ID_POL#030 Published Proofing Policy
Make available the Identity Proofing Policy under which it verifies the identity of applicants[3] 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 (IdPPS)**.

5.3.2.2 Identity Proofing

The enterprise or specific service:

AL3_ID_IDV#000 Identity Proofing classes

a) must include in its Service Definition <u>at least one</u> 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;

[3] 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.

c) must 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) §0, "In-Person Public Identity Verification";

ii) §5.3.2.4, "Remote Public Identity Verification";

iii) §5.2.2.5, "Current Relationship Identity Verification";

iv) §5.3.2.6, "Affiliation Identity Verification".

although, in any of the above cases, the criteria defined in §5.**3**.2.7 may be substituted for identity proofing where the Applicant already possesses a recognized credential at **Level 4**

AL3_ID_IDV#010 - Identity Verification Measures

For each identity proofing service offered (see above [*i.e. AL3_IDV#000*]) justify the identity verification measures **described in its IdPPS (see AL3_ID_POL#040)** by describing how these meet or exceed the requirements of applicable policies, regulations, adopted standards and other relevant conditions in order to maintain a level of rigour consistent with the AL**3.**

Guidance: Although strict requirements for identity proofing and verification can be defined, a real-world approach must account for instances where there is not 100% certitude. To cope with this CSPs need to have a set of prescribed (through policy – see AL3_ID_POL#030) and applied measures (see AL3_ID_POL#040) which observe policy, identify the measures taken according to the degree of certitude determined by each step in the verification process and what additional measures are taken. The CSP must present a case which shows that their solution is sufficient to ensure that the basic requirements of the applicable AL are met or exceeded.

Note that in each set of proofing service criteria below there are criteria with specific requirements for evidence checks and an additional criterion for 'secondary' checks, all of which have an interplay with these overall requirements to have a policy and practice statement and to demonstrate processes which sustain confidence that AL3 is being achieved.

Even though a CSP may use the services of a component service for the performance of the identity-proofing within its own service, it still needs to ensure that its policy is both justified and upheld. Where another service provider is used appropriate stipulations in contracts should be established, but any internal adherence to (e.g.) 'POL#040 should be determined by the fact that the component service is already Kantara Approved.

5.3.2.3 In-Person Public Identity Proofing

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.

5.3.2.4 Remote Public Identity Proofing

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 [omitted] 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 [omitted].

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, according to the inspection rules set by the issuing authorities:

a) the existence of such records with matching name and reference numbers;
b) corroboration of date of birth, contact information of record [omitted], 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
d) for a telephone service account, confirmation that the phone number is associated in Records with the Applicant's name and address of record and by having the applicant demonstrate that they are able to send or receive messages at the phone number.

Confirm contact information of record by at least one of the following means, ensuring that any secret sent over an unprotected channel shall be reset upon first use and shall be valid for a maximum lifetime of seven days:

e) RA sends notice to an address of record confirmed in the records check and receives a mailed or telephonic reply from applicant;
f) 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;
g) 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.
h) **[Omitted]**

Additional checks may be performed so as to establish the uniqueness of the claimed identity (see AL3_ID_SCV#010).

Alternative checks may be performed where the enterprise can show that they lead to a comparable degree of certitude (see AL3_ID_SCV#010).

5.3.2.5 Current Relationship Identity Proofing

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:

AL3_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 AL**3** (or higher) entropy requirements[4].

AL3_ID_CRV#020 Evidence checks
Ensure that it has:

a) only issued the shared secret after originally establishing the applicant's identity:
   iii) with a degree of rigor equivalent to that required under either the AL**3** (or higher) requirements for in-person or remote public verification; or
   iv) by complying with regulatory requirements effective within the applicable jurisdiction which set forth explicit proofing requirements which include a prior in-person appearance by the applicant and are defined as meeting AL**3** (or higher) requirements;
b) an ongoing business relationship sufficient to satisfy the enterprise of the applicant's continued personal possession of the shared secret.

5.3.2.6 Affiliation Identity Proofing

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 §**5.3.2.4**, "**Remote Public Identity 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.

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

5.3.2.7 Identity-proofing based on Recognized Credentials

Where the Applicant already possesses recognized original credentials the CSP may choose to accept the verified identity of the Applicant as a substitute for identity proofing, subject to the following specific provisions. All other requirements of Assurance Level 3 identity proofing must also be observed.

AL3_ID_IDC#010 Authenticate Original Credential
Prior to issuing any derived credential the original credential on which the identity-proofing relies must be:

a) authenticated by a source trusted by the CSP as being valid and un-revoked;
b) issued at **Assurance Level 4**;
c) issued in the same name as that which the Applicant is claiming;
d) proven to be in the possession and under the control of the Applicant.

Guidance: This is the equivalent of recording the details of id documents provided during (e.g.) face-face id-proofing. It is not required that the original credential be issued by a Kantara-Approved CSP.

AL3_ID_IDC#020 Record Original Credential
Record the details of the original credential.

AL3_ID_IDC#030 Issue Derived Credential
Before issuing the derived credential ensure that:

a) for in-person issuance, the claimant is the Applicant;

b) for remote issuance, token activation requires proof of possession of both the derived token and the original **Level 4** token.

5.3.2.8 Secondary Identity-proofing

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:

a) any reasonably 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);

b) any use of processes and/or technologies which may not fully meet the preceding applicable requirements but which are deemed to be comparable and thus able to support **AL3**.

5.3.2.9 Identity-proofing 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, the date and time of verification and the identity of the registrar (person, or entity if remote or automatic) performing the proofing functions.

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 [omitted].

Guidance: Although there is no specific stipulation as to what should be recorded the list below suggests facts which would typically be captured:

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

AL3_ID_VRC#025 Provide Subject Identity Records

If required, provide to qualifying parties records of identity proofing to the extent permitted by applicable legislation and/or agreed by the Subscriber.

Guidance: the qualifier 'if required' is intended to account for circumstances where conditions such as whether a contract or a federation policy permits or is required or jurisdiction / legal injunction demand such provision. A qualifying party is any party to which provision of such info can justified according to circumstance: by contract/policy; with Subject's agreement; with due authority (Court Order, e.g.). The CSP needs to make the case, according to their service's characteristics and operating environment**.**

AL3_ID_VRC#030 Record Retention

Either retain, securely, the record of the verification/revocation process for the duration of the Subject account plus a further period sufficient to allow fulfillment of any period required legally, contractually or by any other form of binding agreement or obligation , or submit the same record to a client CSP that has undertaken to retain the record for the requisite period or longer.

AL3_CM_IDP#010 Revision to Subject information
Provide a means for Subjects 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 instigate the re-issuance of the credential when the data being revised are bound into the credential.

Guidance: The necessity for re-issuance will be determined by, *inter alia*, policy, the technology and practices in use, the nature of change (e.g. registration data not bound into the credential) and the nature of the proofing processes.

AL3_CM_IDP#020 Authenticate Subject Information Changes
Permit only changes which are supported by appropriate and sufficient authentication of the legitimacy of change according, to its type.

Guidance: The requirement to authenticate the legitimacy of a change will depend upon what is retained by the CSP and what is being changed: whereas a change of address may require less demanding authentication than may a change of name, a change of date-of-birth would be very unlikely and therefore would require substantial supporting authentication.

5.3.2.10 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 Subject. 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, 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.

Cf. AL3_CM_POL#020 which expresses a very similar requirement. Although presenting repetition for a single provider, if the identity-proofing functions and credential management functions are provided by separate CSPs, each needs to fulfill this requirement.

AL3_CM_CRN#030 Credential uniqueness
Allow the Subject to select a credential (e.g., UserID) that is verified to be unique within the specified service’s community and assigned uniquely to a single identity Subject.

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 Token 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 Subject.

AL3_CM_CRN#055 No stipulation

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 1, or equivalent, as established by a recognized national technical authority;
b) require password or biometric activation by the Subject or employ a password protocol when being used for authentication;

c) erase any unencrypted copy of the authentication key after each 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 Subject or also employ a password when being used for authentication;

c) erase any unencrypted copy of the authentication key after each authentication.

AL3_CM_CRN#075 No stipulation

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.

AL3_CM_CRN#095 No stipulation

No stipulation

5.3.2.11 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.**

5.3.2.12 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.**

Guidance: The nature of issuance could mean that the Subject is fully aware and therefore no notification is necessary. If any other such circumstances prevailed, the CSP should identify them.

AL3_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 transaction (beyond the first transaction or encounter) by either:

(a) using a temporary secret which was established during **the** prior transaction or encounter **(whilst ensuring that such temporary secrets are used only once)**, or sent to the Applicant's phone number, email address, or physical address of record, or;

(b) matching a biometric sample against a reference sample that was recorded during a prior encounter.

AL3_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.

AL3_CM_CRD#017 Protected Issuance of Permanent Secrets (in person)
Only issue permanent secrets if the CSP has loaded the secret itself onto the physical device, which was either:

a) issued in-person to the Applicant, or;

b) delivered in a manner that confirms the address of record.

AL3_CM_CRD#018 Protected Issuance of Permanent Secrets (remotely)
Only issue permanent secrets within a protected session.

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).

5.3.3 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 Assurance Level 3.

5.3.3.1 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**.

AL3_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.

AL3_CM_RNR#030 Renewal/Re-issuance limitations
a) **No stipulation**;

b) **No stipulation**;

c) **No stipulation**;

d) 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.

AL3_CM_RNR#040 No stipulation
No stipulation.

AL3_CM_RNR#050 Record Retention
Retain, securely, the record of any renewal/re-issuance process for the duration of the Subscriber's account plus a further period sufficient to allow fulfillment of any period required legally, contractually or by any other form of binding agreement or obligation, or submit same record to a client CSP that has undertaken to retain the record for the requisite period or longer.

5.3.4 Part D - Credential Revocation

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

5.3.4.1 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:

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 or the Subject themselves, someone acting with the Subscriber's or the Subject'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); [Omitted]
d) the reason for revocation.

AL3_CM_RVP#060 Record Retention
Retain, securely, the record of the revocation process for a period which is the maximum of:

a) the records retention policy required by AL**3**_CM_CPP#010;

b) applicable legislation, regulation, contract or standards.

5.3.4.2 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:

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 ensuring that the Subject of the credential is uniquely identified.

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 or Subject seeks revocation of the Subject's 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 or Subject**,** 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 Subject'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.

5.3.4.3 No stipulation

5.3.4.4 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.

5.3.5 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.

5.3.5.1 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 Claimant'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.

5.3.6 Part F - Credential Verification/Authentication

These criteria apply to credential validation and identity authentication.

5.3.6.1 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;

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.

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#018 Ensure token validity
Ensure that tokens are either still valid or have been issued within the last 24 hours.

Guidance: The 24-hour period allows for the fact that if a freshly-issued credential is then revoked, notice of the revocation may take 24 hours to be publicised (per AL3_CM_RVP#030).

AL3_CM_ASS#020 Post Authentication
Not authenticate credentials that have been revoked unless the time of the transaction for which verification is sought precedes the time of revocation of the credential.

Guidance: The purpose in this criterion is that, if a verification is intended to refer to the status of a credential at a specific historical point in time, e.g. to determine whether the Claimant was entitled to act as a signatory in a specific capacity at the time of the transaction, this may be done. It is implicit in this thinking that both the request and the response indicate the historical nature of the query and response; otherwise the default time is 'now'. If no such service is offered then this criterion may simply be 'Inapplicable', for that reason.

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#035 Limit authentication attempts

Unless the token authenticator has at least 64 bits of entropy, limit the number of failed authentication attempts to no more than 100 in any 30-day period.

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**.

5.3.6.2 Authenticator-generated challenges

An enterprise and its specified service must:

AL3_CM_AGC#010 Entropy level
Create authentication secrets to be used during the authentication exchange (i.e. with out-of-band or cryptographic device tokens) with a degree of entropy appropriate to the token type in question.

5.3.6.3 Multi-factor authentication

An enterprise and its specified service must:

AL3_CM_MFA#010 Permitted multi-factor tokens
Require two tokens which, when used in combination within a single authentication exchange, are acknowledged as providing an equivalence of AL**3**, as determined by a recognized national technical authority.

5.3.6.4 Verifier's assertion schema

Note: Since assertions and related schema can be complex and may be modeled directly on the needs and preferences of the participants, the details of such schema fall outside the scope of the SAC's herein, which are expressed observing, insofar as is feasible, a technology-agnostic policy. The following criteria, therefore, are perhaps more open to variable conformity through their final implementation than are others in this document.

These criteria are derived directly from NIST SP 800-63-2 and have been expressed in as generic a manner as they can be.

Editor's note: I have avoided reference to the RP here – I am concerned as to what the SAC requires services to do, not who might be using their products. SAC do not refer to RPs.

An enterprise and its specified service must:

AL3_CM_VAS#010 Approved cryptography
Apply assertion protocols which use cryptographic techniques approved by a national authority or other generally-recognized authoritative body.

AL3_CM_VAS#020 No stipulation
No stipulation.

AL3_CM_VAS#030 Assertion assurance level
Create assertions which, either explicitly or implicitly (using a mutually-agreed mechanism), indicate the assurance level at which the initial authentication of the Subject was made.

AL3_CM_VAS#040 No pseudonyms
Create assertions which indicate **only verified Subscriber names** in the credential subject to verification.

AL3_CM_VAS#050 Specify recipient
Create assertions which identify the intended recipient of the verification such that the recipient may validate that it is intended for them.

AL3_CM_VAS#060 No assertion manufacture/modification
Ensure that it is impractical to manufacture an assertion or assertion reference by **Signing the assertion and** using at least one of the following techniques:

a) Signing the assertion;

b) Encrypting the assertion using a secret key shared with the RP;

c) Creating an assertion reference which has a minimum of 64 bits of entropy;

d) Sending the assertion over a protected channel during a mutually-authenticated session.

AL3_CM_VAS#070 Assertion protections
Provide protection of assertion-related data such that:

a) both assertions and assertion references are protected against capture and re-use;

b) assertions are also protected against redirection;

c) assertions, assertion references and session cookies used for authentication purposes, including any which are re-directed, are protected against session hijacking, for at least the duration of their validity (see AL3_CM_VAS#110).

AL3_CM_VAS#080 Single-use assertions
Limit to a single transaction the use of assertions which do not support proof of ownership.

AL3_CM_VAS#090 Single-use assertion references
Limit to a single transaction the use of assertion references.

AL3_CM_VAS#100 Bind reference to assertion

Provide a strong binding between the assertion reference and the corresponding assertion, based on integrity-protected (or signed) communications over which the Verifier has been authenticated.

AL3_CM_VAS#110 SSO provisions

If SSO is supported, provide a re-authentication of the Subject so long as:

a) the Subject has been successfully authenticated within the last 12 hours;

b) the Subject continues to be able to demonstrate that they were the party that was previously authenticated;

c) it can be ensured that the Subscriber has not been inactive for more than 30 minutes.

Guidance: The conditional nature of this criterion is dictated by the phrasing used in NIST SP 800-63 which states '*may*'.

5.4 Assurance Level 4

5.4.1 Part A - Credential Operating Environment

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 Part describe operational implementation specifics.

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.

The following four criteria are **MANDATORY** for all Services, Full or Component, and are individually marked as such:
AL4_CM_CPP#020, AL4_CM_CPP#030, AL4_CM_CTR#030, AL4_CM_SER#010.

5.4.1.1 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
MANDATORY.

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 Subjects 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 Subject must take to terminate their subscription.

AL4_CM_CPP#030 Management Authority
MANDATORY.

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.

AL4_CM_CPP#040 Discretionary Access Control
Apply discretionary access controls that limit access to trusted administrators and to those applications that require access.

Guidance: This requirement was previously AL3_CM_STS#010 b) (part a) having been withdrawn, which left part b) somewhat out of context.

5.4.1.2 Security Controls

An enterprise and its specified service must:

AL4_CM_CTR#010 Withdrawn

AL4_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, **showing that there is sufficient entropy**;
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;

f) session hijacking, 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.

Guidance: Organizations should consider potential protocol threats identified in other sources, e.g. ISO/IEC 29115:2013 “Information technology -- Security techniques – Entity authentication assurance framework”.*AL4_CM_CTR#025 No stipulation*

AL4_CM_CTR#028 No Stipulation

AL4_CM_CTR#030 System threat risk assessment and controls
MANDATORY.

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.

Guidance: the risk assessment should address these threats from any perspective in which they might adversely affect the operation of the service, whether they be from within the organization (e.g. in its development environment, the hosting environment) or without (e.g. network attacks, hackers).

AL4_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 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.

5.4.1.3 Storage of Long-term Secrets

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

AL4_CM_STS#010 Withdrawn
Withdrawn (AL4_CO_SCO#020 (a) & (b) enforce this requirement part a) and AL4_CM_CPP#040 now enforces part b))

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.

5.4.1.4 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
MANDATORY, to the extent that the sub-items relate to the scope of service.

Ensure that such audit records include:

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

5.4.1.5 Subject Options

AL4_CM_OPN#010 Changeable PIN/Password
Withdrawn – see AL4_CM_RNR#010.

5.4.2 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 Assurance Level 4.

5.4.2.1 Identity Proofing Policy

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.

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.

An enterprise and its 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.

Guidance: Cf. AL4_CM_CRN#020 which expresses a very similar requirement. Although presenting repetition for a single provider, if the identity-proofing functions and credential management functions are provided by separate CSPs, each needs to fulfill this requirement.

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 (IdPPS).

[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.

5.4.2.2 Identity Verification

The enterprise or specific service may:

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**;

AL4_ID_IDV#010 - Identity Verification Measures

[Omitted] Justify the identity verification measures described in its IdPPS (see AL**4**_ID_POL#040) by describing how these meet or exceed the requirements of applicable policies, regulations, adopted standards and other relevant conditions in order to maintain a level of rigour consistent with the AL**4.**

Guidance: Although strict requirements for identity proofing and verification can be defined, a real-world approach must account for instances where there is not 100% certitude. To cope with this CSPs need to have a set of prescribed (through policy – see AL4_ID_POL#030) and applied measures (see AL4_ID_POL#040) which observe policy, identify the measures taken according to the degree of certitude determined by each step in the verification process and what additional measures are taken. The CSP must present a case which shows that their solution is sufficient to ensure that the basic requirements of the applicable AL are met or exceeded.

Note that in each set of proofing service criteria below there are criteria with specific requirements for evidence checks and an additional criterion for ‘secondary’ checks, all of which have an interplay with these overall requirements to have a policy and practice statement and to demonstrate processes which sustain confidence that AL3 is being achieved.

Even though a CSP may use the services of a component service for the performance of the identity-proofing within its own service, it still needs to ensure that its policy is both justified and upheld. Where another service provider is used appropriate stipulations in contracts should be established, but any internal adherence to (e.g.) ’POL#040 should be determined by the fact that the component service is already Kantara Approved.

5.4.2.3 In-Person Public Identity Proofing

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:

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 telephone number, such as: utility bill, professional license or membership, or other evidence of equivalent standing.**

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.

5.4.2.4 Remote Public Identity Proofing

Not permitted.

5.4.2.5 Current Relationship Identity Proofing

Not permitted

5.4.2.6 Affiliation Identity Proofing

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 §**5.4.2.3**, "**In-Person Public Identity 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.

5.4.2.7 Issuing Derived Credentials

Where the Applicant already possesses recognized original credentials the CSP may choose to accept the verified identity of the Applicant as a substitute for identity proofing, subject to the following specific provisions. All other identity proofing requirements must also be observed.

AL4_ID_IDC#010 Authenticate Original Credential
Prior to issuing any derived credential the original credential on which the identity-proofing relies must be:

a) authenticated by a source trusted by the CSP as being valid and un-revoked;
b) issued at Assurance Level 4;
c) issued in the same name as that which the Applicant is claiming;
d) proven to be in the possession and under the control of the Applicant**, who shall be physically present**.

Guidance: This is the equivalent of recording the details of id documents provided during (e.g.) face-face id-proofing. It is not required that the original credential be issued by a Kantara-Approved CSP.

AL4_ID_IDC#020 Record Original Credential
Record the details of the original credential**, the biometric sample related to the original credential and the biometric sample captured when authenticating the Applicant**.

AL4_ID_IDC#030 Issue Derived Credential
Only issue the derived credential in-person after performing biometric authentication of the Applicant .

5.4.2.8 Secondary Identity 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).

5.4.2.9 Identity-proofing 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 (person, or entity if remote or automatic) performing the proofing functions, 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 [omitted].

Guidance: Although there is no specific stipulation as to what should be recorded the list below suggests facts which would typically be captured at this level:

a) the Subject's full name;
b) the Subject's current address of record;
c) the Subject'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#025 Provide Subject identity records
If required, provide to qualifying parties records of identity proofing to the extent permitted by applicable legislation and/or agreed by the Subscriber.

Guidance: the qualifier 'if required' is intended to account for circumstances where conditions such as whether a contract or a federation policy permits or is required or jurisdiction / legal injunction demand such provision. A qualifying party is any party to which provision of such info can justified according to circumstance: by contract/policy;

with Subject's agreement; with due authority (Court Order, e.g.). The CSP needs to make the case, according to their service's characteristics and operating environment**.**

AL4_ID_VRC#030 Record Retention
Either retain, securely, the record of the verification/revocation process for the duration of the Subject account plus a further period sufficient to allow fulfillment of any period required legally, contractually or by any other form of binding agreement or obligation, or submit the record to a client CSP that has undertaken to retain the record for the requisite period or longer.

AL4_CM_IDP#010 Revision to Subscriber information
Provide a means for Subscribers and Subjects 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.

AL4_CM_IDP#020 No stipulation

5.4.2.10 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 Subject. 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, 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.

Cf. AL4_CM_POL#020 which expresses a very similar requirement. Although presenting repetition for a single provider, if the identity-proofing functions and credential management functions are provided by separate CSPs, each needs to fulfill this requirement.

AL4_CM_CRN#030 Credential uniqueness

Allow the Subject to select a credential (e.g., UserID) that is verified to be unique within the specified service's community and assigned uniquely to a single identity Subject.

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 Token strength

***Not* use PIN/password tokens.**

AL4_CM_CRN#050 One-time password strength

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

AL4_CM_CRN#055 No stipulation

AL4_CM_CRN#060 Software cryptographic token strength

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

AL4_CM_CRN#070 One-time password 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) require password or biometric activation by the Subject **[omitted];**

c) **Generate a one-time password using an algorithm recognized by a national technical authority**.

AL4_CM_CRN#075 Multi-factor hardware cryptographic 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, PIN or biometric activation by the Subject when being used for authentication;

d) does not permit the export of authentication keys.

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.

AL4_CM_CRN#095 No stipulation
No stipulation

5.4.2.11 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.

5.4.2.12 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.

Guidance: The nature of issuance could mean that the Subject is fully aware and therefore no notification is necessary. If any other such circumstances prevailed, the CSP should identify them.

AL4_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 transaction (beyond the first transaction or encounter) **[deleted]** through the use of a biometric that was recorded during **the first** encounter**.**

AL4_CM_CRD#016 No stipulation
No stipulation.

AL4_CM_CRD#017 Protected Issuance of Permanent Secrets (in person)
Only issue permanent secrets if the CSP has loaded the secret itself onto the physical device, which was either:

a) issued in-person to the Applicant, or;

b) delivered in a manner that confirms the address of record.

AL4_CM_CRD#018 No stipulation
No stipulation.

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).

5.4.3 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 Assurance Level 4.

5.4.3.1 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:

AL4_CM_RNR#010 Changeable PIN/Password
Permit Subjects to change the passwords used to activate their credentials.

AL4_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.

AL4_CM_RNR#030 Renewal/Re-issuance limitations
a) No stipulation;

b) No stipulation;

c) No stipulation;

d) **cryptographically authenticate** all **sensitive** renewal / re-issuance interactions with the Subject **using keys bound to the authentication process**.

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

AL4_CM_RNR#040 Authentication key life
Expire after 24 hours all temporary or short-term keys derived during the authentication process.

AL4_CM_RNR#050 Record Retention
Retain, securely, the record of any renewal/re-issuance process for the duration of the Subscriber's account plus a further period sufficient to allow fulfillment of any period required legally, contractually or by any other form of binding agreement or obligation, or submit same record to a client CSP that has undertaken to retain the record for the requisite period or longer.

5.4.4 Part D - Credential Revocation

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

5.4.4.1 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 Verify Revocation Identity

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

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 or Subject themselves, someone acting with the Subscriber's or Subject'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); [Omitted]
d) the reason for revocation.

AL4_CM_RVP#060 Record Retention

Retain, securely, the record of the revocation process for a period which is the maximum of:

a) the records retention policy required by AL**4**_CM_CPP#**020**;

b) applicable legislation, regulation, contract or standards.

5.4.4.2 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 or Subject seeks revocation of the Subject's 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 or Subject, supported by a **different** credential at **Assurance Level 4**.

AL4_CM_RVR#040 Verify CSP as Revocant
Where a CSP seeks revocation of a Subject'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**.

5.4.4.3 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 Subject seeks a re-key for the Subject'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 Subject, supported by a different credential at Assurance Level 4.

AL4_CM_RKY#020 Re-key requests other than Subject
Re-key requests from any parties other than the Subject must not be accepted.

5.4.4.4 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.

5.4.5 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.

5.4.5.1 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 Claimant'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.

5.4.6 Part F - Credential Verification/Authentication

These criteria apply to credential validation and identity authentication.

5.4.6.1 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;
c) protects assertions against manufacture, modification, substitution and disclosure, and secondary authenticators from manufacture, capture and replay;
d) uses approved **strong** 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.

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#018 Ensure token validity
Ensure that tokens are either still valid or have been issued within the last 24 hours.

Guidance: The 24-hour period allows for the fact that if a freshly-issued credential is then revoked, notice of the revocation may take 24 hours to be publicised (per AL3_CM_RVP#030)..

AL4_CM_ASS#020 Post Authentication
Not authenticate credentials that have been revoked unless the time of the transaction for which verification is sought precedes the time of revocation of the credential.

Guidance: The purpose in this criterion is that, if a verification is intended to refer to the status of a credential at a specific historical point in time, e.g. to determine whether the Claimant was entitled to act as a signatory in a specific capacity at the time of the transaction, this may be done. It is implicit in this thinking that both the request and the response indicate the historical nature of the query and response; otherwise the default time is 'now'. If no such service is offered then this criterion may simply be 'Inapplicable', for that reason.

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#035 No stipulation

AL4_CM_ASS#040 Assertion Life-time
[Omitted] Notify the relying party of how often the revocation status sources are updated.

5.4.6.2 Authenticator-generated challenges

An enterprise and its specified service must:

AL4_CM_AGC#010 Entropy level
Create authentication secrets to be used during the authentication exchange (i.e. with out-of-band or cryptographic device tokens) with a degree of entropy appropriate to the token type in question.

AL4_CM_AGC#020 Limit password validity
Employ one-time passwords which expire within two minutes.

5.4.6.3 Multi-factor authentication

An enterprise and its specified service must:

AL4_CM_MFA#010 Permitted multi-factor tokens
Require two tokens which, when used in combination within a single authentication exchange, are acknowledged as providing an equivalence of AL**4**, as determined by a recognized national technical authority.

5.4.6.4 Verifier's assertion schema

Note: Since assertions and related schema can be complex and may be modeled directly on the needs and preferences of the participants, the details of such schema fall outside the scope of the SAC's herein, which are expressed observing, insofar as is feasible, a technology-agnostic policy. The following criteria, therefore, are perhaps more open to variable conformity through their final implementation than are others in this document.

These criteria are derived directly from NIST SP 800-63-2 and have been expressed in as generic a manner as they can be.

An enterprise and its specified service must:

AL4_CM_VAS#010 Approved cryptography
Apply assertion protocols which use cryptographic techniques approved by a national authority or other generally-recognized authoritative body.

AL4_CM_VAS#020 No browser/bearer assertions
Not issue browser / bearer assertions.

AL4_CM_VAS#030 Assertion assurance level
Create assertions which, either explicitly or implicitly (using a mutually-agreed mechanism), indicate the assurance level at which the initial authentication of the Subject was made.

AL4_CM_VAS#040 No pseudonyms

Create assertions which indicate only verified Subscriber names in the credential subject to verification.

AL4_CM_VAS#050 Specify recipient

Create assertions which identify the intended recipient of the verification such that the recipient may validate that it is intended for them.

AL4_CM_VAS#060 No assertion manufacture/modification

Ensure that it is impractical to manufacture an assertion or assertion reference by Signing the assertion and using at least one of the following techniques:

a) [Omitted];

b) Encrypting the assertion using a secret key shared with the RP;

c) Creating an assertion reference which has a minimum of 64 bits of entropy;

d) Sending the assertion over a protected channel during a mutually-authenticated session.

AL4_CM_VAS#070 Assertion protections

Provide protection of assertion-related data such that:

a) both assertions and assertion references are protected against capture and re-use;

b) assertions are also protected against redirection

c) assertions, assertion references and session cookies used for authentication purposes, including any which are re-directed, are protected against session hijacking, for at least the duration of their validity (see AL1_CM_VAS#110).

AL4_CM_VAS#080 Single-use assertions

Limit to a single transaction the use of assertions which do not support proof of ownership.

AL4_CM_VAS#090 Single-use assertion references

Limit to a single transaction the use of assertion references.

AL4_CM_VAS#100 Bind reference to assertion

Provide a strong binding between the assertion reference and the corresponding assertion, based on integrity-protected (or signed) communications over which the Verifier has been authenticated.

AL4_CM_VAS#110 No stipulation

No stipulation.

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.

These tables also provide an overview of any revisions made to criteria in comparison to v3.0 of this document (see §1.1).

Table 3-5. OP-SAC - AL1 Compliance

Clause	Description	Compliance
Part A – Credential Operating Environment		
AL1_CM_CTR#010	Withdrawn	No conformity requirement
AL1_CM_CTR#020	Protocol threat risk assessment and controls	*Amended; Guidance*
AL1_CM_CTR#025	No stipulation	No conformity requirement
AL1_CM_CTR#028	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	Withdrawn	No conformity requirement
AL1_CM_IDP#020	Withdrawn	No conformity requirement
AL1_CM_IDP#030	Withdrawn	No conformity requirement
AL1_ID_POL#010	Unique service identity	
AL1_ID_POL#020	Unique Subject identity	
AL1_ID_IDV#000	Identity Proofing classes	*New*
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_IDC#010	Authenticate Original Credential	*New*

AL1_ID_SCV#010	Secondary checks	
AL1_ID_VRC#010	No stipulation	No conformity requirement
AL1_ID_VRC#020	No stipulation	No conformity requirement
AL1_ID_VRC#025	Provide Subject Identity Records	*New*
AL1_ID_VRC#030	No stipulation	No conformity requirement
AL1_CM_IDP#010	Revision to Subscriber Information	*Amended; Guidance ; Re-numbered – was ’IDP#040*
AL1_CM_IDP#020	Authenticate Subject Information Changes	*New*
AL1_CM_CRN#010	Authenticated Request	
AL1_CM_CRN#020	No stipulation	No conformity requirement
AL1_CM_CRN#030	Credential uniqueness	
AL1_CM_CRN#035	Convey credential	*New*
AL1_CM_CRN#040	Token strength	*New*
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#018	No stipulation	No conformity requirement
AL1_CM_ASS#020	No Post Authentication	*Editorial*
AL1_CM_ASS#030	Proof of Possession	
AL1_CM_ASS#035	Limit authentication attempts	*New*
AL1_CM_ASS#040	Assertion Lifetime	*Amended*
AL1_CM_VAS#010	No stipulation	No conformity requirement *New*
AL1_CM_VAS#020	No stipulation	No conformity requirement *New*
AL1_CM_VAS#030	Assertion assurance level	*New*
AL1_CM_VAS#040	No stipulation	No conformity requirement *New*
AL1_CM_VAS#050	No stipulation	No conformity requirement *New*

AL1_CM_VAS#060	No assertion manufacture/modification	*New*
AL1_CM_VAS#070	No stipulation	No conformity requirement *New*
AL1_CM_VAS#080	Single-use assertions	*New*
AL1_CM_VAS#090	Single-use assertion references	*New*
AL1_CM_VAS#100	Bind reference to assertion	*New*

4058 **Table 3-6.** OP-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	*Amended; Guidance*
AL2_CM_CTR#025	Authentication protocols	*Amended; Guidance*
AL2_CM_CTR#028	One-time passwords	*Amended*
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	Withdrawn	No conformity requirement
AL2_CM_IDP#020	Withdrawn	No conformity requirement
AL2_CM_IDP#030	Withdrawn	No conformity requirement
AL2_ID_POL#010	Unique service identity	
AL2_ID_POL#020	Unique Subject identity	*Guidance*
AL2_ID_POL#030	Published Proofing Policy	
AL2_ID_POL#040	Adherence to Proofing Policy	
AL2_ID_IDV#000	Identity Proofing classes	*Amended*
AL2_ID_IDV#010	Identity Verification Measures	*New*
AL2_ID_IPV#010	Required evidence	
AL2_ID_IPV#020	Evidence checks	
AL2_ID_RPV#010	Required evidence	*Amended*
AL2_ID_RPV#020	Evidence checks	*Amended*
AL2_ID_CRV#010	Required evidence	
AL2_ID_CRV#020	Evidence checks	*Amended*
AL2_ID_AFV#000	Meet preceding criteria	
AL2_ID_AFV#010	Required evidence	
AL2_ID_AFV#020	Evidence checks	
AL2_ID_IDC#010	Authenticate Original Credential	*New*

AL2_ID_IDC#020	Record Original Credential	*New*
AL2_ID_IDC#030	Issue Derived Credential	*New*
AL2_ID_SCV#010	Secondary checks	*Amended*
AL2_ID_VRC#010	Verification Records for Personal Applicants	*Amended*
AL2_ID_VRC#020	Verification Records for Affiliated Applicants	*Amended*
AL2_ID_VRC#025	Provide Subject identity records	*New*
AL2_ID_VRC#030	Record Retention	
AL2_CM_IDP#010	Revision to Subscriber information	*Amended; Guidance ; Re-numbered – was ’IDP#040*
AL2_CM_IDP#020	Authenticate Subject Information Changes	*New*
AL2_CM_CRN#010	Authenticated Request	
AL2_CM_CRN#020	Unique identity	*Guidance*
AL2_CM_CRN#030	Credential uniqueness	
AL2_CM_CRN#035	Convey credential	
AL2_CM_CRN#040	Password strength	*Amended*
AL2_CM_CRN#050	One-time password strength	
AL2_CM_CRN#055	One-time password lifetime	*Amended*
AL2_CM_CRN#060	Software cryptographic token strength	*Amended*
AL2_CM_CRN#070	Hardware token strength	*Amended*
AL2_CM_CRN#075	No stipulation	No conformity requirement
AL2_CM_CRN#080	No stipulation	No conformity requirement
AL2_CM_CRN#090	Nature of Subject	
AL2_CM_CRN#095	Pseudonym’s Real Identity	*New*
AL2_CM_CRD#010	Notify Subject of Credential Issuance	*Guidance*
AL2_CM_CRD#015	Confirm Applicant’s identity (in person)	*Amended*
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	*Amended*
AL2_CM_RNR#040	No stipulation	No conformity requirement
AL2_CM_RNR#050	Record Retention	*New*
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#045	Notification of Revoked Credential	*New*
AL2_CM_RVP#050	Revocation Records	
AL2_CM_RVP#060	Record Retention	*Amended*
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#013	No stipulation	
AL2_CM_ASS#015	No False Authentication	
AL2_CM_ASS#018	No stipulation	*New*
AL2_CM_ASS#020	No Post Authentication	*Editorial; Guidance*
AL2_CM_ASS#030	Proof of Possession	
AL2_CM_ASS#035	Limit authentication attempts	*New*
AL2_CM_ASS#040	Assertion Lifetime	*Amended*
AL2_CM_AGC#010	Entropy level	*New*
AL2_CM_MFA#010	Permitted multi-factor tokens	*New*
AL2_CM_VAS#010	Approved cryptography	*New*
AL2_CM_VAS#020	No stipulation	No conformity requirement *New*
AL2_CM_VAS#030	Assertion assurance level	*New*
AL2_CM_VAS#040	Notify pseudonyms	*New*
AL2_CM_VAS#050	Specify recipient	*New*

AL2_CM_VAS#060	No assertion manufacture/modification	*New*
AL2_CM_VAS#070	Assertion protections	*New*
AL2_CM_VAS#080	Single-use assertions	*New*
AL2_CM_VAS#090	Single-use assertion references	*New*
AL2_CM_VAS#100	Bind reference to assertion	*New*

4061 **Table 3-7.** OP-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	Withdrawn	No conformity requirement
AL3_CM_CTR#020	Protocol threat risk assessment and controls	*Amended; Guidance*
AL3_CM_CTR#025	Permitted authentication protocols	*Amended*
AL3_CM_CTR#028	No stipulation	No conformity requirement
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_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_IDV#010	Identity Verification Measures	
AL3_ID_IPV#010	Required evidence	
AL3_ID_IPV#020	Evidence checks	
AL3_ID_RPV#010	Required evidence	*Amended*
AL3_ID_RPV#020	Evidence checks	*Amended*
AL3_ID_CRV#010	Required evidence	*New*
AL3_ID_CRV#020	Evidence checks	*New*
AL3_ID_AFV#000	Meet preceding criteria	
AL3_ID_AFV#010	Required evidence	
AL3_ID_AFV#020	Evidence checks	
AL3_ID_IDC#010	Authenticate Original Credential	*New*
AL3_ID_IDC#020	Record Original Credential	*New*

AL3_ID_IDC#030	Issue Derived Credential	*New*
AL3_ID_SCV#010	Secondary checks	*Amended*
AL3_ID_VRC#010	Verification Records for Personal Applicants	*Amended*
AL3_ID_VRC#020	Verification Records for Affiliated Applicants	*Amended; Guidance*
AL3_ID_VRC#025	Provide Subject Identity Records	*New*
AL3_ID_VRC#030	Record Retention	
AL3_CM_IDP#010	Revision to Subscriber information	*Amended; Guidance ;* *Re-numbered – was ’IDP#040*
AL3_CM_IDP#020	Authenticate Subject Information Changes	*New*
AL3_CM_CRN#010	Authenticated Request	
AL3_CM_CRN#020	Unique identity	*Guidance*
AL3_CM_CRN#030	Credential uniqueness	
AL3_CM_CRN#035	Convey credential	
AL3_CM_CRN#040	PIN/Password strength	*Editorial*
AL3_CM_CRN#050	One-time password strength	
AL3_CM_CRN#055	No stipulation	No conformity requirement
AL3_CM_CRN#060	Software cryptographic token strength	*Amended*
AL3_CM_CRN#070	Hardware token strength	*Amended*
AL3_CM_CRN#075	No stipulation	No conformity requirement
AL3_CM_CRN#080	Binding of key	
AL3_CM_CRN#090	Nature of Subject	
AL3_CM_CRN#095	No stipulation	No conformity requirement
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	*Guidance*
AL3_CM_CRD#015	Confirm Applicant’s identity (in person)	*New*
AL3_CM_CRD#016	Confirm Applicant’s identity (remotely)	*New*
AL3_CM_CRD#017	Protected Issuance of Permanent Secrets (in person)	*New*
AL3_CM_CRD#018	Protected Issuance of Permanent Secrets (remotely)	*New*
AL3_CM_CRD#020	Subject's acknowledgement	
Part C – Credential Renewal and Re-issuing		
AL3_CM_RNR#010	Changeable PIN/Password	

AL3_CM_RNR#020	Proof-of-possession on Renewal/Re-issuance	*New*
AL3_CM_RNR#030	Renewal/Re-issuance limitations	*New*
AL3_CM_RNR#040	No stipulation	No conformity requirement
AL3_CM_RNR#050	Record Retention	*New*
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	*Amended*
AL3_CM_RVP#060	Record Retention	*Amended*
AL3_CM_RVR#010	Verify revocation identity	*Amended*
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	*Amended*
AL3_CM_ASS#015	No False Authentication	
AL3_CM_ASS#018	Ensure token validity	New
AL3_CM_ASS#020	Post Authentication	Guidance
AL3_CM_ASS#030	Proof of Possession	*New*
AL3_CM_ASS#035	Limit authentication attempts	New
AL3_CM_ASS#040	Assertion Lifetime	
AL3_CM_AGC#010	Entropy level	*New*
AL3_CM_MFA#010	Permitted multi-factor tokens	*New*
AL3_CM_VAS#010	Approved cryptography	*New*
AL3_CM_VAS#020	No stipulation	No conformity requirement

AL3_CM_VAS#030	Assertion assurance level	*New*
AL3_CM_VAS#040	Notify pseudonyms	*New*
AL3_CM_VAS#050	Specify recipient	*New*
AL3_CM_VAS#060	No assertion manufacture/modification	*New*
AL3_CM_VAS#070	Assertion protections	*New*
AL3_CM_VAS#080	Single-use assertions	*New*
AL3_CM_VAS#090	Single-use assertion references	*New*
AL3_CM_VAS#100	Bind reference to assertion	*New*
AL3_CM_VAS#110	SSO provisions	*New*

4064 **Table 3-8.** OP-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_CPP#040	Discretionary Access Control	*New*
AL4_CM_CTR#010	Withdrawn	No conformity requirement
AL4_CM_CTR#020	Protocol threat risk assessment and controls	*Amended; Guidance*
AL4_CM_CTR#025	No stipulation	No conformity requirement
AL4_CM_CTR#028	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	Withdrawn	No conformity requirement *Re-numbered as AL4_CO_SCO#020 & AL4_CM_CPP#040*
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_ID_POL#010	Unique service identity	
AL4_ID_POL#020	Unique Subject identity	*Guidance*
AL4_ID_POL#030	Published Proofing Policy	
AL4_ID_POL#040	Adherence to Proofing Policy	*Editorial*
AL4_ID_IDV#000	Identity Proofing classes	
AL4_ID_IDV#010	Identity Verification Measures	*New*
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_IDC#010	Authenticate Original Credential	*New*
AL4_ID_IDC#020	Record Original Credential	*New*
AL4_ID_IDC#030	Issue Derived Credential	*New*
AL4_ID_SCV#010	Secondary checks	
AL4_ID_VRC#010	Verification Records for Personal Applicants	*Amended*
AL4_ID_VRC#020	Verification Records for Affiliated Applicants	*Amended; Guidance*
AL4_ID_VRC#025	Provide Subject identity records	*New*
AL4_ID_VRC#030	Record Retention	
AL4_CM_IDP#010	Revision to Subscriber information	*Amended; Guidance ; Re-numbered – was 'IDP#040*
AL4_CM_IDP#020	No stipulation	No conformity requirement
AL4_CM_CRN#010	Authenticated Request	
AL4_CM_CRN#020	Unique identity	*Guidance*
AL4_CM_CRN#030	Credential uniqueness	
AL4_CM_CRN#035	Convey credential	
AL4_CM_CRN#040	PIN/Password strength	*Editorial*
AL4_CM_CRN#050	One-time password strength	
AL4_CM_CRN#055	No stipulation	No conformity requirement
AL4_CM_CRN#060	Software cryptographic token strength	
AL4_CM_CRN#070	Hardware token strength	*New*
AL4_CM_CRN#075	Multi-factor hardware cryptographic token strength	*Amended*
AL4_CM_CRN#080	Binding of key	
AL4_CM_CRN#090	Nature of Subject	
AL4_CM_CRN#095	No stipulation	No conformity requirement
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	*Guidance*
AL4_CM_CRD#015	Confirm Applicant's identity (in person)	*New*
AL4_CM_CRD#016	No stipulation	No conformity requirement
AL4_CM_CRD#017	Protected Issuance of Permanent Secrets (in person)	*New*
AL4_CM_CRD#018	No stipulation	No conformity requirement
AL4_CM_CRD#020	Subject's acknowledgement	
Part C – Credential Renewal and Re-issuing		

AL4_CM_RNR#010	Changeable PIN/Password	
AL4_CM_RNR#020	Proof-of-possession on Renewal/Re-issuance	*New*
AL4_CM_RNR#030	Renewal/Re-issuance limitations	*New*
AL4_CM_RNR#040	Authentication key life	*New*
AL4_CM_RNR#050	Record Retention	*New*
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	Verify Revocation Identity	*New*
AL4_CM_RVP#050	Revocation Records	*Amended*
AL4_CM_RVP#060	Record Retention	*Amended*
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 Subject	
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	*Amended*
AL4_CM_ASS#015	No False Authentication	
AL3_CM_ASS#018	Ensure token validity	*New*
AL4_CM_ASS#020	Post Authentication	*Guidance*
AL4_CM_ASS#030	Proof of Possession	
AL3_CM_ASS#035	No stipulation	No conformity requirement
AL4_CM_ASS#040	Assertion Lifetime	
AL4_CM_AGC#010	Entropy level	*New*

AL4_CM_AGC#020	Limit password validity	*New*
AL4_CM_MFA#010	Permitted multi-factor tokens	*New*
AL4_CM_VAS#010	Approved cryptography	*New*
AL4_CM_VAS#020	No browser/bearer assertions	*New*
AL4_CM_VAS#030	Assertion assurance level	*New*
AL4_CM_VAS#040	Notify pseudonyms	*New*
AL4_CM_VAS#050	Specify recipient	*New*
AL4_CM_VAS#060	No assertion manufacture/modification	*New*
AL4_CM_VAS#070	Assertion protections	*New*
AL4_CM_VAS#080	Single-use assertions	*New*
AL4_CM_VAS#090	Single-use assertion references	*New*
AL4_CM_VAS#100	Bind reference to assertion	*New*
AL4_CM_VAS#110	No stipulation	No conformity requirement

6 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., ed., "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

7 REVISION HISTORY

1. 2008-05-08 – Identity Assurance Framework Version 1.0 Initial Draft
    a. Released by Liberty Alliance
    b. Revision and scoping of Initial Draft release
2. 2008-06-23 – Identity Assurance Framework Version 1.1 Final Draft
    a. Released by Liberty Alliance
    b. Inclusion of comments to Final Draft
3. 2009-10-01 – Identity Assurance Framework Version 1.1 Final Draft
    a. Documents contributed to Kantara Initiative by Liberty Alliance
4. 2010-04-dd – SAC Version 2.0
    a. Released by Kantara Initiative
    b. Significant scope build
    c. Original Identity Assurance Framework all inclusive document broken in to a set of documents with specific focus:
        i. Kantara IAF-1000-Overview
        ii. Kantara IAF-1100-Glossary
        iii. Kantara IAF-1200-Levels of Assurance
        iv. Kantara IAF-1300-Assurance Assessment Scheme
        v. Kantara IAF-1400-Service Assessment Criteria (this document)
        vi. Kantara IAF-1600-Assessor Qualifications and Requirements
5. 2012-10-10 - SAC Version 3.0
    a. Revision to accommodate Full/Component Service Assessment and Approval.
6. 2014-05-12 – SAC Version 4.0*bis*
    a. Revision to map SAC against NIST SP 800-63-2;
    b. Alignment to revised Glossary;
    c. Inclusion of reference to formal approving ballot (in *bis* release).