

Identity Assurance Framework:
Service Assessment Criteria

**Version**: 3.0-h

**Date**: 2013-05-29

**Editor**: Richard G. Wilsher
 Zygma LLC

**Contributors**

The full list of contributors can be referenced here: [http://kantarainitiative.org/confluence/display/idassurance/IAF+2.0+Contributors](http://kantarainitiative.org/confluence/display/idassurance/IAF%2B2.0%2BContributors)

**Abstract**

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

The latest versions of each of these documents can be found on Kantara’s [Identity Assurance Framework - General Information web page](http://kantarainitiative.org/confluence/x/e4R7Ag).

**Filename:** Kantara IAF-1400 SAC v4-0

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.

Copyright: The content of this document is copyright of Kantara Initiative.
© 2013 Kantara Initiative.

Contents

[1 INTRODUCTION 5](#_Toc337678245)

[1.1 Changes in this revision 5](#_Toc337678246)

[2 ASSURANCE LEVELS 7](#_Toc337678247)

[3 SERVICE ASSESSMENT CRITERIA - GENERAL 8](#_Toc337678248)

[3.1 Context and Scope 8](#_Toc337678249)

[3.2 Criteria Applicability 8](#_Toc337678250)

[3.3 Status and Readership 8](#_Toc337678251)

[3.4 Criteria Descriptions 9](#_Toc337678252)

[3.5 Terminology 11](#_Toc337678253)

[4 COMMON ORGANIZATIONAL SERVICE ASSESSMENT CRITERIA 12](#_Toc337678254)

[4.1 Assurance Level 1 12](#_Toc337678255)

[4.1.1 Enterprise and Service Maturity 12](#_Toc337678256)

[4.1.2 Notices and User information 13](#_Toc337678257)

[4.1.3 Not used 14](#_Toc337678258)

[4.1.4 Not used 14](#_Toc337678259)

[4.1.5 Not used 14](#_Toc337678260)

[4.1.6 Not used 14](#_Toc337678261)

[4.1.7 Secure Communications 14](#_Toc337678262)

[4.2 Assurance Level 2 15](#_Toc337678263)

[4.2.1 Enterprise and Service Maturity 15](#_Toc337678264)

[4.2.2 Notices and User Information/Agreements 16](#_Toc337678265)

[4.2.3 Information Security Management 18](#_Toc337678266)

[4.2.4 Security-relevant Event (Audit) Records 20](#_Toc337678267)

[4.2.5 Operational infrastructure 21](#_Toc337678268)

[4.2.6 External Services and Components 22](#_Toc337678269)

[4.2.7 Secure Communications 22](#_Toc337678270)

[4.3 Assurance Level 3 25](#_Toc337678271)

[4.3.1 Enterprise and Service Maturity 25](#_Toc337678272)

[4.3.2 Notices and User Information 26](#_Toc337678273)

[4.3.3 Information Security Management 28](#_Toc337678274)

[4.3.4 Security-Relevant Event (Audit) Records 31](#_Toc337678275)

[4.3.5 Operational Infrastructure 31](#_Toc337678276)

[4.3.6 External Services and Components 33](#_Toc337678277)

[4.3.7 Secure Communications 33](#_Toc337678278)

[4.4 Assurance Level 4 35](#_Toc337678279)

[4.4.1 Enterprise and Service Maturity 35](#_Toc337678280)

[4.4.2 Notices and Subscriber Information/Agreements 36](#_Toc337678281)

[4.4.3 Information Security Management 38](#_Toc337678282)

[4.4.4 Security-Related (Audit) Records 41](#_Toc337678283)

[4.4.5 Operational Infrastructure 41](#_Toc337678284)

[4.4.6 External Services and Components 43](#_Toc337678285)

[4.4.7 Secure Communications 43](#_Toc337678286)

[4.5 Compliance Tables 45](#_Toc337678287)

[5 OPERATIONAL SERVICE ASSESSMENT CRITERIA 52](#_Toc337678288)

[5.1 Assurance Level 1 52](#_Toc337678289)

[5.1.1 Part A - Credential Operating Environment 52](#_Toc337678290)

[5.1.2 Part B - Credential Issuing 54](#_Toc337678291)

[5.1.3 Part C - Credential Renewal and Re-issuing 56](#_Toc337678292)

[5.1.4 Part D - Credential Revocation 56](#_Toc337678293)

[5.1.5 Part E - Credential Status Management 57](#_Toc337678294)

[5.1.6 Part F - Credential Validation/Authentication 57](#_Toc337678295)

[5.2 Assurance Level 2 59](#_Toc337678296)

[5.2.1 Part A - Credential Operating Environment 59](#_Toc337678297)

[5.2.2 Part B - Credential Issuing 61](#_Toc337678298)

[5.2.3 Part C - Credential Renewal and Re-issuing 70](#_Toc337678299)

[5.2.4 Part D - Credential Revocation 70](#_Toc337678300)

[5.2.5 Part E - Credential Status Management 73](#_Toc337678301)

[5.2.6 Part F - Credential Validation/Authentication 74](#_Toc337678302)

[5.3 Assurance Level 3 76](#_Toc337678303)

[5.3.1 Part A - Credential Operating Environment 76](#_Toc337678304)

[5.3.2 Part B - Credential Issuing 79](#_Toc337678305)

[5.3.3 Part C - Credential Renewal and Re-issuing 88](#_Toc337678306)

[5.3.4 Part D - Credential Revocation 88](#_Toc337678307)

[5.3.5 Part E - Credential Status Management 91](#_Toc337678308)

[5.3.6 Part F - Credential Validation/Authentication 92](#_Toc337678309)

[5.4 Assurance Level 4 94](#_Toc337678310)

[5.4.1 Part A - Credential Operating Environment 94](#_Toc337678311)

[5.4.2 Part B - Credential Issuing 97](#_Toc337678312)

[5.4.3 Part C - Credential Renewal and Re-issuing 105](#_Toc337678313)

[5.4.4 Part D - Credential Revocation 106](#_Toc337678314)

[5.4.5 Part E - Credential Status Management 109](#_Toc337678315)

[5.4.6 Part F - Credential Validation/Authentication 110](#_Toc337678316)

[5.5 Compliance Tables 112](#_Toc337678317)

[6 REFERENCES 123](#_Toc337678318)

[7 SAC v2.0 to SAC v3.0 CRITERIA MAPPING 126](#_Toc337678319)

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*](http://www.kantarainitiative.org/) 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](http://kantarainitiative.org/confluence/x/e4R7Ag).

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](#NIST80063)] 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.

## Changes in this revision

The principal reason for changes in this revision is to capture results of a mapping between this version 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.

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.

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](#M0404)] and NIST Special Publication 800-63 [[NIST800-63](#NIST80063)]. 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](http://kantarainitiative.org/confluence/x/e4R7Ag).

SERVICE ASSESSMENT CRITERIA - GENERAL

## 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’.

## 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.

## 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.

## 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.

## 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](http://kantarainitiative.org/confluence/x/e4R7Ag).

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.

# COMMON ORGANIZATIONALSERVICE 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](#Section2). 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.

## Assurance Level 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.

[US / EZP800-63-2: §7.3.1.3 e) iii)]

**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).

[US / EZP800-63-2: §5.3.1.1.9, §7.3.1.3 e) iii)]

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.

[US / EZP800-63-2: §5.3.1.1.9]

**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.

### 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:

1. 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:

1. indicate, prior to receiving service, that they have read and accept the terms of service as defined in the Service Definition;
2. 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;
3. 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).

### Not used

### Not used

### Not used

### Not used

### Secure Communications

AL1\_CO\_SCO#010 No stipulation

AL1\_CO\_SCO#020 Limited access to shared secrets

Ensure that:

1. access to shared secrets shall be subject to discretionary controls which permit access to those roles/applications needing such access;
 [US / EZP800-63-2: §7.3.1.1 a) i)]
2. stored shared secrets are not held in their plaintext form unless given adequate physical or logical protection;
 [US / EZP800-63-2: §7.3.1.1 a) ii)]
3. any plaintext passwords or secrets are not transmitted across any public or unsecured network.

[US / EZP800-63-2: §8.3.2.1.3]

## 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.

### 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**.

[US / EZP800-63-2: §7.3.1.2 e) iii)]

**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).

[US / EZP800-63-2: §5.3.1.2.2; §5.3.1.2.9, §7.3.1.2 e) iii)]

**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.

[US / EZP800-63-2: §5.3.1.2.9]

**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.

### 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:

1. Privacy**,** **Identity Proofing & Verification, Renewal/Re-issuance, and Revocation and Termination Policies;** [US / EZP800-63-2: §7.3.1.2 c) i)]
2. **the country in or legal jurisdiction under which the service is operated;**
3. **if different from the above, the legal jurisdiction under which Subscriber and any relying party agreements are entered into;**
4. **applicable legislation with which the service complies;**
5. **obligations incumbent upon the CSP;**
6. **obligations incumbent upon the Subscriber/Subject;**
7. **notifications and guidance for relying parties, especially in respect of actions they are expected to take should they choose to rely upon the service;**
8. **statement of warranties;**
9. **statement of liabilities toward Subscribers, Subjects and Relying Parties;**
10. **procedures for notification of changes to terms and conditions;**
11. **steps the CSP will take in the event that it chooses or is obliged to terminate the service;**
12. **availability of the specified service *per se* and of its help desk facility.**

[US / EZP800-63-2: §5.3.1.2.3]

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:

1. indicate, prior to receiving service, that they have read and accept the terms of service as defined in the Service Definition;
2. 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;
3. 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.

### 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.**

[US / EZP800-63-2: §7.3.1.2 f), §8.3.2.2.3]

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:**

* + - 1. **version control for software system components;**
			2. **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.**

[US / EZP800-63-2: §7.3.1.2 f)]

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.**

[US / EZP800-63-2: §7.3.1.2 f)]

**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’ 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. This could be accomplished by fulfilling the AL2\_CO\_ISM#090 requirement on a 12-monthly basis.

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.

### 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.**

[US / EZP800-63-2: §7.3.1.2 f)]

**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.

### 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.**

[US / EZP800-63-2: §7.3.1.2 f) , §8.3.2.2.3, ’2.7]

**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:**

1. **access to sensitive areas is restricted to authorized personnel;**
2. **all removable media and paper documents containing sensitive information as plain-text are stored in secure containers.**

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

AL2\_CO\_OPN#070 Logical access control

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

### 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.**

### 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, the communications must be cryptographically authenticated, including long-term and session tokens, by an authentication method that meets, at a minimum, the requirements of AL2 and encrypted using an encryption method approved by a national authority or other generally-recognized authoritative body.**

[US / EZP800-63-2: §5.3.1.2.4, §7.3.1.2 b) ii & iii)]

AL2\_CO\_SCO#015 Verification / Authentication confirmation messages

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

[US / EZP800-63-2: §5.3.1.2.4, §7.3.1.2 b) iv)]

AL2\_CO\_SCO#016 Verification of Revoked Credential

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

1. **the confirmation message shall be time-stamped, or;**
2. **the session keys shall expire with an expiration time no longer than that of the applicable revocation list, or;**
3. **the time-stamped message, binding, and credential shall all be signed by the service.**

[US / EZP800-63-2: §5.3.1.2.4, §7.3.1.2 b) v)]

AL2\_CO\_SCO#020 Limited access to shared secrets

Ensure that:

* + - 1. access to shared secrets shall be subject to discretionary controls that only permit access by those roles/applications requiring such access;
			 [US / EZP800-63-2: §7.3.1.2 a) i)]
			2. stored shared secrets are not held in their plaintext form unless given adequate physical or logical protection;
			 [US / EZP800-63-2: §7.3.1.2 a) ii)]
			3. **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).**
			 [US / EZP800-63-2: §7.3.1.2 b) i)]

 **In addition, these roles should be defined and documented by the CSP in accordance with AL2\_CO\_OPN#020 above**.

[US / EZP800-63-2: §7.3.1.2 f)]

AL2\_CO\_SCO#030 Logical protection of shared secrets

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

* 1. **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;**
	2. **encryption using an Approved algorithm and modes, and the shared secret decrypted only when immediately required for authentication, or;**
	3. **any secure method allowed to protect shared secrets at Level 3 or 4.**

## Assurance Level 3

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

### 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.

[US / EZP800-63-2: §7.3.1.3 e) iii)]

**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).

[US / EZP800-63-2: §5.3.1.3.2; §5.3.1.3.9, §7.3.1.3 e) iii)]

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.

[US / EZP800-63-2: §5.3.1.3.9]

**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.**

### 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:

1. Privacy, Identity Proofing & Verification, Renewal/Re-issuance,and Revocation and Termination Policies;
 [US / EZP800-63-2: §7.3.1.3 c) α] *(EZP800-63-2 needs poss revision to add a clause)*
2. the country in or the legal jurisdiction under which the service is operated;
3. if different to the above, the legal jurisdiction under which Subscriber and any relying party agreements are entered into;
4. applicable legislation with which the service complies;
5. obligations incumbent upon the CSP;
6. obligations incumbent upon the Subscriber and Subject;
7. 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;
8. statement of warranties;
9. statement of liabilitiestoward both Subjects and Relying Parties;
10. procedures for notification of changes to terms and conditions;
11. steps the CSP will take in the event that it chooses or is obliged to terminate the service;
12. availability of the specified service *per se* and of its help desk facility.

[US / EZP800-63-2: §5.3.1.3.3]

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:

1. indicate, prior to receiving service, that they have read and accept the terms of service as defined in the Service Definition;
2. 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;
3. 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.

### 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**](#IS27001)**] practices**.

[US / EZP800-63-2: §7.3.1.3 b) iv), §7.3.1.3 f), , §8.3.2.2.7]

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 placea configuration management system that at least includes:

1. version control for software system components;
2. timely identification and installation of all organizationally-approved patches for any software used in the provisioning of the specified service**;**
3. **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 placea 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:**

1. **the software and hardware development environments, for customized components;**
2. **the procurement process for commercial off-the-shelf (COTS) components;**
3. **contracted consultancy/support services;**
4. **shipment of system components;**
5. **storage of system components;**
6. **installation environment security;**
7. **system configuration;**
8. **transfer to operational status**.

[US / EZP800-63-2: §7.3.1.3 b) iv) , §7.3.1.3 f)]

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 itsorganizational size or due to other **justifiable** operational restrictions it is unreasonable to be so audited.

[US / EZP800-63-2: §7.3.1.3 b) iv) , §7.3.1.3 f)]

**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 the third-party audit required by AL3\_CO\_ISM#090 to provide the independent audit instead of the assignment of an internal audit function is not an acceptable means of fulfilling this criterion.  Management systems require that there be internal audit conducted as an inherent part of management review processes.  Third-party audit of the management system is a fully separate requirement, intended to show that the internal management system controls are being appropriately applied.

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.

### 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.

 [US / EZP800-63-2: §7.3.1.3 f)]

**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.

### 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.

[US / EZP800-63-2: §7.3.1.3 b) iv), §7.3.1.3 f)]

**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:

1. access to sensitive areas is restricted to authorized personnel;
2. all removable media and paper documents containing sensitive information as plain-text are stored in secure containers;
3. 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.

### 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.

### 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, the communications must be cryptographically authenticated, including [**omitted**] session tokens **but excluding long-term secrets**, by an authentication protocol that meets, at a minimum, the requirements of AL**3** and encrypted using **either a FIPS 140-2 [**[**FIPS140-2**](http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf)**] 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.

[US / EZP800-63-2: §5.3.1.3.4, §7.3.1.3 b) iii), §8.3.2.3.3, ’3.6]

AL2\_CO\_SCO#015 Verification / Authentication confirmation messages

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

[US / EZP800-63-2: §8.3.2.3.3]

AL2\_CO\_SCO#016 Verification of Revoked Credential

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

1. the confirmation message shall be time-stamped, or;
2. the session keys shall expire with an expiration time no longer than that of the applicable revocation list, or;
3. the time-stamped message, binding, and credential shall all be signed by the service.

[US / EZP800-63-2: §8.3.2.3.3]

AL3\_CO\_SCO#020 Limited access to shared secrets

Ensure that:

1. access to shared secrets shall be subject to discretionary controls that permit access to those roles/applications requiring such access;
 [US / EZP800-63-2: §7.3.1.3 a) i), §8.3.2.3.4]
2. 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**](http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf)**] 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;**
 [US / EZP800-63-2: §7.3.1.3 a) ii)]

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

1. 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).
 [US / EZP800-63-2: §7.3.1.3 a) i), §8.3.2.3.4]

 **These roles should be defined and documented by the CSP in accordance with AL3\_CO\_OPN#020 above**.

[US / EZP800-63-2: §7.3.1.3 f)]

## Assurance Level 4

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

### 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.

[US / EZP800-63-2: §7.3.1.4 e) iii)]

**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).

[US / EZP800-63-2: §5.3.1.4.2; §5.3.1.4.9, §7.3.1.4 e) iii)]

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.

[US / EZP800-63-2: §5.3.1.4.9]

**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.

### 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:

1. Privacy, Identity Proofing & Verification, Renewal/Re-issuance,and Revocation and Termination Policies;
 [US / EZP800-63-2: §7.3.1.4 c) α] *(EZP800-63-2 needs poss revision to add a clause)*
2. the country in or legal jurisdiction under which the service is operated;
3. if different to the above, the legal jurisdiction under which Subscriber and any relying party agreements are entered into;
4. applicable legislation with which the service complies;
5. obligations incumbent upon the CSP;
6. obligations incumbent upon the Subscriber and Subject;
7. 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;
8. statement of warranties;
9. statement of liabilities toward both Subjects and Relying Parties;
10. procedures for notification of changes to terms and conditions;
11. steps the CSP will take in the event that it chooses or is obliged to terminate the service;
12. availability of the specified service per se and of its help desk facility.

[US / EZP800-63-2: §5.3.1.4.3]

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:

1. 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;
2. 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;
3. 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.

### 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 CobITor [[IS27001](#IS27001)] methods.

[US / EZP800-63-2: §7.3.1.4 b) iv), §7.3.1.4 f)]

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:

1. version control for software system components;
2. timely identification and installation of all organizationally-approved patches for any software used in the provisioning of the specified service;
3. 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:

1. the software and hardware development environments, for customized components;
2. the procurement process for commercial off-the-shelf (COTS) components;
3. contracted consultancy/support services;
4. shipment of system components;
5. storage of system components;
6. installation environment security;
7. system configuration;
8. transfer to operational status.

[US / EZP800-63-2: §7.3.1.4 b) iv) , §7.3.1.4 f)]

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 organizationalsize or due to other justifiable operational restrictions it is unreasonable to be so audited.

[US / EZP800-63-2: §7.3.1.4 b) iv) , §7.3.1.4 f)]

**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 the third-party audit required by AL4\_CO\_ISM#090 to provide the independent audit instead of the assignment of an internal audit function is not an acceptable means of fulfilling this criterion.  Management systems require that there be internal audit conducted as an inherent part of management review processes.  Third-party audit of the management system is a fully separate requirement, intended to show that the internal management system controls are being appropriately applied.

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**](#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.

### 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.

[US / EZP800-63-2: §7.3.1.4 f)]

**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.

### 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.

[US / EZP800-63-2: §7.3.1.4 b) iv), §7.3.1.4 f)]

**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:

1. access to sensitive areas is restricted to authorized personnel;
2. all removable media and paper documents containing sensitive information as plain-text are stored in secure containers;
3. 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.

### 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.

### 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, the communications must be cryptographically authenticated, including [**omitted**] session tokens **but excluding long-term secrets**, by an authentication protocol that meets the requirements of AL4 and encrypted using either a FIPS 140-2 [[FIPS140-2](http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf)] 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.

[US / EZP800-63-2: §5.3.1.4.4, §7.3.1.4 b) iii) , §8.3.2.4.2, §8.3.2.4.5]

AL4\_CO\_SCO#020 Limited access to shared secrets

Ensure that:

1. access to shared secrets shall be subject to discretionary controls which permit access to those roles/applications which need such access;
 [US / EZP800-63-2: §7.3.1.4 a) i) , §8.3.2.4.2]
2. 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](http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf)] 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;
 [US / EZP800-63-2: §7.3.1.4 a) ii)]

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

1. 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**.

[US / EZP800-63-2: §7.3.1.4 f)]

## Compliance Tables

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

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

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

Table 3-1. CO-SAC - AL1 Compliance

| **Clause** | **Description** | **Compliance** |
| --- | --- | --- |
| AL1\_CO\_ESM#010 | [Established enterprise](#_Hlk221478373) |  |
| AL1\_CO\_ESM#020 | Withdrawn |  |
| AL1\_CO\_ESM#030 | [Legal & Contractual compliance](#_Hlk221478411) |  |
| AL1\_CO\_ESM#040 | [No stipulation](#_Hlk246240259) |  |
| AL1\_CO\_ESM#040 | [No stipulation](#_Hlk246240280) |  |
| AL1\_CO\_ESM#055 | [Termination provisions](#_Hlk239696555) |  |
| AL1\_CO\_NUI#010 | [General Service Definition](#_Hlk221478436) |  |
| AL1\_CO\_NUI#020 | [Service Definition inclusions](#_Hlk239694966) |  |
| AL1\_CO\_NUI#030 | [Due notification](#_Hlk221478552) |  |
| AL1\_CO\_NUI#040 | [User Acceptance](#_Hlk221478535) |  |
| AL1\_CO\_NUI#050 | [Record of User Acceptance](#_Hlk245606623) |  |
| AL1\_CO\_SCO#020 | [Limited access to shared secrets](#_Hlk221478601) |  |

Table 3-2. CO-SAC - AL2 Compliance

| Clause | Description | Compliance |
| --- | --- | --- |
| AL2\_CO\_ESM#010 | [Established enterprise](#_Hlk221478638) |  |
| AL2\_CO\_ESM#020 | Withdrawn |  |
| AL2\_CO\_ESM#030 | [Legal & Contractual compliance](#_Hlk221478677) |  |
| AL2\_CO\_ESM#040 | [Financial Provisions](#_Hlk221478683) |  |
| AL2\_CO\_ESM#050 | [Data Retention and Protection](#_Hlk230078526) |  |
| AL2\_CO\_ESM#055 | [Termination provisions](#_Hlk239696760) |  |
| AL2\_CO\_NUI#010 | [General Service Definition](#_Hlk221478708) |  |
| AL2\_CO\_NUI#020 | [Service Definition inclusions](#_Hlk221478719) |  |
| AL2\_CO\_NUI#030 | [Due notification](#_Hlk221478743) |  |
| AL2\_CO\_NUI#040 | [User Acceptance](#_Hlk221478752) |  |
| AL2\_CO\_NUI#050 | [Record of User Acceptance](#_Hlk221478780) |  |
| AL2\_CO\_NUI#060 | Withdrawn | No conformity requirement |
| AL2\_CO\_NUI#070 | [Change of Subscriber Information](#_Hlk221478795) |  |
| AL2\_CO\_NUI#080 | Withdrawn | No conformity requirement |
| AL2\_CO\_ISM#010 | [Documented policies and procedures](#_Hlk221478837) |  |
| AL2\_CO\_ISM#020 | [Policy Management and Responsibility](#_Hlk221478846)  |  |
| AL2\_CO\_ISM#030 | [Risk Management](#_Hlk221478854) |  |
| AL2\_CO\_ISM#040 | [Continuity of Operations Plan](#_Hlk221478903) |  |
| AL2\_CO\_ISM#050 | [Configuration Management](#_Hlk221478910) |  |
| AL2\_CO\_ISM#060 | [Quality Management](#_Hlk230078682) |  |
| AL2\_CO\_ISM#070 | [System Installation and Operation Controls](#_Hlk221478951) |  |
| AL2\_CO\_ISM#080 | [Internal Service Audit](#_Hlk221478959) |  |
| AL2\_CO\_ISM#090 | [Independent Audit](#_Hlk221478965) |  |
| AL2\_CO\_ISM#100 | [Audit Records](#_Hlk230078729) |  |
| AL2\_CO\_ISM#110 | Withdrawn | No conformity requirement |
| AL2\_CO\_SER#010 | [Security event logging](#_Hlk221489048) |  |
| AL2\_CO\_OPN#010 | [Technical security](#_Hlk221489089) |  |
| AL2\_CO\_OPN#020 | [Defined security roles](#_Hlk221489115) |  |
| AL2\_CO\_OPN#030 | [Personnel recruitment](#_Hlk221489129) |  |
| AL2\_CO\_OPN#040 | [Personnel skills](#_Hlk221489154) |  |
| AL2\_CO\_OPN#050 | [Adequacy of Personnel resources](#_Hlk221489306) |  |
| AL2\_CO\_OPN#060 | [Physical access control](#_Hlk221489312) |  |
| AL2\_CO\_OPN#070 | [Logical access control](#_Hlk221489318) |  |
| AL2\_CO\_ESC#010 | [Contracted policies and procedures](#_Hlk221489333) |  |
| AL2\_CO\_ESC#020 | [Visibility of contracted parties](#_Hlk221489382) |  |
| AL2\_CO\_SCO#010 | [Secure remote communications](#_Hlk221489390) |  |
| AL2\_CO\_SCO#015 | [Verification / Authentication confirmation messages](#_Hlk230431896) |  |
| AL2\_CO\_SCO#016 | [Verification of Revoked Credential](#_Hlk230431905) |  |
| AL2\_CO\_SCO#020 | [Limited access to shared secrets](#_Hlk221489398) |  |
| AL2\_CO\_SCO#030 | [Logical protection of shared secrets](#_Hlk230079201) |  |

Table 3-3. CO-SAC - AL3 compliance

| Clause | Description | Compliance |
| --- | --- | --- |
| AL3\_CO\_ESM#010 | [Established enterprise](#_Hlk221489445) |  |
| AL3\_CO\_ESM#020 | Withdrawn |  |
| AL3\_CO\_ESM#030 | [Legal & Contractual compliance](#_Hlk221489458) |  |
| AL3\_CO\_ESM#040 | [Financial Provisions](#_Hlk221489465) |  |
| AL3\_CO\_ESM#050 | [Data Retention and Protection](#_Hlk221489485) |  |
| AL3\_CO\_ESM#055 | [Termination provisions](#_Hlk239696831) |  |
| AL3\_CO\_ESM#060 | [Ownership](#_Hlk221489493) |  |
| AL3\_CO\_ESM#070 | [Independent management and operations](#_Hlk221489553) |  |
| AL3\_CO\_NUI#010 | [General Service Definition](#_Hlk221489627) |  |
| AL3\_CO\_NUI#020 | [Service Definition inclusions](#_Hlk221489661) |  |
| AL3\_CO\_NUI#030 | [Due notification](#_Hlk221489878) |  |
| AL3\_CO\_NUI#040 | [User Acceptance](#_Hlk221489883) |  |
| AL3\_CO\_NUI#050 | [Record of User Acceptance](#_Hlk221489892) |  |
| AL3\_CO\_NUI#060 | Withdrawn | No conformity requirement |
| AL3\_CO\_NUI#070 | [Change of Subscriber Information](#_Hlk230079419) |  |
| AL3\_CO\_NUI#080 | Withdrawn | No conformity requirement |
| AL3\_CO\_ISM#010 | [Documented policies and procedures](#_Hlk221489986) |  |
| AL3\_CO\_ISM#020 | [Policy Management and Responsibility](#_Hlk221490007) |  |
| AL3\_CO\_ISM#030 | [Risk Management](#_Hlk230079460) |  |
| AL3\_CO\_ISM#040 | [Continuity of Operations Plan](#_Hlk221490079) |  |
| AL3\_CO\_ISM#050 | [Configuration Management](#_Hlk221490095) |  |
| AL3\_CO\_ISM#060 | [Quality Management](#_Hlk221490108) |  |
| AL3\_CO\_ISM# 070 | [System Installation and Operation Controls](#_Hlk221490120) |  |
| AL3\_CO\_ISM#080 | [Internal Service Audit](#_Hlk221490135) |  |
| AL3\_CO\_ISM#090 | [Independent Audit](#_Hlk221490142) |  |
| AL3\_CO\_ISM#100 | [Audit Records](#_Hlk221490226) |  |
| AL3\_CO\_ISM#110 | Withdrawn | No conformity requirement |
| AL3\_CO\_ISM#120 | [Best Practice Security Management](#_Hlk221490243) |  |
| AL3\_CO\_SER#010 | [Security Event Logging](#_Hlk221490204) |  |
| AL3\_CO\_OPN#010 | [Technical security](#_Hlk221490280) |  |
| AL3\_CO\_OPN#020 | [Defined security roles](#_Hlk221490293) |  |
| AL3\_CO\_OPN#030 | [Personnel recruitment](#_Hlk221490332) |  |
| AL3\_CO\_OPN#040 | [Personnel skills](#_Hlk221490338) |  |
| AL3\_CO\_OPN#050 | [Adequacy of Personnel resources](#_Hlk221490351) |  |
| AL3\_CO\_OPN#060 | [Physical access control](#_Hlk221490369) |  |
| AL3\_CO\_OPN#070 | [Logical access control](#_Hlk221490378) |  |
| AL3\_CO\_ESC#010 | [Contracted policies and procedures](#_Hlk221490457) |  |
| AL3\_CO\_ESC#020 | [Visibility of contracted parties](#_Hlk221490465) |  |
| AL3\_CO\_SCO#010 | [Secure remote communications](#_Hlk221490427) |  |
| AL3\_CO\_SCO#020 | [Limited access to shared secrets](#_Hlk221490414) |  |

Table 3-4. CO-SAC - AL4 compliance

| Clause | Description | **Compliance** |
| --- | --- | --- |
| AL4\_CO\_ESM#010 | [Established enterprise](#_Hlk221490494) |  |
| AL4\_CO\_ESM#020 | Withdrawn |  |
| AL4\_CO\_ESM#030 | [Legal & Contractual compliance](#_Hlk221490522) |  |
| AL4\_CO\_ESM#040 | [Financial Provisions](#_Hlk221490609) |  |
| AL4\_CO\_ESM#050 | [Data Retention and Protection](#_Hlk221490592) |  |
| AL4\_CO\_ESM#055 | [Termination provisions](#_Hlk239696890) |  |
| AL4\_CO\_ESM#060 | [Ownership](#_Hlk221490581) |  |
| AL4\_CO\_ESM#070 | [Independent Management and Operations](#_Hlk221490627) |  |
| AL4\_CO\_NUI#010 | [General Service Definition](#_Hlk221490833) |  |
| AL4\_CO\_NUI#020 | [Service Definition inclusions](#_Hlk221490850) |  |
| AL4\_CO\_NUI#030 | [Due Notification](#_Hlk221490867) |  |
| AL4\_CO\_NUI#040 | [User Acceptance](#_Hlk221490875) |  |
| AL4\_CO\_NUI#050 | [Record of User Acceptance](#_Hlk221490989) |  |
| AL4\_CO\_NUI#060 | Withdrawn | No conformity requirement |
| AL4\_CO\_NUI#070 | [Change of Subscriber Information](#_Hlk221490973) |  |
| AL4\_CO\_NUI#080 | Withdrawn | No conformity requirement |
| AL4\_CO\_ISM#010 | [Documented policies and procedures](#_Hlk221491048) |  |
| AL4\_CO\_ISM#020 | [Policy Management and Responsibility](#_Hlk221491061) |  |
| AL4\_CO\_ISM#030 | [Risk Management](#_Hlk221491067) |  |
| AL4\_CO\_ISM#040 | [Continuity of Operations Plan](#_Hlk221491080) |  |
| AL4\_CO\_ISM#050 | [Configuration Management](#_Hlk221491088) |  |
| AL4\_CO\_ISM#060 | [Quality Management](#_Hlk221491098) |  |
| AL4\_CO\_ISM#070 | [System Installation and Operation Controls](#_Hlk221491133) |  |
| AL4\_CO\_ISM#080 | [Internal Service Audit](#_Hlk221491146) |  |
| AL4\_CO\_ISM#090 | [Independent Audit](#_Hlk221491157) |  |
| AL4\_CO\_ISM#100 | [Audit Records](#_Hlk221491163) |  |
| AL4\_CO\_ISM#110 | Withdrawn | No conformity requirement |
| AL4\_CO\_ISM#120 | [Best Practice Security Management](#_Hlk221491198) |  |
| AL4\_CO\_SER#010 | [Security Event Logging](#_Hlk221491213) |  |
| AL4\_CO\_OPN#010 | [Technical Security](#_Hlk221491241) |  |
| AL4\_CO\_OPN#020 | [Defined Security Roles](#_Hlk221491249) |  |
| AL4\_CO\_OPN#030 | [Personnel Recruitment](#_Hlk221491271) |  |
| AL4\_CO\_OPN#040 | [Personnel skills](#_Hlk230079814) |  |
| AL4\_CO\_OPN#050 | [Adequacy of Personnel resources](#_Hlk221489209) |  |
| AL4\_CO\_OPN#060 | [Physical access control](#_Hlk221489232) |  |
| AL4\_CO\_OPN#070 | [Logical access control](#_Hlk221489240) |  |
| AL4\_CO\_ESC#010 | [Contracted Policies and Procedures](#_Hlk221491364) |  |
| AL4\_CO\_ESC#020 | [Visibility of Contracted Parties](#_Hlk221491371) |  |
| AL4\_CO\_SCO#010 | [Secure remote communications](#_Hlk221491384) |  |
| AL4\_CO\_SCO#020 | [Limited access to shared secrets](#_Hlk221491394) |  |

# 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](#Section2). 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.

## Assurance Level 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.

#### Not used

No stipulation.

#### Security Controls

An enterprise and its specified service must:

AL1\_CM\_CTR#010 No stipulation

AL1\_CM\_CTR#020 Protocol threat risk assessment and controls

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

1. password guessing, such that there are at least 14 bits of entropy to resist an on-line guessing attack against a selected user/password;

[US / EZP800-63-2: §6.3.1.1.1 a), b), §6.3.1.1.2 a), c), d)]

1. message replay.

AL1\_CM\_CTR#025 No stipulation

AL1\_CM\_CTR#030 System threat risk assessment and controls

**MANDATORY**.

Account for the following system threats and apply appropriate controls:

1. the introduction of malicious code;
2. compromised authentication arising from insider action;
3. out-of-band attacks by other users and system operators (e.g., the ubiquitous shoulder-surfing);
4. spoofing of system elements/applications;
5. malfeasance on the part of Subscribers and Subjects.

#### Storage of Long-term Secrets

AL1\_CM\_STS#010 Withdrawn

Withdrawn (AL1\_CO\_SCO#020 (a) & (b) enforce this requirement)

####  Not used

#### Subject Options

AL1\_CM\_OPN#010 Withdrawn

Withdrawn – see AL1\_CM\_RNR#010.

### 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.

#### 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\_CM\_IDP#010 Withdrawn

Withdrawn.

AL1\_CM\_IDP#020 Withdrawn

Withdrawn.

AL1\_CM\_IDP#030 Withdrawn

Withdrawn.

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.

[US / EZP800-63-2: §5.3.1.1.5 a)]

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.

[US / EZP800-63-2: §5.3.1.1.5 a)]

#### Identity Verification

The enterprise or specific service:

AL1\_ID\_IDV#000 Identity Proofing classes

1. must include in its Service Definition at least one of the following classes of identity proofing service, and;
2. may offer any additional classes of identity proofing service it chooses, subject to the nature and the entitlement of the CSP concerned;
3. 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:
	1. §5.1.2.3, “[In-Person Public Identity Proofing](#_Ref76218312" \s "1,86151,86180,5,,In-Person Public Verification)”;
	2. §5.1.2.4, “[Remote Public Identity Proofing](#_Ref76218318" \s "1,87154,87180,5,,Remote Public Verification)”.

[US / EZP800-63-2: §5.3.5.1]

#### 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.

[US / EZP800-63-2: §5.3.1.1.5 c)]

AL1\_ID\_IPV#020 Evidence checks

Accept self-attestation of evidence.

[US / EZP800-63-2: §5.3.1.1.5 c)]

#### 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:

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

#### Not used

#### Not used

#### 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 the applicable class of identity proofing must also be observed.

AL1\_ID\_ROC#010 Authenticate Original Credential

Prior to issuing any derived credential the original credential on which the identity-proofing relies must be:

1. authenticated by a source trusted by the CSP as being valid and un-revoked;
2. no stipulation;
3. issued in the same name as that which the Applicant is claiming;
4. proven to be in the possession and under the control of the Applicant.

**Guidance**: This is the equivalent of recording the details of id documents provided during (e.g.) face-face id-proofing.

[US / EZP800-63-2: §5.3.5.3]

AL1\_ID\_ROC#020 Authenticate Original Credential

Record the details of the original credential and any biometric sample captured when authenticating it.

#### 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 any anomalous circumstances that can be reasonably anticipated (e.g., a legitimate and recent change of address that has yet to be established as the address of record).

#### Identity Verification Records

AL1\_CM\_IDP#040 Revision to Subscriber information

Provide a means for Subscribers and Subjects to amend their stored information after registration.

#### 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.

[US / EZP800-63-2: §5.3.1.1.5 a)]

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

* + 1. For a memorized secret, apply a rule-set such that there shall be a minimum of 14 bits of entropy in the pin or pass-phrase;
		 [US / EZP800-63-2: §6.3.1.1.1 a), b)]
		2. For a knowledge-based question, apply a rule-set such that there shall be:
			1. a minimum of 14 bits of entropy in the pin or pass-phrase OR;
			2. a set of knowledge-based questions created by the user OR;
			3. a set of knowledge-based questions selected by the user from a service-generated list of at least five questions.

			Note – null or empty answers in either case above shall not be permitted.
			 [US / EZP800-63-2: §6.3.1.1.2 a), c), d), e)]

**Only allow password tokens that have a resistance to online guessing attack against a selected user/password of at least 1 in 214 (16,384), accounting for state-of-the-art attack strategies, and at least 10 bits of min-entropy3.**

[US / EZP800-63-2: §6.3.1.1.1 a), b), d), f), g)]

#### Not used

#### Not used

#### Identity Verification Records

The specific service must be able to uniquely identify each Subscriber and their tokens/credentials and provide them to qualifying parties when so required.

An enterprise or specified service must:

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.**

[US / EZP800-63-2: §5.3.1.1.5 b)]

### 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.

#### 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.

### 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:

#### Not used

#### Not used

#### 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.

### 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.

#### 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.

### Part F - Credential Verification/Authentication

These criteria apply to credential validation and identity authentication.

#### 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:

1. requires authentication of the specified service or of the validation source;
2. ensures the integrity of the authentication assertion;
3. protects assertions against manufacture, modification and substitution, and secondary authenticators from manufacture;

and which, specifically:

1. creates assertions which are specific to a single transaction;
2. where assertion references are used, generates a new reference whenever a new assertion is created;
3. 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;
4. requires the secondary authenticator to:
	1. be signed when provided directly to Relying Party, or;
	2. have a minimum of 64 bits of entropy when provision is indirect (i.e. through the credential user).

AL1\_CM\_ASS#015 No stipulation

AL1\_CM\_ASS#020 No Post Authentication

*Not* authenticate credentials that have been revoked.

AL1\_CM\_ASS#030 Proof of Possession

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

AL1\_CM\_ASS#035 Limit authentication attempts (

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

[US / EZP800-63-2: §6.3.1.1.1 c), §6.3.1.1.2 b), f)]

AL1\_CM\_ASS#040 Assertion Lifetime

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

1. 12 hours after their creation, where the service shares a common internet domain with the Relying Party;
2. five minutes after their creation, where the service does not share a common internet domain with the Relying Party.

#### Authenticator-generated challenges

No stipulation.

#### Multi-factor authentication

No stipulation.

#### 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:

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 initial authentication of the Subject was made.

[US / EZP800-63-2: §9.3.2.0.1]

AL1\_CM\_VAS#040 Specify recipient

No stipulation.

AL1\_CM\_VAS#050 Specify recipient

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:

* + - 1. Signing the assertion;
			2. Encrypting the assertion using a secret key shared by with the RP;
			3. Creating an assertion reference which has a minimum of 64 bits of entropy;

[US / EZP800-63-2: §9.3.2.1.1, ’1.2]

* + - 1. Sending the assertion over a protected channel during a mutually-authenticated session.

[US / EZP800-63-2: §9.3.2.1.5]

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.

[US / EZP800-63-2: §9.3.2.1.3]

AL1\_CM\_VAS#090 Single-use assertion referencess

Limit to a single transaction the use of assertion references.

[US / EZP800-63-2: §9.3.2.1.4]

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.

[US / EZP800-63-2: §9.3.2.1.6]

AL1\_CM\_VAS#110 Assertion expiration

Set assertions to expire such that:

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

[US / EZP800-63-2: §9.3.2.1.7]

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

[US / EZP800-63-2: §9.3.2.1.8]

## Assurance Level 2

### 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.

#### 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:**

1. **if applicable, any OIDs related to the Practice and Policy Statement;**
2. **how users may subscribe to the service/apply for credentials and how users’ credentials will be delivered to them;**
3. **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);**
4. **how credentials may be renewed, modified, revoked, and suspended, including how requestors are authenticated or their identity re-proven;**
5. **what actions a Subject must take to terminate a subscription;**
6. **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.**

#### Security Controls

An enterprise and its specified service must:

AL2\_CM\_CTR#010 Secret revelation

**Withdrawn.**

AL2\_CM\_CTR#020 Protocol threat risk assessment and controls

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

1. password guessing, such that there are at least 24 bits of entropy to resist an on-line guessing attack against a selected user/password
 [US / EZP800-63-2: §56.3.1.2.1 a), b), §56.3.1.2.2 a), c), d), §8.3.2.2.3]
2. message replay**, showing that it is impractical**;
 [US / EZP800-63-2: §8.3.2.2.3]
3. **eavesdropping, showing that it is impractical;**
 [US / EZP800-63-2: §8.3.2.2.4]
4. **no stipulation;**
5. **man-in-the-middle attack;**
 [US / EZP800-63-2: §8.3.2.2.5]
6. **session hijacking.**
 [US / EZP800-63-2: §8.3.2.2.3]

AL2\_CM\_CTR#025 Permitted authentication protocols

**Permit only the following authentication protocols:**

1. **tunneled password;**
2. **zero knowledge-base password;**
3. **SAML assertions.**

AL2\_CM\_CTR#028 One-time passwords

**Use only one-time passwords which:**

1. **are generated using an approved block-cipher or hash function to combine a symmetric key, stored on the device, with a nonce;**
2. **derive the nonce from a date and time, or a counter generated on the device;**
3. **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**:

1. the introduction of malicious code;
2. compromised authentication arising from insider action;
3. out-of-band attacks by both users and system operators (e.g., the ubiquitous shoulder-surfing);
4. spoofing of system elements/applications;
5. malfeasance on the part of Subscribers and Subjects;
6. **intrusions leading to information theft.**

AL2\_CM\_CTR#040 Specified Service’s Key Management

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

1. **the physical security of the environment;**
2. **access control procedures limiting access to the minimum number of authorized personnel;**
3. **public-key publication mechanisms;**
4. **application of controls deemed necessary as a result of the service’s risk assessment;**
5. **destruction of expired or compromised private keys in a manner that prohibits their retrieval, or their archival in a manner that prohibits their reuse;**
6. **applicable cryptographic module security requirements, quoting FIPS 140‑2 [**[**FIPS140-2**](http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf)**] or equivalent, as established by a recognized national technical authority*.***

#### Storage of Long-term Secrets

AL2\_CM\_STS#010 Withdrawn

Withdrawn (AL2\_CO\_SCO#020 (a) & (b) enforce this requirement).

#### Security-Relevant Event (Audit) Records

#### No stipulation

AL2\_CM\_OPN#010 Withdrawn

Withdrawn – see AL2\_CM\_RNR#010.

### 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.

#### 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\_CM\_IDP#010 Withdrawn

Withdrawn.

AL2\_CM\_IDP#020 Withdrawn

Withdrawn.

AL2\_CM\_IDP#030 Withdrawn

Withdrawn

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.

[US / EZP800-63-2: §5.3.1.2.5 a)]

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.

[US / EZP800-63-2: §5.3.1.2.5 a)]

AL2\_ID\_POL#030 Published Proofing Policy

**Make available the Identity Proofing Policy under which it verifies the identity of applicants[[1]](#footnote-1) in form, language, and media accessible to the declared community of Users.**

[US / EZP800-63-2: §5.3.1.2.3]

AL2\_ID\_POL#040 Adherence to Proofing Policy

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

[US / EZP800-63-2: §5.3.1.2.3]

#### Identity Verification

The enterprise or specific service:

AL2\_ID\_IDV#000 Identity Proofing classes

1. **must include in its Service Definition at least one of the following classes of identity proofing service, and;**
2. **may offer any additional classes of identity proofing service it chooses, Subject to the nature and the entitlement of the CSP concerned;**
3. **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:**
	1. **§5.2.2.3, “**[**In-Person Public Identity** **Verification**](#_Ref76218312)**”;**
	2. **§5.2.2.4, “**[**Remote Public Identity Verification**](#_Ref76218318)**”;**

[US / EZP800-63-2: §5.3.1.2.10 (NOTE – only the above clauses align to this clause.)]

* 1. **§5.2.2.5, “**[**Current Relationship Identity Verification**](#_Toc90010627)**”;**
	2. **§5.2.2.6, “**[**Affiliation Identity Verification**](#_Toc90010628)**”;**

**athough, 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.**

[US / EZP800-63-2: §5.3.1.2.10, §5.3.5.1]

#### 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.**

[US / EZP800-63-2: §5.3.1.2.11 a, i)]

AL2\_ID\_IPV#020 Evidence checks

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

1. **appears to be a genuine document properly issued by the claimed issuing authority and valid at the time of application;**
2. **bears a photographic image of the holder that matches that of the applicant;**
3. **provides all reasonable certainty that the identity exists and that it uniquely identifies the applicant.**

[US / EZP800-63-2: §5.3.1.2.11 b, i)]

####  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 Picture ID document, and one of:**

1. **a second Government ID;**
2. **an employee or student ID number;**
3. **a financial account number (e.g., checking account, savings account, loan or credit card) or;**
4. **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:**

1. **a name that matches the referenced photo-ID;**
2. **date of birth and;**
3. **current address or personal telephone 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.**

[US / EZP800-63-2: §5.3.1.2.11 c)]

AL2\_ID\_RPV#020 Evidence checks

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

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

[US / EZP800-63-2: §5.3.1.2.11 d) i - iv)]

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

1. **RA sends notice to an address of record confirmed in the records check and receives a mailed or telephonic reply from applicant;**
2. **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;**
3. **RA issues credentials in a manner that confirms ability of the applicant to receive telephone communications at telephone number or email at email address associated with the applicant in records. Any secret sent over an unprotected channel shall be reset upon first use.** [US / EZP800-63-2: §5.3.1.2.11 d) vii)]

[US / EZP800-63-2: §5.3.1.2.11 d) vi)]

**Additional checks should 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 at least the same degree of certitude (See AL2\_ID\_SCV#010).**

#### 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]](#footnote-2).**

AL2\_ID\_CRV#020 Evidence checks

**Ensure that it has:**

1. **only issued the shared secret after originally establishing the applicant’s identity with a degree of rigor equivalent to that required under either the AL2 (or higher) requirements for in-person or remote public verification;**
2. **an ongoing business relationship sufficient to satisfy the enterprise of the applicant’s continued personal possession of the shared secret.**

#### 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**](#_Toc90010627)**”.**

AL2\_ID\_AFV#010 Required evidence

**Ensure that the applicant possesses:**

1. **identification from the organization with which it is claiming affiliation;**
2. **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:**

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

#### 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 the applicable class of identity proofing must also be observed.

AL2\_ID\_ROC#010 Authenticate Original Credential

Prior to issuing any derived credential the original credential on which the identity-proofing relies must be:

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

**Guidance**: This is the equivalent of recording the details of id documents provided during (e.g.) face-face id-proofing.

[US / EZP800-63-2: §5.3.5.2, ’5.3]

AL2\_ID\_ROC#020 Authenticate Original Credential

**Record the details of the original credential and any biometric sample captured when authenticating it.**

[US / EZP800-63-2: §5.3.5.6]

#### 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 any anomalous circumstances that can be reasonably anticipated (e.g., a legitimate and recent change of address that has yet to be established as the address of record).

[US / EZP800-63-2: §5.3.1.2.11 b) ii), d) iv), §5.3.1.2.12, §5.3.1.5.1, ’5.2]

#### 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.

An enterprise or specified service must:

AL2\_ID\_VRC#010 Verification Records for Personal Applicants

**Log, taking account of all applicable legislative and policy obligations, a record of the facts of the verification process, including a reference relating to the verification processes and the date and time of verification.**

[US / EZP800-63-2: §5.3.1.2.1]

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

AL2\_ID\_VRC#020 Verification Records for Affiliated Applicants

**In addition to the foregoing, log, taking account of all applicable legislative and policy obligations, a record of the additional facts of the verification process must be performed. At a minimum, records of identity information must include:**

1. **the Subject’s[[3]](#footnote-3) full name;**
2. **the Subject’s current address of record;**
3. **the Subject’s current telephone or email address of record;**
4. **the Subscriber’s acknowledgement for issuing the Subject with a credential;**
5. **type, issuing authority, and reference number(s) of all documents checked in the identity proofing process.**

[US / EZP800-63-2: §5.3.1.2.1]

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.**

[US / EZP800-63-2: §5.3.1.2.2; §5.3.1.2.5 b)]

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.**

[US / EZP800-63-2: §5.3.1.2.1]

AL2\_CM\_IDP#040 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**.

#### 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.**

[US / EZP800-63-2: §5.3.1.2.5 a)]

**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.

[US / EZP800-63-2: §5.3.1.2.5 a)]

AL2\_CM\_CRN#035 Convey credential

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

[US / EZP800-63-2: §5.3.1.2.5 b)]

AL2\_CM\_CRN#040 Token strength

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

1. For a memorized secret, apply a rule-set such that there shall be a minimum of **24** bits of entropy in the pin or pass-phrase;
 [US / EZP800-63-2: §6.3.1.2.1 a), b)]
2. For a knowledge-based question, apply a rule-set such that there shall be:
3. a minimum of **20** bits of entropy in the pin or pass-phrase OR;
4. a set of knowledge-based questions created by the user OR;
5. a set of knowledge-based questions selected by the user from a service-generated list of at least **seven** questions.
 [US / EZP800-63-2: §6.3.1.2.2 a), c), d), e)]

Note – null or empty answers in either case above shall not be permitted.
6. **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);**
 [US / EZP800-63-2: §6.3.1.2.3 a), c)]
7. **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;**
 [US / EZP800-63-2: §6.3.1.2.4 a)]
8. **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;**
 [US / EZP800-63-2: §6.3.1.2.5 a), b)]
9. **Use a cryptographic device validated at FIPS 140-2 Level 1 or higher.**
 [US / EZP800-63-2: §6.3.1.2.6 a)]

**.**

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 214 (16,384), accounting for state-of-the-art attack strategies, and at least 10 bits of min-entropy3.**

[US / EZP800-63-2: §6.3.1.2.1 a), b), §6.3.1.2.2 a), c), d)]

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.**

[US / EZP800-63-2: §6.3.1.2.5 c)]

AL2\_CM\_CRN#060 Software cryptographic token strength

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

1. **are protected by a key and cryptographic protocol that are evaluated against FIPS 140-2 [**[**FIPS140-2**](http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf)**] Level 2, or equivalent, as established by a recognized national technical authority.**

[**Omitted**]

[US / EZP800-63-2: §6.3.1.2.6 e)]

AL2\_CM\_CRN#070 Hardware token strength

**Ensure that hardware tokens used to store cryptographic keys:**

1. **employ a cryptographic module that is evaluated against FIPS 140-2 [**[**FIPS140-2**](http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf)**] Level 1 or higher, or equivalent, as established by a recognized national technical authority.**

[**Omitted**]

[US / EZP800-63-2: §6.3.1.2.5 d)]

AL2\_CM\_CRN#080 No stipulation

AL2\_CM\_CRN#090 Nature of Subject

**Record the nature of the Subject of the credential (which must correspond to the manner of identity proofing performed), i.e., physical person, a named person acting on behalf of a corporation or other legal entity, corporation or legal entity, or corporate machine entity, in a manner that can be unequivocally associated with the credential and the identity that it asserts. If the credential is based upon a pseudonym this must be indicated in the credential.**

[US / EZP800-63-2: §5.3.1.2.6, ’.7]

#### Subject Key Pair Generation

No stipulation.

#### 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 informationby:**

* 1. **sending notice to the address of record confirmed during identity proofing or;**
	2. **issuing the credential(s) in a manner that confirms the address of record supplied by the applicant during identity proofing or;**
	3. **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.**

[US / EZP800-63-2: §5.3.1.2.11 b) iii)]

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:**

1. **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;**
2. **through the use of a biometric that was recorded during a prior encounter.**

[US / EZP800-63-2: §5.3.1.6.2 b) i)]

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.**

[US / EZP800-63-2: §5.3.1.2.11 b) iv), §5.3.1.6.2 b) ii)]

### 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.

#### 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.**

[US / EZP800-63-2: §7.3.1.2 c) ii)]

AL2\_CM\_RNR#030 Renewal/Re-issuance limitations

* 1. **not renew but may re-issue Passwords;**
	2. **neither renew nor re-issue expired tokens;**
	3. **neither set to default nor re-use any token secrets;**

[US / EZP800-63-2: §7.3.1.2 c) iii)]

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

[US / EZP800-63-2: §7.3.1.2 c) iv)]

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

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 7.5 years.**

[US / EZP800-63-2: §7.3.1.2 e) ii)]

### Part D - Credential Revocation

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

#### 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

1. **State the conditions under which revocation of an issued credential may occur;**
2. **State the processes by which a revocation request may be submitted;**
3. **State the persons and organizations from which a revocation request will be accepted;**
4. **State the validation steps that will be applied to ensure the validity (identity) of the Revocant, and;**
5. **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.**

[US / EZP800-63-2: §7.3.1.2 d)]

AL2\_CM\_RVP#040 Verify revocation identity

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

AL2\_CM\_RVP#050 Revocation Records

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

1. **the Revocant’s full name;**
2. **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);**
3. **the Credential Issuer’s identity (if not directly responsible for the identity proofing service);**
4. **the identity associated with the credential (whether the Subject’s name or a pseudonym);**
5. **the reason for revocation.**

[US / EZP800-63-2: §7.3.1.2 e) i)]

AL2\_CM\_RVP#060 Record Retention

**Retain, securely, the record of the revocation process** **for the duration of the Subscriber’s account plus 7.5 years.**

[US / EZP800-63-2: §7.3.1.2 e) ii)]

#### 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:**

1. **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;**
2. **if remote:**
	* + 1. **electronically verify a signature against records (if available), confirmed with a call to a telephone number of record, or;**
			2. **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:**

* + 1. **from the specified service itself, with authorization as determined by established procedures, or;**
		2. **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:**

1. **if in-person, verify the identity of the person presenting the request;**
2. **if remote:**
	* + 1. **in paper/facsimile form, verify the origin of the legal document by a database check or by telephone with the issuing authority, or;**
			2. **as an electronic request, authenticate it as being from a recognized legal office, supported by a credential at Assurance Level 2 or higher.**

#### 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.

### 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.

#### 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.

[US / EZP800-63-2: §7.3.1.2 e) i)]

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:**

1. **the requesting source as one from which the specified service expects to receive such requests;**
2. **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.**

### Part F - Credential Verification/Authentication

These criteria apply to credential validation and identity authentication.

#### 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:

1. requires authentication of the specified service, itself, or of the validation source;
2. ensures the integrity of the authentication assertion;
3. protects assertions against manufacture, modification**, substitution and disclosure**, and secondary authenticators from manufacture**, capture and replay**;
4. **uses approved cryptography techniques;**

and which, specifically:

1. creates assertions which are specific to a single transaction;
2. where assertion references are used, generates a new reference whenever a new assertion is created;
3. 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;
4. **send assertions either via a channel mutually-authenticated with the Relying Party, or signed and encrypted for the Relying Party;**
5. requires the secondary authenticator to:
	1. be signed when provided directly to Relying Party, or;
	2. have a minimum of 64 bits of entropy when provision is indirect (i.e. through the credential user);
	3. **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;**
	4. **not be subsequently transmitted over an unprotected channel or to an unauthenticated party while it remains valid**.

[US / EZP800-63-2: §8.3.2.2.7]

AL2\_CM\_ASS#015 No False Authentication

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

AL2\_CM\_ASS#020 No Post Authentication

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

[US / EZP800-63-2: §8.3.2.2.2]

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.

[US / EZP800-63-2: §6.3.1.2.1 c), §6.3.1.2.2 b), f) , §6.3.1.2.3 b), d) , §6.3.1.2.4 d)]

AL2\_CM\_ASS#040 Assertion Lifetime

Generate assertions so as to indicate and effect their expiration:

1. 12 hours after their creation, where the service shares a common internet domain with the Relying Party;
2. five minutes after their creation, where the service does not share a common internet domain with the Relying Party.

#### 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.**

[US / EZP800-63-2: §6.3.1.2.4 b), c), §6.3.1.2.6 f)]

#### 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.**

[US / EZP800-63-2: §6.3.1.2]

#### 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.

[US / EZP800-63-2: §9.3.2.0.1]

AL2\_CM\_VAS#040 Notify pseudonyms

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

[US / EZP800-63-2: §9.3.2.2.1]

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.**

[US / EZP800-63-2: §9.3.2.2.3]

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:

1. Signing the assertion;
2. Encrypting the assertion using a secret key shared by with the RP;

[US / EZP800-63-2: §9.3.2.2.8]

1. Creating an assertion reference which has a minimum of 64 bits of entropy;

[US / EZP800-63-2: §9.3.2.1.1, ’1.2]

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

[US / EZP800-63-2: §9.3.2.1.5]

AL2\_CM\_VAS#070 Assertion protections

**Provide protection of assertion-related data such that:**

1. **both assertions and assertion references are protected against capture and re-use;**
2. **assertions are also protected against redirection;**

[US / EZP800-63-2: §9.3.2.2.2]

1. **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).**

[US / EZP800-63-2: §9.3.2.2.5, 2.6, ’2.7’]

AL2\_CM\_VAS#080 Single-use assertions

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

[US / EZP800-63-2: §9.3.2.1.3]

AL2\_CM\_VAS#090 Single-use assertion referencess

Limit to a single transaction the use of assertion references.

[US / EZP800-63-2: §9.3.2.1.4]

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.

[US / EZP800-63-2: §9.3.2.1.6]

AL2\_CM\_VAS#110 Assertion expiration

Set assertions to expire such that:

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

[US / EZP800-63-2: §9.3.2.1.7]

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

[US / EZP800-63-2: §9.3.2.1.8]

## Assurance Level 3

### 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.

#### 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:

1. if applicable, any OIDs related to the Credential Policy and Practice Statement;
2. how users may subscribe to the service/apply for credentials and how the users’ credentials will be delivered to them;
3. 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);
4. how credentials may be renewed, modified, revoked, and suspended, including how requestors are authenticated or their identity proven;
5. what actions a Subscriber or Subject must take to terminate a subscription;
6. 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.

#### Security Controls

AL3\_CM\_CTR#010 No stipulation

AL3\_CM\_CTR#020 Protocol threat risk assessment and controls

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

1. password guessing, such that the resistance to an on-line guessing attack against a selected user/password is at least 1 in 214 (16,384);
 [US / EZP800-63-2: §8.3.2.3.5]
2. message replay, showing that it is impractical;
3. eavesdropping, showing that it is impractical;
4. **relying party (verifier) impersonation, showing that it is impractical;**
5. man-in-the-middle attack;
6. **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.**

AL3\_CM\_CTR#025 Permitted authentication protocols

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

1. tunneled password;
2. zero knowledge-base password;
3. SAML assertions.

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:

1. the introduction of malicious code;
2. compromised authentication arising from insider action;
3. out-of-band attacks by both users and system operators (e.g., shoulder-surfing);
4. spoofing of system elements/applications;
5. malfeasance on the part of Subscribers and Subjects;
6. intrusions leading to information theft.

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

AL3\_CM\_CTR#040 Specified Service’s Key Management

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

1. the physical security of the environment;
2. access control procedures limiting access to the minimum number of authorized personnel;
3. public-key publication mechanisms;
4. application of controls deemed necessary as a result of the service’s risk assessment;
5. destruction of expired or compromised private keys in a manner that prohibits their retrieval or their archival in a manner that prohibits their reuse;
6. applicable cryptographic module security requirements, quoting FIPS 140-2 [[FIPS140-2](http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf)] or equivalent, as established by a recognized national technical authority.

#### 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:**

1. **the encryption key for the shared secret file is encrypted under a key held in a FIPS 140-2 [**[**FIPS140-2**](http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf)**] 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;**
2. **the shared secret file is decrypted only as immediately required for an authentication operation;**
3. **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;**
4. **shared secrets are split by an "*n from m*" cryptographic secret sharing method.**

#### 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:

1. the identity of the point of registration (irrespective of whether internal or outsourced);
2. generation of the Subject’s keys or the evidence that the Subject was in possession of both parts of their own key-pair;
3. generation of the Subject’s certificate;
4. dissemination of the Subject’s certificate;
5. any revocation or suspension associated with the Subject’s certificate.

#### Subject options

AL3\_CM\_OPN#010 Changeable PIN/Password

Withdrawn – see AL3\_CM\_RNR#010.

### 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.

#### 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\_CM\_IDP#010 Withdrawn

Withdrawn.

AL3\_CM\_IDP#020 Withdrawn

Withdrawn.

AL3\_CM\_IDP#030 Withdrawn

Withdrawn**.**

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.

[US / EZP800-63-2: §5.3.1.3.5 a)]

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.

[US / EZP800-63-2: §5.3.1.3.5 a)]

AL3\_ID\_POL#030 Published Proofing Policy

Make available the Identity Proofing Policy under which it verifies the identity of applicants[[4]](#footnote-5) in form, language, and media accessible to the declared community of Users.

[US / EZP800-63-2: §5.3.1.3.3]

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**.

[US / EZP800-63-2: §5.3.1.3.3]

#### Identity Proofing

The enterprise or specific service:

AL3\_ID\_IDV#000 Identity Proofing classes

1. must include in its Service Definition at least one of the following classes of identity proofing services, and;
2. may offer any additional classes of identity proofing service it chooses, Subject to the nature and the entitlement of the CSP concerned;
3. 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:
4. **§5.3.2.3, “[In-Person Public](#_Toc90010635" \s "1,97106,97135,5,,In-Person Public Verification)****[Identity Verification](#_Toc90010635" \s "1,97106,97135,5,,In-Person Public Verification)”;**
5. **§5.3.2.4, “[Remote Public Identity Verification](#_Toc90010636" \s "1,98263,98289,5,,Remote Public Verification)”;**

[US / EZP800-63-2: §5.3.1.3.10 (NOTE – only the above clauses align to this clause.)]

1. **§5.3.2.6, “[Affiliation Identity Verification](#_Toc90010637" \s "1,100946,100970,5,,Affiliation Verification)”.**

[US / EZP800-63-2: §5.3.5.1]

#### 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.

[US / EZP800-63-2: §5.3.1.3.11 a, ii)]

AL3\_ID\_IPV#020 Evidence checks

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

1. appears to be a genuine document properly issued by the claimed issuing authority and valid at the time of application;
2. bears a photographic image of the holder that matches that of the applicant;
3. **is electronically verified by a record check with the specified issuing authority or through similar databases that:**
4. **establishes the existence of such records with matching name and reference numbers;**
5. **corroborates date of birth, current address of record, and other personal information sufficient to ensure a unique identity;**
6. provides all reasonable certainty that the identity exists and that it uniquely identifies the applicant.

[US / EZP800-63-2: §5.3.1.3.8, §5.3.1.3.11 b, ii)]]

#### 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 Picture ID document, and one of:

a) a second Government ID;

b) an employee or student ID number;

c) a financial account number (e.g., checking account, savings account, loan, or credit card), or;

d) a utility service account number (e.g., electricity, gas, or water) for an address matching that in the primary document.

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

e) a name that matches the referenced photo-ID;

f) date of birth;

g) current address or personal telephone 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.

[US / EZP800-63-2: §5.3.1.3.11 c)]

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:

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

[US / EZP800-63-2: §5.3.1.3.8, §5.3.1.3.11 d) i - iii)]

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

1. RA sends notice to an address of record confirmed in the records check and receives a mailed or telephonic reply from applicant;
2. 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;
3. RA issues credentials in a manner that confirms ability of the applicant to receive telephone communications at telephone number or email at email address associated with the applicant in records. Any secret sent over an unprotected channel shall be reset upon first use.

[US / EZP800-63-2: §5.3.1.3.8, §5.3.1.3.11 d) v)]

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

#### Current Relationship Identity Proofing

No stipulation.

#### 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**](#_Toc90010636)”.

AL3\_ID\_AFV#010 Required evidence

Ensure that the applicant possesses:

1. identification from the organization with which it is claiming affiliation;
2. 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 whichensure that the presented documents:

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

[US / EZP800-63-2: §5.3.1.3.8]

#### 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 the applicable class of identity proofing must also be observed.

AL3\_ID\_ROC#010 Authenticate Original Credential

Prior to issuing any derived credential the original credential on which the identity-proofing relies must be:

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

**Guidance**: This is the equivalent of recording the details of id documents provided during (e.g.) face-face id-proofing.

[US / EZP800-63-2: §5.3.5.2, ’5.3]

AL3\_ID\_ROC#020 Authenticate Original Credential

Record the details of the original credential.

[US / EZP800-63-2: §5.3.5.6]

#### 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 any anomalous circumstance that can reasonably be anticipated (e.g., a legitimate and recent change of address that has yet to be established as the address of record).

[US / EZP800-63-2: §5.3.1.3.11 d) i – iv), §5.3.1.3.12, §5.3.1.5.3, ’5.4]

#### 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 and the date and time of verification.

[US / EZP800-63-2: §5.3.1.3.1]

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

AL3\_ID\_VRC#020 Verification Records for Affiliated Applicants

In addition to the foregoing, log, taking account of all applicable legislative and policy obligations, a record of the additional facts of the verification process must be performed. At a minimum, records of identity information must include:

1. the ‘full name;
2. the Subject’s[[5]](#footnote-6) current address of record;
3. the Subject’s current telephone or email address of record;
4. the Subject’s acknowledgement of issuing the Subject with a credential;
5. type, issuing authority, and reference number(s) of all documents checked in the identity proofing process;
6. **where required, a telephone or email address for related contact and/or delivery of credentials/notifications.**

[US / EZP800-63-2: §5.3.1.3.1]

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.

[US / EZP800-63-2: §5.3.1.3.2; §5.3.1.3.5 b)]

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.

[US / EZP800-63-2: §5.3.1.3.1, §7.3.1.3 e) ii)]

AL3\_CM\_IDP#040 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, where necessary, instigate the re-issuance of the credential.**

#### 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.

[US / EZP800-63-2: §5.3.1.3.5 a)]

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.

[US / EZP800-63-2: §5.3.1.3.5 a)]

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.

[US / EZP800-63-2: §5.3.1.3.5 a)]

AL3\_CM\_CRN#035 Convey credential

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

[US / EZP800-63-2: §5.3.1.3.5 b)]

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:

1. **depend on a symmetric key stored on a personal hardware device evaluated against FIPS 140-2 [**[**FIPS140-2**](http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf)**] Level 1 or higher, or equivalent, as established by a recognized national technical authority;**
2. **permit at least 106 possible password values;**
3. **require password or biometric activation by the Subject.**

AL3\_CM\_CRN#060 Software cryptographic token strength

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

1. are protected by a key and cryptographic protocol that are evaluated against FIPS 14-2 [[FIPS140-2](http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf)] Level 2, or equivalent, as established by a recognized national technical authority;
2. **require password or biometric activation by the Subject or employ a password protocol when being used for authentication;**
3. **erase any unencrypted copy of the authentication key after each authentication.**

[US / EZP800-63-2: §6.3.1.3.1 a)]

AL3\_CM\_CRN#070 Hardware token strength

Ensure that hardware tokens used to store cryptographic keys:

1. employ a cryptographic module that is evaluated against FIPS 140-2 [[FIPS140-2](http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf)] Level 1 or higher, or equivalent, as established by a recognized national technical authority;
2. **require password or biometric activation by the Subject or also employ a password when being used for authentication;**
3. **erase any unencrypted copy of the authentication key after each authentication.**

AL3\_CM\_CRN#080 Binding of key

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

AL3\_CM\_CRN#090 Nature of Subject

Record the nature of the Subject of the credential (which must correspond to the manner of identity proofing performed), i.e., private person, a named person acting on behalf of a corporation or other legal entity, corporation or legal entity, or corporate machine entity, in a manner that can be unequivocally associated with the credential and the identity that it asserts. **[Omitted]**

#### 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:**

1. **use a FIPS 140-2 [**[**FIPS140-2**](http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf)**] compliant algorithm, or equivalent, as established by a recognized national technical authority, that is recognized as being fit for the purposes of the service;**
2. **only create keys of a key length and for use with a FIPS 140-2 [**[**FIPS140-2**](http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf)**] compliant public key algorithm, or equivalent, as established by a recognized national technical authority, recognized as being fit for the purposes of the service;**
3. **generate and store the keys securely until delivery to and acceptance by the Subject;**
4. **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:**

1. **used a FIPS 140-2 [**[**FIPS140-2**](http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf)**] compliant algorithm, or equivalent, as established by a recognized national technical authority, that is recognized as being fit for the purposes of the service;**
2. **created keys of a key length and for use with a FIPS 140-2 [**[**FIPS140-2**](http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf)**] compliant public key algorithm, or equivalent, as established by a recognized national technical authority, recognized as being fit for the purposes of the service.**

#### 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 informationby:

1. sending notice to the address of record confirmed during identity proofing**, and either:**
2. **issuing the credential(s) in a manner that confirms the address of record supplied by the applicant during identity proofing, or;**
3. **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.**

[US / EZP800-63-2: §5.3.1.3.11 b) iii)]

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:

1. 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;
2. through the use of a biometric that was recorded during a prior encounter.

[US / EZP800-63-2: §5.3.1.6.2 c) i)]

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.

[US / EZP800-63-2: §5.3.1.6.2 c) iii)]

AL3\_CM\_CRD#017 Protected Issuance of Permanent Secrets (in person)

**Only issue permanent secrets if the CSP has:**

1. **loaded the secret itself onto the physical device, which was either:**
	1. **issued in-person to the Applicant, or;**
	2. **delivered in a manner that confirms the address of record.**

[US / EZP800-63-2: §5.3.1.6.2 c) ii)]

AL3\_CM\_CRD#018 Protected Issuance of Permanent Secrets (remotely)

**Only issue permanent secrets within a protected session.**

[US / EZP800-63-2: §5.3.1.6.2 c) iv)]

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).**

### 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.

#### 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.

[US / EZP800-63-2: §7.3.1.3 c) i)]

AL3\_CM\_RNR#030 Renewal/Re-issuance limitations

1. **No stipulation**;
2. **No stipulation**;
3. **No stipulation**;
4. conduct all renewal / re-issuance interactions with the Subject over a protected channel such as SSL/TLS.
 [US / EZP800-63-2: §7.3.1.3 c) ii)]

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

AL3\_CM\_RNR#040 Authentication key life

**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 7.5 years.

[US / EZP800-63-2: §7.3.1.3 e) ii)]

### Part D - Credential Revocation

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

#### 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

1. State the conditions under which revocation of an issued credential may occur;
2. State the processes by which a revocation request may be submitted;
3. State the persons and organizations from which a revocation request will be accepted;
4. State the validation steps that will be applied to ensure the validity (identity) of the Revocant, and;
5. 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.**

[US / EZP800-63-2: §7.3.1.3 d i)]

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:

1. the Revocant’s full name;
2. 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);
3. the Credential Issuer’s identity (if not directly responsible for the identity proofing service);
4. the reason for revocation.

AL3\_CM\_RVP#060 Record Retention

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

1. **the records retention policy required by AL3\_CM\_CPP#020, and;**
2. **applicable legislation;**

**and which, in addition, must be not less than** the duration of the Subscriber’s account plus 7.5 years.

[US / EZP800-63-2: §7.3.1.3 e) ii & iii)]

#### 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:

1. if in-person, require presentation of a primary Government Picture ID document that shall be electronicallyverified by a record check against the provided identity with the specified issuing authority’s records;
2. if remote:
	* + 1. electronicallyverify a signature against records (if available), confirmed with a call to a telephone number of record, or;
			2. 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:

1. from the specified service itself, with authorization as determined by established procedures, or;
2. 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:

1. if in person, verify the identity of the person presenting the request, or;
2. if remote:
	* + 1. in paper/facsimile form, verify the origin of the legal document by a database check or by telephone with the issuing authority, or;
			2. as an electronic request, authenticate it as being from a recognized legal office**,** supported by a credential at Assurance Level **3** or higher.

#### 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.

### 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.

#### 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.

[US / EZP800-63-2: §7.3.1.3 e) i)]

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:

1. the requesting source as one from which the specified service expects to receive such requests;
2. 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.

### Part F - Credential Verification/Authentication

These criteria apply to credential validation and identity authentication.

#### 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:

1. requires authentication of the specified service, itself, or of the validation source;
2. ensures the integrity of the authentication assertion.

[US / EZP800-63-2: §7.3.1.3 b) i)]

AL3\_CM\_ASS#015 No False Authentication

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

[US / EZP800-63-2: §7.3.1.3 b) i)]

AL3\_CM\_ASS#018 Ensure token validity

**Ensure that tokens are either still valid or have been issued within the last 24 hours.**

[US / EZP800-63-2: §7.3.1.3 d) iii)]

**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 publicisied (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 No stipulation

*Note – merely following NIST guidance ... but why not here as well?*

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**.

#### 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.

[US / EZP800-63-2: §6.3.1.3.1 b)]

AL3\_CM\_AGC#020 No stipulation

No stipulation.

#### 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.

[US / EZP800-63-2: §6.3.1.2, §8.3.2.3.1]

#### 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.

[US / EZP800-63-2: §9.3.2.0.1]

AL3\_CM\_VAS#040 No pseudonyms

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

[US / EZP800-63-2: §9.3.2.3.3]

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.

[US / EZP800-63-2: §9.3.2.2.3]

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:

1. Signing the assertion;

[US / EZP800-63-2: §9.3.2.3.2]

1. Encrypting the assertion using a secret key shared by with the RP;

[US / EZP800-63-2: §9.3.2.2.8]

1. Creating an assertion reference which has a minimum of 64 bits of entropy;

[US / EZP800-63-2: §9.3.2.1.1, ’1.2]

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

[US / EZP800-63-2: §9.3.2.1.5]

AL3\_CM\_VAS#070 Assertion protections

Provide protection of assertion-related data such that:

1. both assertions and assertion references are protected against capture and re-use;
2. assertions are also protected against redirection;

[US / EZP800-63-2: §9.3.2.2.2]

1. 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).

[US / EZP800-63-2: §9.3.2.2.5, 2.6, ’2.7’]

AL3\_CM\_VAS#080 Single-use assertions

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

[US / EZP800-63-2: §9.3.2.1.3]

AL3\_CM\_VAS#090 Single-use assertion referencess

Limit to a single transaction the use of assertion references.

[US / EZP800-63-2: §9.3.2.1.4]

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.

[US / EZP800-63-2: §9.3.2.1.6]

AL3\_CM\_VAS#110 Assertion expiration

Set assertions to expire such that:

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

[US / EZP800-63-2: §9.3.2.3.6]

1. those used within a single internet domain become invalid **30 minutes** after their creation (including assertions contained in or referenced by cookies).

[US / EZP800-63-2: §9.3.2.3.5]

AL3\_CM\_VAS#120 SSO provisions

**If SSO is supported [*Note -* *800-63 says ‘may’*], provide a re-authentication of the Subject so long as:**

1. **The Subject has been successfully authenticated within the last 12 hours;**
2. **The Subject remains able to demonstrate that they were the party that was previously authenticated;**
3. **It can be ensured that the Subscriber has not been inactive for more than 30 minutes.**

[US / EZP800-63-2: §9.3.2.3.7]

## Assurance Level 4

### 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.

#### 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**](#RFC3647)**] 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:**

1. **applicable OIDs for each certificate type issued;**
2. **how users may subscribe to the service/apply for certificates, and how certificates will be issued to them;**
3. **if users present their own keys, how they will be required to demonstrate possession of the private key;**
4. **if users’ keys are generated for them, how the private keys will be delivered to them;**
5. **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);**
6. **how certificates may be renewed, re-keyed, modified, revoked, and suspended, including how requestors are authenticated or their identity proven;**
7. **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.

#### Security Controls

An enterprise and its specified service must:

AL4\_CM\_CTR#010 No stipulation

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:

1. password guessing, **showing that there is sufficient entropy**;
2. message replay, showing that it is impractical;
3. eavesdropping, showing that it is impractical;
4. relying party (verifier) impersonation, showing that it is impractical;
5. man-in-the-middle attack, showing that it is impractical;
 [US / EZP800-63-2: §8.3.2.4.6]
6. **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.

AL4\_CM\_CTR#025 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:

1. the introduction of malicious code;
 [US / EZP800-63-2: §8.3.2.4.2]
2. compromised authentication arising from insider action;
3. out-of-band attacks by both users and system operators (e.g., shoulder-surfing);
4. spoofing of system elements/applications;
5. malfeasance on the part of Subscribers and Subjects;
6. 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.

[US / EZP800-63-2: §8.3.2.4.2]

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:

1. the physical security of the environment;
2. access control procedures limiting access to the minimum number of authorized personnel;
3. public-key publication mechanisms;
4. application of controls deemed necessary as a result of the service’s risk assessment;
5. destruction of expired or compromised private keys in a manner that prohibits their retrieval, or their archival in a manner which prohibits their reuse;
6. applicable cryptographic module security requirements, quoting FIPS 140-2 [[FIPS140-2](http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf)] or equivalent, as established by a recognized national technical authority.

#### Storage of Long-term Secrets

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

AL4\_CM\_STS#010 Stored Secrets

**a)** Withdrawn(AL4\_CO\_SCO#020 (a) & (b) enforce this requirement)

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

AL4\_CM\_STS#020 Stored Secret Encryption

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

1. the encryption key for the **[omitted]** secret file is encrypted under a key held in a FIPS 140‑2 [[FIPS140-2](http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf)] 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;
2. the **[omitted]** secret file is decrypted only as immediately required for a key recovery operation;
3. **[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;
4. escrowed secrets are split by an "*n from m*" cryptographic secret **storing** method.

#### 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:

1. the identity of the point of registration (irrespective of whether internal or outsourced);
2. generation of the Subject’s keys or evidence that the Subject was in possession of both parts of the key-pair;
3. generation of the Subject’s certificate;
4. dissemination of the Subject’s certificate;
5. any revocation or suspension associated with the Subject’s credential.

#### Subject Options

AL4\_CM\_OPN#010 Changeable PIN/Password

Withdrawn – see AL4\_CM\_RNR#010.

### 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.

#### 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\_CM\_IDP#010 Withdrawn

Withdrawn.

AL4\_CM\_IDP#020 Withdrawn

Withdrawn.

AL4\_CM\_IDP#030 Withdrawn

Withdrawn.

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.

[US / EZP800-63-2: §5.3.1.4.5 a)]

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.[US / EZP800-63-2: §5.3.1.4.5 a)]

AL4\_ID\_POL#030 Published Proofing Policy

Make available the Identity Proofing Policy under which it verifies the identity of applicants[[6]](#footnote-7) in form, language, and media accessible to the declared community of users.

[US / EZP800-63-2: §5.3.1.4.3]

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.

[US / EZP800-63-2: §5.3.1.4.3]

#### 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**;

[US / EZP800-63-2: §5.3.1.4.10, §5.3.5.1]

The enterprise or specified service must:

#### In-Person Public Identity Proofing

AL4\_ID\_IPV#010 Required evidence

Ensure that the applicant is in possession of:

1. a primary Government Picture ID document that bears a photographic image of the **holder and either:**
2. **secondary Government Picture ID or an account number issued by a regulated financial institution or;**
3. **two items confirming name, and address or telephone number, such as: utility bill, professional license or membership, or other evidence of equivalent standing.**

[US / EZP800-63-2: §5.3.1.411]

AL4\_ID\_IPV#020 No stipulation

AL4\_ID\_IPV#030 Evidence checks – primary ID

**Ensure that the presented document:**

1. **appears to be a genuine document properly issued by the claimed issuing authority and valid at the time of application;**
2. **bears a photographic image of the holder which matches that of the applicant;**
3. **is electronically verified by a record check with the specified issuing authority or through similar databases that:**
	1. **establishes the existence of such records with matching name and reference numbers;**
	2. **corroborates date of birth, current address of record, and other personal information sufficient to ensure a unique identity;**
4. **provides all reasonable certainty, at AL4, that the identity exists and that it uniquely identifies the applicant.**

[US / EZP800-63-2: §5.1.4.11 b) i - iv)]]

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:**

1. **appears to be a genuine document properly issued by the claimed issuing authority and valid at the time of application;**
2. **bears a photographic image of the holder which matches that of the applicant;**
3. **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:**

* 1. **establishes the existence of such records with matching name and reference numbers;**
	2. **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:**

1. **each appears to be a genuine document properly issued by the claimed issuing authority;**
2. **corroborates current address of record or telephone number sufficient to ensure a unique identity.**

[US / EZP800-63-2: §5.1.4.11 b) iv)]]

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.**

#### Remote Public Identity Proofing

**Not permitted.**

#### Current Relationship Identity Proofing

**Not permitted**

#### 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**](#_Toc90010644)”.

AL4\_ID\_AFV#010 Required evidence

Ensure that the applicant possesses:

1. identification from the organization with which it is claiming affiliation;
2. 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 whichensure that the presented documents:

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

#### 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 identity proofing requirements must also be observed.

AL4\_ID\_ROC#010 Authenticate Original Credential

Prior to issuing any derived credential the original credential on which the identity-proofing relies must be:

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

[US / EZP800-63-2: §5.3.5.3, ’5.8, §8.3.2.4.2]

AL4\_ID\_ROC#020 Authenticate Original Credential

Record the details of the original credential **and the biometric sample captured when authenticating the Applicant**.

[US / EZP800-63-2: §5.3.5.9, §8.3.2.4.2]

#### 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).

[US / EZP800-63-2: §5.3.1.4.12]

#### Identity-proofingRecords

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

The enterprise or specified service must:

AL4\_ID\_VRC#010 Verification Records for Personal Applicants

Log, taking account of all applicable legislative and policy obligations, a record of the facts of the verification process and the identity of the registrar, including a reference relating to the verification processes and the date and time of verification **issued by a trusted time-source**.

[US / EZP800-63-2: §5.3.1.4.1]

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

AL4\_ID\_VRC#020 Verification Records for Affiliated Applicants

In addition to the foregoing, log, taking account of all applicable legislative and policy obligations, a record of the additional facts of the verification process must be performed. At a minimum, records of identity information must include:

1. the Subject’s[[7]](#footnote-8) full name;
2. the Subject’s current address of record;
3. the Subject’s current telephone or email address of record;
4. the Subscriber’s authorization for issuing the Subject a credential;
5. type, issuing authority, and reference number(s) of all documents checked in the identity proofing process;
6. **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.**

[US / EZP800-63-2: §5.3.1.4.1]

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.

 [US / EZP800-63-2: §5.3.1.4.2; §5.3.1.4.5 b)]

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.

[US / EZP800-63-2: §5.3.1.4.1, §7.3.1.4 e) ii)]

AL4\_CM\_IDP#040 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.

[US / EZP800-63-2: §8.3.2.4.2]

#### Credential Creation

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

Note, however, that a token and credential created according to these criteria may not necessarily provide that level of assurance for the claimed identity of the 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**.

[US / EZP800-63-2: §8.3.2.4.2]

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.

[US / EZP800-63-2: §5.3.1.4.5 a)]

**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.

[US / EZP800-63-2: §5.3.1.4.5 a)]

AL4\_CM\_CRN#035 Convey credential

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

[US / EZP800-63-2: §5.3.1.4.5 b)]

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#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:

1. employ a cryptographic module that is validated against FIPS 140-2[[FIPS140-2](#FIPS1402)] Level **2** or higher, or equivalent, as determined by a recognized national technical authority;
2. require password or biometric activation by the Subject **[omitted];**
3. **Generate a one-time password using an algorithm recognized by a national technical authority**.

[US / EZP800-63-2: §6.3.1.4.1 a), b), c), d)]

AL4\_CM\_CRN#075 Multi-factor hardware cryptographic token strength

**Ensure that hardware tokens used to store cryptographic keys:**

1. **employ a cryptographic module that is validated against FIPS 140-2 [[FIPS140-2](#FIPS1402)] Level 2 or higher, or equivalent, as determined by a recognized national technical authority;**
2. **require password, PIN or biometric activation by the Subject when being used for authentication;**
3. **does not permit the export of authentication keys.**

[US / EZP800-63-2: §6.3.1.4.2 a), b), c), d), §8.3.2.4.8]

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.

#### 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:

1. use a FIPS 140-2 [[FIPS140-2](http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf)] compliant algorithm, or equivalent, as established by a recognized national technical authority, that is recognized as being fit for the purposes of the service;
2. only create keys of a key length and for use with a FIPS 140-2 [[FIPS140-2](http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf)] compliant public key algorithm, or equivalent, as established by a recognized national technical authority, recognized as being fit for the purposes of the service;
3. generate and store the keys securely until delivery to and acceptance by the Subject;
4. 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:

1. used a FIPS 140-2 [[FIPS140-2](http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf)] compliant algorithm, or equivalent, as established by a recognized national technical authority, that is recognized as being fit for the purposes of the service;
2. created keys of a key length and for use with a FIPS 140-2 [[FIPS140-2](http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf)] compliant public key algorithm, or equivalent, as established by a recognized national technical authority, recognized as being fit for the purposes of the service.

#### 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 informationby:

1. sending notice to the address of record confirmed during identity proofing**;**
2. **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;**
3. **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.**

[US / EZP800-63-2: §5.3.1.4.11 b) v)]

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**.**

[US / EZP800-63-2: §5.3.1.6.2 d) i)]

AL3\_CM\_CRD#016 No stipulation

**No stipulation.**

AL3\_CM\_CRD#017 Protected Issuance of Permanent Secrets (in person)

Only issue permanent secrets if the CSP has:

1. loaded the secret itself onto the physical device, which was either:
2. issued in-person to the Applicant, or;
3. delivered in a manner that confirms the address of record.
4. [US / EZP800-63-2: §5.3.1.6.2 d) ii), §5.3.1.6.3]

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).

### 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.

#### 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

1. **No stipulation**;
2. **No stipulation**;
3. **No stipulation**;
4. **cryptographically authenticate** all **sensitive** renewal / re-issuance interactions with the Subject **using keys bound to the authentication process**.
 [US / EZP800-63-2: §7.3.1.4 c) i)]

**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.**

[US / EZP800-63-2: §7.3.1.4 c) ii)]

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 **10.5** years.

[US / EZP800-63-2: §7.3.1.3 e) ii)]

### Part D - Credential Revocation

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

#### 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

1. State the conditions under which revocation of an issued certificate may occur;
2. State the processes by which a revocation request may be submitted;
3. State the persons and organizations from which a revocation request will be accepted;
4. State the validation steps that will be applied to ensure the validity (identity) of the Revocant, and;
5. 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).

[US / EZP800-63-2: §8.3.2.4.2]

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.

[US / EZP800-63-2: §7.3.1.4 d) i,), §8.3.2.4.2]

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.

[US / EZP800-63-2: §8.3.2.4.2]

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:

1. the Revocant’s full name;
2. 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);
3. the Credential Issuer’s identity (if not directly responsible for the identity proofing service);
4. the reason for revocation.

[US / EZP800-63-2: §7.3.1.4 e) i), §8.3.2.4.2]

AL4\_CM\_RVP#060 Record Retention

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

1. the records retention policy required by AL2\_CM\_CPP#010, and;
2. applicable legislation;

and which, in addition, must be not less than the duration of the Subscriber’s account plus **10.5** years.

[US / EZP800-63-2: §7.3.1.4 e) ii)]

#### 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:

1. 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;
2. if remote:
	* 1. verify a signature against records (if available), confirmed with a call to a telephone number of record, or;
		2. 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:

1. from the specified service itself, with authorization as determined by established procedures, or;
2. 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:

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

#### 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:**

1. **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;**
2. **if remote:**
	* + 1. **verify a signature against records (if available), confirmed with a call to a telephone number of record, or;**
			2. **authenticate an electronic request as being from the same Subject, supported by a different credential at Assurance Level 4.**

[US / EZP800-63-2: §8.3.2.4.2]

AL4\_CM\_RKY#020 Re-key requests other than Subject

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

#### 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.

### 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.

#### 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.

[US / EZP800-63-2: §7.3.1.4 e) i)]

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:

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

[US / EZP800-63-2: §8.3.2.4.2]

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.

[US / EZP800-63-2: §8.3.2.4.2]

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.

[US / EZP800-63-2: §8.3.2.4.2]

AL4\_CM\_CSM#050 Inactive Credentials

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

### Part F - Credential Verification/Authentication

These criteria apply to credential validation and identity authentication.

#### 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:

1. requires authentication of the specified service, itself, or of the validation source;
2. ensures the integrity of the authentication assertion.

[US / EZP800-63-2: §7.3.1.4 b) i), §8.3.2.4.2]

AL4\_CM\_ASS#015 No False Authentication

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

[US / EZP800-63-2: §7.3.1.4 b) i)]

AL4\_CM\_ASS#018 Ensure token validity

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

[US / EZP800-63-2: §7.3.1.4 d) iii)]

**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 publicisied (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

*Note – merely following NIST guidance ... but why not here as well?*

AL4\_CM\_ASS#040 Assertion Life-time

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

#### 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.

[US / EZP800-63-2: §6.3.1.4.2 e)]

AL4\_CM\_AGC#020 Limit password validity

**Employ one-time passwords which expire within two minutes.**

 [US / EZP800-63-2: §6.3.1.4.1 e)]

#### 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.

[US / EZP800-63-2: §6.3.1.2, §8.3.2.4.8]

#### 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:

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.**

[US / EZP800-63-2: §9.3.2.4.1]

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.

[US / EZP800-63-2: §9.3.2.0.1]

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:

1. [Omitted];
2. Encrypting the assertion using a secret key shared by with the RP;
3. Creating an assertion reference which has a minimum of 64 bits of entropy;
4. 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:

1. both assertions and assertion references are protected against capture and re-use;
2. assertions are also protected against redirection
3. 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 referencess

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 Assertion expiration

Set assertions to expire such that:

1. those used outside of the internet domain of the Verifier become invalid 5 minutes after their creation; or
2. those used within a single internet domain become invalid 30 minutes after their creation (including assertions contained in or referenced by cookies).

AL4\_CM\_VAS#120 No stipulation

No stipulation.

## Compliance Tables

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

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

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

Table 3-5. OP-SAC - AL1 Compliance

| **Clause** | **Description** | **Compliance** |
| --- | --- | --- |
| Part A – Credential Operating Environment |
| AL1\_CM\_CTR#010 | No stipulation | No conformity requirement |
| AL1\_CM\_CTR#020 | [Protocol threat risk assessment and controls](#_Hlk230082509) |  |
| AL1\_CM\_CTR#025 | No stipulation | No conformity requirement |
| AL1\_CM\_CTR#030 | [System threat risk assessment and controls](#_Hlk230082535) |  |
| AL1\_CM\_STS#010 | Withdrawn | No conformity requirement |
| AL1\_CM\_OPN#010 | [Changeable PIN/Password](#_Hlk230082601) |  |
| 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](#_Hlk90047632) |  |
| AL1\_ID\_POL#020 | [Unique Subject identity](#_Hlk88563030) |  |
| AL1\_ID\_IPV#010 | [Required evidence](#_Hlk88563137) |  |
| AL1\_ID\_IPV#020 | [Evidence checks](#_Hlk88563367) |  |
| AL1\_ID\_RPV#010 | [Required evidence](#_Hlk88563509) |  |
| AL1\_ID\_RPV#020 | [Evidence checks](#_Hlk88563367) |  |
| AL1\_ID\_SCV#010 | [Secondary checks](#_Hlk90047714) |  |
| AL1\_CM\_IDP#040 | [Revision to Subscriber information](#_Hlk230083048) |  |
| AL1\_CM\_CRN#010 | [Authenticated Request](#_Hlk230083064)  |  |
| AL1\_CM\_CRN#020 | No stipulation | No conformity requirement |
| AL1\_CM\_CRN#030 | [Credential uniqueness](#_Hlk230083799) |  |
| Part C – Credential Renewal and Re-issuing |
| AL1\_CM\_RNR#010 | [Changeable PIN/Password](#_Hlk230084522) |  |
| Part D – Credential Revocation |
| AL1\_CM\_SRR#010 | [Submit Request](#_Hlk230083833) |  |
| Part E – Credential Status Management |
| AL1\_CM\_CSM#010 | [Maintain Status Record](#_Status_Maintenance) |  |
| 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](#_Status_Maintenance) |  |
| Part F – Credential Validation / Authentication |
| AL1\_CM\_ASS#010 | [Validation and Assertion Security](#_Assertion_Security) |  |
| AL1\_CM\_ASS#015 | No stipulation | No conformity requirement |
| AL1\_CM\_ASS#020 | [No Post Authentication](#_Hlk221494228) |  |
| AL1\_CM\_ASS#030 | [Proof of Possession](#_Assertion_Security) |  |
| AL1\_CM\_ASS#040 | [Assertion Lifetime](#_Assertion_Security) |  |

Table 3-6. OP-SAC - AL2 Compliance

| **Clause** | **Description** | **Compliance** |
| --- | --- | --- |
| Part A - Credential Operating Environment |
| AL2\_CM\_CPP#010 | [Credential Policy and Practice Statement](#_Credential_Policy_&) |  |
| AL2\_CM\_CPP#020 | No stipulation | No conformity requirement |
| AL2\_CM\_CPP#030 | [Management Authority](#_Credential_Policy_&) |  |
| AL2\_CM\_CTR#010 | Withdrawn | No conformity requirement |
| AL2\_CM\_CTR#020 | [Protocol threat risk assessment and controls](#_Security_Controls_1) |  |
| AL2\_CM\_CTR#025 | [Permitted authentication protocols](#_Hlk221493825) |  |
| AL2\_CM\_CTR#028 | [One-time passwords](#_Hlk230440191) |  |
| AL2\_CM\_CTR#030 | [System threat risk assessment and controls](#_Security_Controls_1) |  |
| AL2\_CM\_CTR#040 | [Specified Service's Key Management](#_Security_Controls_1) |  |
| 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](#_Hlk230080619) |  |
| AL2\_ID\_POL#020 | [Unique Subject identity](#_Hlk230080946) |  |
| AL2\_ID\_POL#030 | [Published Proofing Policy](#_Hlk230080959) |  |
| AL2\_ID\_POL#040 | [Adherence to Proofing Policy](#_Hlk74642049) |  |
| AL2\_ID\_IDV#000 | [Identity Proofing classes](#_Hlk221491780) |  |
| AL2\_ID\_IPV#010 | [Required evidence](#_Hlk230081001) |  |
| AL2\_ID\_IPV#020 | [Evidence checks](#_Hlk76312325) |  |
| AL2\_ID\_RPV#010 | [Required evidence](#_Hlk230081080) |  |
| AL2\_ID\_RPV#020 | [Evidence checks](#_Hlk76312393) |  |
| AL2\_ID\_CRV#010 | [Required evidence](#_Hlk230081149) |  |
| AL2\_ID\_CRV#020 | [Evidence checks](#_Hlk230081164) |  |
| AL2\_ID\_AFV#000 | [Meet preceding criteria](#_Hlk221491841) |  |
| AL2\_ID\_AFV#010 | [Required evidence](#_Hlk230081210) |  |
| AL2\_ID\_AFV#020 | [Evidence checks](#_Hlk230081233) |  |
| AL2\_ID\_SCV#010 | [Secondary checks](#_Hlk230081247) |  |
| AL2\_ID\_VRC#010 | [Verification Records for Personal Applicants](#_Hlk230081264) |  |
| AL2\_ID\_VRC#020 | [Verification Records for Affiliated Applicants](#_Hlk230081295) |  |
| AL2\_ID\_VRC#030 | [Record Retention](#_Hlk230081312) |  |
| AL2\_CM\_IDP#040 | [Revision to Subscriber information](#_Identity_Proofing_1) |  |
| AL2\_CM\_CRN#010 | [Authenticated Request](#_Credential_Creation_1) |  |
| AL2\_CM\_CRN#020 | [Unique identity](#_Hlk230083187) |  |
| AL2\_CM\_CRN#030 | [Credential uniqueness](#_Hlk230083226) |  |
| AL2\_CM\_CRN#035 | [Convey credential](#_Hlk230083263) |  |
| AL2\_CM\_CRN#040 | [Password strength](#_Hlk230083325) |  |
| AL2\_CM\_CRN#050 | [One-time password strength](#_Hlk230083434) |  |
| AL2\_CM\_CRN#060 | [Software cryptographic token strength](#_Hlk230083473) |  |
| AL2\_CM\_CRN#070 | [Hardware token strength](#_Hlk230083498) |  |
| AL2\_CM\_CRN#080 | No stipulation | No conformity requirement |
| AL2\_CM\_CRN#090 | [Nature of Subject](#_Hlk230083548) |  |
| AL2\_CM\_CRD#010 | [Notify Subject of Credential Issuance](#_Hlk230083576) |  |
| AL2\_CM\_CRD#015 | [Confirm Applicant’s identity (in person)](#_Hlk230083611) |  |
| AL2\_CM\_CRD#016 | [Confirm Applicant’s identity (remotely)](#_Hlk230083629) |  |
| Part C – Credential Renewal and Re-issuing |
| AL2\_CM\_RNR#010 | [Changeable PIN/Password](#_Hlk230084620) |  |
| AL2\_CM\_RNR#020 | [Proof-of-possession on Renewal/Re-issuance](#_Hlk230084636) |  |
| AL2\_CM\_RNR#030 | [Renewal/Re-issuance limitations](#_Hlk230084650) |  |
| Part D – Credential Revocation |
| AL2\_CM\_RVP#010 | [Revocation procedures](#_Hlk230085010) |  |
| AL2\_CM\_ RVP#020 | [Secure status notification](#_Hlk230085022) |  |
| AL2\_CM\_ RVP#030 | [Revocation publication](#_Hlk230085037) |  |
| AL2\_CM\_RVP#040 | [Verify revocation identity](#_Hlk76312508) |  |
| AL2\_CM\_RVP#050 | [Revocation Records](#_Hlk230085123) |  |
| AL2\_CM\_RVP#060 | [Record Retention](#_Hlk76312252) |  |
| AL2\_CM\_RVR#010 | [Verify revocation identity](#_Hlk230085262) |  |
| AL2\_CM\_RVR#020 | [Revocation reason](#_Hlk76312532) |  |
| AL2\_CM\_RVR#030 | [Verify Subscriber as Revocant](#_Hlk76312595) |  |
| AL2\_CM\_RVR#040 | [CSP as Revocant](#_Hlk76312626) |  |
| AL2\_CM\_RVR#050 | [Verify Legal Representative as Revocant](#_Hlk76312662) |  |
| AL2\_CM\_SRR#010 | [Submit Request](#_Hlk230085497) |  |
| Part E – Credential Status Management |
| AL2\_CM\_CSM#010 | [Maintain Status Record](#_Hlk230085536) |  |
| AL2\_CM\_CSM#020 | [Validation of Status Change Requests](#_Hlk230085563) |  |
| AL2\_CM\_CSM#030 | [Revision to Published Status](#_Hlk230085589) |  |
| AL2\_CM\_CSM#040 | [Status Information Availability](#_Hlk230085600) |  |
| AL2\_CM\_CSM#050 | [Inactive Credentials](#_Hlk230085609) |  |
| Part F – Credential Validation / Authentication |
| AL2\_CM\_ASS#010 | [Validation and Assertion Security](#_Hlk230085642) |  |
| AL2\_CM\_ASS#015 | [No False Authentication](#_Hlk221494320) |  |
| AL2\_CM\_ASS#020 | [No Post Authentication](#_Hlk230085662) |  |
| AL2\_CM\_ASS#030 | [Proof of Possession](#_Hlk230085672) |  |
| AL2\_CM\_ASS#040 | [Assertion Lifetime](#_Hlk230085681) |  |

Table 3-7. OP-SAC - AL3 compliance

| **Clause** | **Description** | **Compliance** |
| --- | --- | --- |
| Part A – Credential Operating Environment |
| AL3\_CM\_CPP#010 | [Credential Policy and Practice Statement](#_Hlk230085747) |  |
| AL3\_CM\_CPP#020 | No stipulation | No conformity requirement |
| AL3\_CM\_CPP#030 | [Management Authority](#_Hlk230085849) |  |
| AL3\_CM\_CTR#010 | No stipulation | No conformity requirement |
| AL3\_CM\_CTR#020 | [Protocol threat risk assessment and controls](#_Hlk230085898) |  |
| AL3\_CM\_CTR#025 | [Permitted authentication protocols](#_Hlk230085918) |  |
| AL3\_CM\_CTR#030 | [System threat risk assessment and controls](#_Hlk230086027) |  |
| AL3\_CM\_CTR#040 | [Specified Service's Key Management](#_Hlk230086039) |  |
| AL3\_CM\_STS#010 | Withdrawn | No conformity requirement |
| AL3\_CM\_STS#020 | [Stored Secret Encryption](#_Hlk230086082) |  |
| AL3\_CM\_SER#010 | [Security event logs](#_Hlk230086103) |  |
| AL3\_CM\_OPN#010 | [Changeable PIN/Password](#_Hlk230086119) |  |
| Part B – Credential Issuing |
| AL3\_CM\_IDP#010 | Withdrawn | No conformity requirement |
| AL3\_CM\_IDP#020 | Withdrawn | No conformity requirement |
| AL3\_CM\_IDP#030 | Withdrawn | No conformity requirement |
| AL3\_ID\_POL#010 | [Unique service identity](#_Hlk230081362) |  |
| AL3\_ID\_POL#020 | [Unique Subject identity](#_Hlk230081378) |  |
| AL3\_ID\_POL#030 | [Published Proofing Policy](#_Hlk230081469) |  |
| AL3\_ID\_POL#040 | [Adherence to Proofing Policy](#_Hlk230081485) |  |
| AL3\_ID\_IDV#000 | [Identity Proofing classes](#_Hlk221491928) |  |
| AL3\_ID\_IPV#010 | [Required evidence](#_Hlk230081511) |  |
| AL3\_ID\_IPV#020 | [Evidence checks](#_Hlk230081533) |  |
| AL3\_ID\_RPV#010 | [Required evidence](#_Hlk230081560) |  |
| AL3\_ID\_RPV#020 | [Evidence checks](#_Hlk230081575) |  |
| AL3\_ID\_AFV#000 | [Meet preceding criteria](#_Hlk221491986) |  |
| AL3\_ID\_AFV#010 | [Required evidence](#_Hlk230081597) |  |
| AL3\_ID\_AFV#020 | [Evidence checks](#_Hlk230081615) |  |
| AL3\_ID\_SCV#010 | [Secondary checks](#_Hlk230081635) |  |
| AL3\_ID\_VRC#010 | [Verification Records for Personal Applicants](#_Hlk230081653) |  |
| AL3\_ID\_VRC#020 | [Verification Records for Affiliated Applicants](#_Hlk230081687) |  |
| AL3\_ID\_VRC#030 | [Record Retention](#_Hlk230081702) |  |
| AL3\_CM\_IDP#040 | [Revision to Subscriber information](#_Hlk230086203) |  |
| AL3\_CM\_CRN#010 | [Authenticated Request](#_Hlk230086213)  |  |
| AL3\_CM\_CRN#020 | [Unique identity](#_Hlk230086226) |  |
| AL3\_CM\_CRN#030 | [Credential uniqueness](#_Hlk230086242) |  |
| AL3\_CM\_CRN#035 | [Convey credential](#_Hlk230086256) |  |
| AL3\_CM\_CRN#040 | [PIN/Password strength](#_Hlk230086283) |  |
| AL3\_CM\_CRN#050 | [One-time password strength](#_Hlk230086294) |  |
| AL3\_CM\_CRN#060 | [Software cryptographic token strength](#_Hlk230086325) |  |
| AL3\_CM\_CRN#070 | [Hardware token strength](#_Hlk230086339) |  |
| AL3\_CM\_CRN#080 | [Binding of key](#_Hlk230086351) |  |
| AL3\_CM\_CRN#090 | [Nature of Subject](#_Hlk230086361) |  |
| AL3\_CM\_SKP#010 | [Key generation by Specified Service](#_Hlk230086372) |  |
| AL3\_CM\_SKP#020 | [Key generation by Subject](#_Hlk230086384) |  |
| AL3\_CM\_CRD#010 | [Notify Subject of Credential Issuance](#_Hlk221375806) |  |
| AL3\_CM\_CRD#020 | [Subject's acknowledgement](#_Hlk230086534) |  |
| Part C – Credential Renewal and Re-issuing |
| AL3\_CM\_RNR#010 | [Changeable PIN/Password](#_Hlk230084708) |  |
| Part D – Credential Revocation |
| AL3\_CM\_RVP#010 | [Revocation procedures](#_Hlk230087007) |  |
| AL3\_CM\_ RVP#020 | [Secure status notification](#_Hlk230423253) |  |
| AL3\_CM\_ RVP#030 | [Revocation publication](#_Hlk230423267) |  |
| AL3\_CM\_RVP#040 | [Verify Revocation Identity](#_Hlk230423276) |  |
| AL3\_CM\_RVP#050 | [Revocation Records](#_Hlk230423291) |  |
| AL3\_CM\_RVP#060 | [Record Retention](#_Hlk230423304) |  |
| AL3\_CM\_RVR#010 | [Verify revocation identity](#_Hlk230423340) |  |
| AL3\_CM\_RVR#020 | [Revocation reason](#_Hlk230423352) |  |
| AL3\_CM\_RVR#030 | [Verify Subscriber as Revocant](#_Hlk230423363) |  |
| AL3\_CM\_RVR#040 | [Verify CSP as Revocant](#_Hlk230423379) |  |
| AL3\_CM\_RVR#050 | [Verify Legal Representative as Revocant](#_Hlk230423438) |  |
| AL3\_CM\_SRR#010 | [Submit Request](#_Hlk230423450) |  |
| Part E – Credential Status Management |
| AL3\_CM\_CSM#010 | [Maintain Status Record](#_Hlk230424060) |  |
| AL3\_CM\_CSM#020 | [Validation of Status Change Requests](#_Hlk230424070) |  |
| AL3\_CM\_CSM#030 | [Revision to Published Status](#_Hlk230424082) |  |
| AL3\_CM\_CSM#040 | [Status Information Availability](#_Hlk230424091) |  |
| AL3\_CM\_CSM#050 | [Inactive Credentials](#_Hlk230424103) |  |
| Part F – Credential Validation / Authentication |
| AL3\_CM\_ASS#010 | [Validation and Assertion Security](#_Hlk230424137) |  |
| AL3\_CM\_ASS#015 | [No False Authentication](#_Hlk221494862) |  |
| AL3\_CM\_ASS#020 | [Post Authentication](#_Hlk230424157) |  |
| AL3\_CM\_ASS#030 | [Proof of Possession](#_Hlk230424182) |  |
| AL3\_CM\_ASS#040 | [Assertion Lifetime](#_Hlk230424191) |  |

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](#_Hlk230424350) |  |
| AL4\_CM\_CPP#030 | [Management Authority](#_Hlk230424364) |  |
| AL4\_CM\_CTR#010 | No stipulation | No conformity requirement |
| AL4\_CM\_CTR#020 | [Protocol threat risk assessment and controls](#_Hlk230424397) |  |
| AL4\_CM\_CTR#025 | No stipulation | No conformity requirement |
| AL4\_CM\_CTR#030 | [System threat risk assessment and controls](#_Hlk230424417) |  |
| AL4\_CM\_CTR#040 | [Specified Service’s Key Management](#_Hlk230424429) |  |
| AL4\_CM\_STS#010 | [Stored Secrets](#_Hlk230424488) |  |
| AL4\_CM\_STS#020 | [Stored Secret Encryption](#_Hlk230424502) |  |
| AL4\_CM\_SER#010 | [Security event logs](#_Hlk230424516) |  |
| AL4\_CM\_OPN#010 | Withdrawn | No conformity requirement |
| Part B – Credential Issuing |
| AL4\_CM\_IDP#010 | Withdrawn | No conformity requirement |
| AL4\_CM\_IDP#020 | Withdrawn | No conformity requirement |
| AL4\_CM\_IDP#030 | Withdrawn | No conformity requirement |
| AL4\_ID\_POL#010 | [Unique service identity](#_Hlk230081757) |  |
| AL4\_ID\_POL#020 | [Unique Subject identity](#_Hlk230081770) |  |
| AL4\_ID\_POL#030 | [Published Proofing Policy](#_Hlk230081785) |  |
| AL4\_ID\_POL#040 | [Adherence to Proofing Policy](#_Hlk230081799) |  |
| AL3\_ID\_IDV#000 | [Identity Proofing classes](#_Hlk230081858) |  |
| AL4\_ID\_IPV#010 | [Required evidence](#_Hlk230081879) |  |
| AL4\_ID\_IPV#020 | No stipulation | No conformity requirement |
| AL4\_ID\_IPV#030 | [Evidence checks – primary ID](#_Hlk230081905) |  |
| AL4\_ID\_IPV#040 | [Evidence checks – secondary ID](#_Hlk230081922) |  |
| AL4\_ID\_IPV#050 | [Applicant knowledge checks](#_Hlk230081945) |  |
| AL4\_ID\_AFV#000 | [Meet preceding criteria](#_Hlk221492261) |  |
| AL4\_ID\_AFV#010 | [Required evidence](#_Hlk230081976) |  |
| AL4\_ID\_AFV#020 | [Evidence checks](#_Hlk230081998) |  |
| AL4\_ID\_SCV#010 | [Secondary checks](#_Hlk230082014) |  |
| AL4\_ID\_VRC#010 | [Verification Records for Personal Applicants](#_Hlk230082028) |  |
| AL4\_ID\_VRC#020 | [Verification Records for Affiliated Applicants](#_Hlk230082105) |  |
| AL4\_ID\_VRC#030 | [Record Retention](#_Hlk230082126) |  |
| AL4\_CM\_IDP#040 | [Revision to Subscriber information](#_Hlk230424718) |  |
| AL4\_CM\_CRN#010 | [Authenticated Request](#_Hlk230424704) |  |
| AL4\_CM\_CRN#020 | [Unique identity](#_Hlk230424732) |  |
| AL4\_CM\_CRN#030 | [Credential uniqueness](#_Hlk230424764) |  |
| AL4\_CM\_CRN#035 | [Convey credential](#_Hlk230424789) |  |
| AL4\_CM\_CRN#040 | [PIN/Password strength](#_Hlk230425597) |  |
| AL4\_CM\_CRN#050 | [One-time password strength](#_Hlk230425606) |  |
| AL4\_CM\_CRN#060 | [Software cryptographic token strength](#_Hlk230425614) |  |
| AL4\_CM\_CRN#070 | [Hardware token strength](#_Hlk230425631) |  |
| AL4\_CM\_CRN#080 | [Binding of key](#_Hlk230425649) |  |
| AL4\_CM\_CRN#090 | [Nature of Subject](#_Hlk230425669) |  |
| AL4\_CM\_SKP#010 | [Key generation by Specified Service](#_Hlk230425679) |  |
| AL4\_CM\_SKP#020 | [Key generation by Subject](#_Hlk230425689) |  |
| AL4\_CM\_CRD#010 | [Notify Subject of Credential Issuance](#_Hlk230425715) |  |
| AL4\_CM\_CRD#020 | [Subject’s acknowledgement](#_Hlk230425722) |  |
| Part C – Credential Renewal and Re-issuing |
| AL4\_CM\_RNR#010 | [Changeable PIN/Password](#_Hlk230084756) |  |
| Part D – Credential Revocation |
| AL4\_CM\_RVP#010 | [Revocation procedures](#_Hlk230425776) |  |
| AL4\_CM\_ RVP#020 | [Secure status notification](#_Hlk230425787) |  |
| AL4\_CM\_ RVP#030 | [Revocation publication](#_Hlk230425794) |  |
| AL4\_CM\_RVP#040 | No stipulation | No conformity requirement |
| AL4\_CM\_RVP#050 | [Revocation Records](#_Hlk230425808) |  |
| AL4\_CM\_RVP#060 | [Record Retention](#_Hlk230425816) |  |
| AL4\_CM\_RVR#010 | [Verify revocation identity](#_Hlk230425829) |  |
| AL4\_CM\_RVR#020 | [Revocation reason](#_Hlk230425839) |  |
| AL4\_CM\_RVR#030 | [Verify Subscriber as Revocant](#_Hlk230425871) |  |
| AL4\_CM\_RVR#040 | [Verify CSP as Revocant](#_Hlk230425880) |  |
| AL4\_CM\_RVR#050 | [Verify Legal Representative as Revocant](#_Hlk230425920) |  |
| AL4\_CM\_RKY#010 | [Verify Requestor as Subscriber](#_Hlk230425953) |  |
| AL4\_CM\_RKY#020 | [Re-key requests other than Subject](#_Hlk230425987) |  |
| AL4\_CM\_SRR#010 | [Submit Request](#_Hlk230425970) |  |
| Part E – Credential Status Management |
| AL4\_CM\_CSM#010 | [Maintain Status Record](#_Hlk230426053) |  |
| AL4\_CM\_CSM#020 | [Validation of Status Change Requests](#_Hlk230426061) |  |
| AL4\_CM\_CSM#030 | [Revision to Published Status](#_Hlk230426076) |  |
| AL4\_CM\_CSM#040 | [Status Information Availability](#_Hlk230426084) |  |
| AL4\_CM\_CSM#050 | [Inactive Credentials](#_Hlk230426093) |  |
| Part F – Credential Validation / Authentication |
| AL4\_CM\_ASS#010 | [Validation and Assertion Security](#_Hlk230426110) |  |
| AL4\_CM\_ASS#015 | [No False Authentication](#_Hlk221494912) |  |
| AL4\_CM\_ASS#020 | [Post Authentication](#_Hlk230426130) |  |
| AL4\_CM\_ASS#030 | [Proof of Possession](#_Hlk230426144) |  |
| AL4\_CM\_ASS#040 | [Assertion Lifetime](#_Hlk230426153) |  |

 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>

Revision History

1. 2008-05-08 – Identity Assurance Framework Version 1.0 Initial Draft
	1. Released by Liberty Alliance
	2. Revision and scoping of Initial Draft release
2. 2008-06-23 – Identity Assurance Framework Version 1.1 Final Draft
	1. Released by Liberty Alliance
	2. Inclusion of comments to Final Draft
3. 2009-10-01 – Identity Assurance Framework Version 1.1 Final Draft
	1. Documents contributed to Kantara Initiative by Liberty Alliance
4. 2010-04-dd – SAC Version 2.0
	1. Released by Kantara Initiative
	2. Significant scope build
	3. Original Identity Assurance Framework all inclusive document broken in to a set of documents with specific focus:
		1. Kantara IAF-1000-Overview
		2. Kantara IAF-1100-Glossary
		3. Kantara IAF-1200-Levels of Assurance
		4. Kantara IAF-1300-Assurance Assessment Scheme
		5. Kantara IAF-1400-Service Assessment Criteria (this document)
		6. Kantara IAF-1600-Assessor Qualifications and Requirements
5. 2013-mm-dd – Identity Assurance Framework Version 2.0
	1. Major revision to map SAC against NIST SP 800-63-2;
	2. ???

# SAC v2.0 to SAC v3.0 CRITERIA MAPPING

Deleted – at the time of formal publication of these revisions SAC V3.0 had been published for over twelve months, and thereby all ongoing and new Approvals should be grnated against at least v3.0.

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. [↑](#footnote-ref-1)
2. Refer to NIST SP 800-63 “Appendix A: Estimating Entropy and Strength” or similar recognized sources of such information. [↑](#footnote-ref-2)
3. At this stage, the Subject is the entity acting in the role of Applicant, in anticipation of being issued a credential in which they shall be identified as the ‘Subject’ of that credential. [↑](#footnote-ref-3)
4. For an identity proofing service that is within the management scope of a Credential Management service provider, this should be the Credential Management service’s definitive policy; for a stand-alone identity proofing service, the policy may be either that of a client who has defined one through contract, the ID service’s own policy or a separate policy that explains how the client’s policies will be complied with. [↑](#footnote-ref-5)
5. At this stage, the Subject is the entity acting in the role of Applicant, in anticipation of being issued a credential in which they shall be identified as the ‘Subject’ of that credential. [↑](#footnote-ref-6)
6. 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. [↑](#footnote-ref-7)
7. At this stage, the Subject is the entity acting in the role of Applicant, in anticipation of being issued a credential in which they shall be identified as the ‘Subject’ of that credential. [↑](#footnote-ref-8)