



Identity Assurance Framework: SAC mapping - ISO/IEC 29115:2013 / ITU-T X.1254 (09/2012) - *Entity authentication assurance framework*

Version: 1.0
Date: 2015-12-03
Status: Final Report
Approval: IAWG20151203

Editor: Richard G. Wilsher, Zyigma LLC

Contributors:

Voting Members of the IAWG as of publication date:

<https://kantarainitiative.org/confluence/x/k4PEAw>

Abstract:

The Kantara Initiative Identity Assurance Work Group (IAWG) was formed to foster adoption of identity trust services. The primary deliverable of the IAWG is the Identity Assurance Framework (IAF). This document presents a mapping between a joint ISO/IEC and ITU-T standard on 'entity authentication' and the Kantara Service Assessment Criteria, 'SAC', v4.0*bis*.

The latest versions of Kantara documents can be found on Kantara's [Identity Assurance Framework - General Information web page](#).

Notice:

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

Content in this document is based on that in [X.1254] (see Bibliography), published by ITU-T, which has been extended with Kantara-generated content which serves to meet the objectives of mapping parts of Kantara's Identity Assurance Framework specifications to [X.1254]. Implementation or use of certain elements of this document may require licenses under third party intellectual property rights, including without limitation, patent rights. Entities using this document are advised that it has content derived directly from an ITU-T Recommendation ([X.1254]) which falls under ITU-T's permissions as

stated in that Recommendation. 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.

Readership

This report is intended to be read and used as guidance by:

- a) those designing and implementing Identity and Credential Management Services or components for which they seek Kantara Approval, and who wish to demonstrate their alignment or compliance to NIST SP 800-63-2;
- b) those who wish to develop US-specific profiles of Kantara's SAC to facilitate the demonstration of strict compliance to SP 800-63-2;
- c) those who are responsible for reviewing or more formally assessing (e.g. as a Kantara-Accredited Assessor) Identity and Credential Management Services against SP 800-63-2.

Feedback

Users of this report are encouraged to provide feedback to Kantara concerning any alternative views on, alternatives to, or enhancement of, the mappings presented herein.

Apologia

All following parts of this document are taken directly from [X.1254] except as annotated in one of the following manners:

- 1) where it has been felt absolutely necessary, in order to ensure clarity of understanding or for the purposes of readability, deleted text ~~is shown thus~~ and additional text is shown thus;
- 2) where source text has been excised simply because it made statements not applicable to the present document’s mapping purpose and scope, or was otherwise considered to be extraneous (e.g. all references to NPEs have been removed, since these are not within the present scope of the KI IAF), its removal is indicated by the phrase “*«source text excised»*”;
- 3) original text has been broken into discrete paragraphs in order to isolate [X.1254] text against which a commentary or a mapping to [KI-SAC] criteria is provided (see below);
- 4) Mappings relating to the relationship between the Kantara SAC and [X.1254] are shown as follows:

{KI.«section_reference»#«sequence_no.»: Original text from [X.1254] (possibly modified in accordance with preceding qualifiers).

{AL*_«SAC tag ref.»}

In such mappings ‘AL*’ indicates applicability at all ALs, whereas any qualification with numbers, e.g. ‘AL2/3’ indicates applicability at only the cited Assurance Levels.

- 5) Commentary relating to the relationship between the Kantara SAC and [X.1254] or on any aspect or interpretation of [X.1254] is shown as follows:

{KI.« section_reference »#«sequence_no »: NOTE/comment. }

For the purposes of understanding the mappings offered by this document, use of the reference [X.1254] should be taken to be synonymous with [IS.29115], noting the editorial changes made to adopt any specific variance with the ISO-published document (such changes being indicated in accordance with 1) above). For this reason, unless a reference to [IS.29115] is explicitly intended to be to that publication uniquely, references to the source text will use [X.1254].

The Editor believes it to be worth noting that, although Kantara made substantial contribution to the development of [IS29115], evidence of which can be seen in the broad structure of, and in many clauses within, the standard, the general level of direction given by this standard’s requirements in clauses 6 – 9 frequently lacks clarity and precision and is not an adequate document against which any significant implementation could be found conformant or not. [KI-SAC] provides a much ‘tighter’ set of requirements in these areas (i.e. more explicit and granular across ALs), and any CSP meeting the requirements of [KI-SAC] is almost certainly going to be conformant with [IS.29115 / X.1254]. In that regard, some mappings are more ‘by inference’ than because there is a direct correlation between an explicit requirement in [X.1254] and a requirement in [KI-SAC]: §8.3.1 of this document is a case in point.

FOREWORD

«source text excised»

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

A similar text is published as ISO/IEC 29115:2013. It differs from this text in four instances:

- 1) clause 3.1.6: the definition for credential is different and in this Recommendation references the definition in Recommendation ITU-T X.1252;
{KI.0#01: This document also includes the definition from [IS29115]}
- 2) Table 10-1: ISO/IEC 29115 includes an example for impersonation that includes use of an identity for an entity that does not exist;
{KI.0#02: This document also includes the example from [IS29115]}
- 3) clause 10.2.2.1: ISO/IEC 29115 describes SSL as an example of a protected channel;
{KI.0#03: This document also includes the text from [IS29115]}
- 4) In this Recommendation, Annex A, *Characteristics of a credential*, is normative.
{KI.0#04: This document makes no determination on the normative status of Annex A, on the basis that it has no bearing upon the mappings *per se* and no Annexes are included within this document. }

NOTE

In this [ITU-T] Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

{KI.0#05: This mapping interpretation is intended to apply to any enterprise implementing or assessing, or being otherwise interested in, the application of the requirements to entity authentication services.
The term 'administration' would therefore more usefully be taken to refer to a CSP, in Kantara-speak. }

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

«*source text excised*»

Kantara Initiative is grateful to ITU-T for providing this Recommendation without restriction on its reproduction in a manner which is consistent with its original purpose.

Kantara Initiative recognizes that content in this document originating in ITU-T's Recommendation [X.1254] remains the intellectual property of ITU-T and is used in accordance with ITU-T's copyright provisions. © ITU-T 2013.

For specific mapping-related text provided by the Kantara Initiative, the following applies: [Option Patent & Copyright: Reciprocal Royalty Free with Opt-Out to Reasonable And Non discriminatory \(RAND\)](#) | © Kantara Initiative 2015

PRECEDENCE

This document is intended to reflect the requirements of both [IS29115] and [X.1254] with minimal change. Where changes have been made this will be only to accommodate a clarification or other contextual need, or to ensure inclusion of requirements from [IS29115] where the two referenced documents differ (see Foreword, above). In the event of any difference in how a requirement is expressed or in perceived meaning or interpretation, the formal publications from ISO and ITU-T respectively shall take precedence.

TABLE OF CONTENTS

1	Scope	1
2	References	1
3	Definitions	2
	3.1 Terms defined elsewhere	2
	3.2 Terms defined in this Recommendation	3
4	Abbreviations and acronyms	4
5	Conventions	5
6	Levels of assurance	5
	6.1 Level of assurance 1 (LoA1)	6
	6.2 Level of assurance 2 (LoA2)	6
	6.3 Level of assurance 3 (LoA3)	7
	6.4 Level of assurance 4 (LoA4)	7
	6.5 Selecting the appropriate level of assurance	7
	6.6 LoA mapping and interoperability	9
	6.7 Exchanging authentication results based on the 4 LoAs	9
7	Actors	10
	7.1 Entity	10
	7.2 Credential service provider	10
	7.3 Registration authority	11
	7.4 Relying party	11
	7.5 Verifier	11
	7.6 Trusted third party	11
8	Entity authentication assurance framework phases	11
	8.1 Enrolment phase	12
	8.1.1 Application and initiation	12
	8.1.2 Identity proofing and identity information verification	12
	8.1.3 Record-keeping/recording	16
	8.1.4 Registration	16
	8.2 Credential management phase	16
	8.2.1 Credential creation	16
	8.2.2 Credential issuance	17
	8.2.3 Credential activation	17

8.2.4	Credential storage	18
8.2.5	Credential suspension, revocation and/or destruction	18
8.2.6	Credential renewal and/or replacement	18
8.2.7	Record-keeping	19
8.3	Entity authentication phase.....	19
8.3.1	Authentication	19
8.3.2	Record-keeping	19
9	Management and organizational considerations.....	19
9.1	Service establishment	20
9.2	Legal and contractual compliance	20
9.3	Financial provisions	20
9.4	Information security management and audit	20
9.5	External service components	21
9.6	Operational infrastructure.....	21
9.7	Measuring operational capabilities.....	21
10	Threats and controls.....	22
10.1	Threats to, and controls for, the enrolment phase	22
10.1.1	Enrolment phase threats	22
10.1.2	Required LoA controls to protect against enrolment phase threats.....	22
10.2	Threats to, and controls for, the credential management phase	25
10.2.1	Credential management threats	25
10.2.2	Required LoA controls to protect against credential management phase threats	26
10.3	Threats to, and controls for, the authentication phase	32
10.3.1	Authentication phase threats.....	32
10.3.2	Required LoA controls to protect against threats to the use of credentials	33
11	Service assurance criteria	37

INTRODUCTION

Many electronic transactions within or between ICT systems have security requirements which depend upon an understood or specified level of confidence in the identities of the entities involved. Such requirements may include the protection of assets and resources against unauthorized access, for which an access control mechanism might be used, and/or the enforcement of accountability by the maintenance of audit logs of relevant events, as well as for accounting and charging purposes.

Recommendation ITU-T X.1254 provides a framework for entity authentication assurance. Assurance within this Recommendation refers to the confidence placed in all of the processes, management activities and technologies used to establish and manage the identity of an entity for use in authentication transactions.

Technical		Management and organizational
Enrolment phase	<ul style="list-style-type: none"> • Application and initiation • Identity proofing and identity information verification 	<ul style="list-style-type: none"> • Record-keeping/recording • Registration
Credential management phase	<ul style="list-style-type: none"> • Credential creation • Credential pre-processing • Credential issuance • Credential activation • Credential storage 	<ul style="list-style-type: none"> • Credential suspension, revocation, and/or destruction • Credential renewal and/or replacement • Record-keeping
Entity authentication phase	<ul style="list-style-type: none"> • Authentication • Record-keeping 	<ul style="list-style-type: none"> • Service establishment • Legal and contractual compliance • Financial provisions • Information security management and audit • External service components • Operational infrastructure • Measuring operational capabilities

X.1254(12)_F01

Figure 1 – Overview of the entity authentication assurance framework

Using four specified levels of assurance (LoAs), this Recommendation provides guidance concerning control technologies, processes and management activities, as well as assurance criteria, that should be used to mitigate authentication threats in order to implement the four LoAs. It also provides guidance for the mapping of other authentication assurance schemes to the specified four levels, as well as guidance for exchanging the results of an authentication transaction. Finally, this Recommendation provides guidance concerning the protection of personally identifiable information (PII) associated with the authentication process.

This Recommendation is intended to be used principally by credential service providers (CSPs) and by others having an interest in their services (e.g., relying parties, assessors and auditors of those services). This entity authentication assurance framework (EAAF) specifies the minimum technical, management and process requirements for four LoAs to ensure equivalence among the credentials issued by various CSPs. It also provides some additional management and organizational considerations that affect entity authentication assurance, but it does not set forth specific criteria for those considerations. Relying parties (RPs) and others may find this Recommendation helpful to gain an understanding of what each LoA provides. Additionally, it may be adopted for use within a trust framework to define technical requirements for LoAs. The EAAF is intended for, but not limited to, session-based and document-

centric use cases using various authentication technologies. Both direct and brokered trust scenarios are possible, within either legal/bilateral arrangements or federations.

1 Entity authentication assurance framework¹

2 1 Scope

3 {KI.1#01: This document is intended to provide a mapping to the Kantara [KI-SAC], thereby facilitating demonstration of
4 alignment with [IS29115 / X.1254] for entities also seeking conformity with the [KI-SAC]. Those entities seeking formal
5 conformance to either [IS29115] or [X.1254] should refer to the formally-published versions of either of those documents,
6 which shall take precedence over the present document.}

7 This Recommendation provides a framework for managing entity authentication assurance in a given
8 context. In particular, it:

- 9 – {KI.1#02: specifies four levels of entity authentication assurance;
10 {{[KI-SAC] provides criteria at various degrees of rigor in order to meet the objectives of [b-OMB].}}
- 11 – {KI.1#03: specifies criteria and guidelines for achieving each of the four levels of entity
12 authentication assurance;
13 {{[KI-SAC] provides criteria which address entity authentication, these being the focus of this mapping.}}
- 14 – provides guidance for mapping other authentication assurance schemes to the four LoAs;
- 15 – provides guidance for exchanging the results of authentication that are based on the four LoAs;
16 and
- 17 – {KI.1#04: provides guidance concerning controls that should be used to mitigate authentication
18 threats.
19 {{[KI-SAC] provides criteria which address these controls.}}

20 2 References

21 None.

22

¹ Korea (Republic of) has expressed a reservation and will not apply this Recommendation because this Recommendation is in conflict with regulations in Korea, with regard to the required four levels of entity authentication assurance and their criteria for achieving each of the four levels of entity authentication assurance.

23

24 **3 Definitions**

25 {KI.3#01: [KI-GLOSS] provides a glossary of terms used within the Kantara IAF. This mapping does NOT extend to a
26 comparison between the definitions herein and those used within the IAF. Users of this mapping are advised to review the
27 definitions in each source document and ensure their interpretations and implementations are aligned accordingly.}

28 **3.1 Terms defined elsewhere**

29 This Recommendation uses the following terms defined elsewhere:

30 **3.1.1 assertion** [b-ITU-T X.1252]: A statement made by an entity without accompanying evidence of
31 its validity.

32 NOTE – The meaning of the terms claim and assertion are generally agreed to be somewhat similar but with
33 slightly different meanings. For the purposes of this Recommendation, an assertion is considered to be a stronger
34 statement than a claim.

35 **3.1.2 authentication** [b-ISO/IEC 18014-2]: Provision of assurance in the identity of an entity.

36 **3.1.3 authentication factor** [b-ISO/IEC 19790]: Piece of information and/or process used to
37 authenticate or verify the identity of an entity.

38 NOTE – Authentication factors are divided into four categories:

- 39 – something an entity has (e.g., device signature, passport, hardware device containing a credential, private
40 key);
- 41 – something an entity knows (e.g., password, PIN);
- 42 – something an entity is (e.g., biometric characteristic);
- 43 – something an entity typically does (e.g., behaviour pattern).

44 **3.1.4 claim** [b-ITU-T X.1252]: To state as being the case, without being able to give proof.

45 NOTE – The meaning of the terms claim and assertion are generally agreed to be somewhat similar but with
46 slightly different meanings. For the purposes of this Recommendation, an assertion is considered to be a stronger
47 statement than a claim.

48 **3.1.5 context** [b-ITU-T X.1252]: An environment with defined boundary conditions in which entities
49 exist and interact.

50 **3.1.6 credential** [b-ITU-T X.1252]: A set of data presented as evidence of a claimed identity and/or
51 entitlements.

52 NOTE – See Appendix I for additional characteristics of a credential.

53 **3.1.6bis** set of data presented as evidence of a claimed or asserted identity and/or entitlements (From [IS29115].)

54 **3.1.7 entity** [b-ITU-T X.1252]: Something that has separate and distinct existence and that can be
55 identified in a context.

56 NOTE – For the purposes of this Recommendation, entity is also used in the specific case for something that is
57 claiming an identity.

58 **3.1.8 identity** [b-ISO/IEC 24760]: Set of attributes related to an entity.

59 NOTE – Within a particular context, an identity can have one or more identifiers to allow an entity to be uniquely
60 recognized within that context.

61 **3.1.9 multifactor authentication** [b-ISO/IEC 19790]: Authentication with at least two independent
62 authentication factors.

63 **3.1.10 non-repudiation** [b-ITU-T X.1252]: The ability to protect against denial by one of the entities
64 involved in an action of having participated in all or part of the action.

65 **3.1.11 repudiation** [b-ITU-T X.1252]: Denial in having participated in all or part of an action by one
66 of the entities involved.

67 **3.2 Terms defined in this Recommendation**

68 This Recommendation defines the following terms:

69 **3.2.1 authentication protocol**: A defined sequence of messages between an entity and a verifier that
70 enables the verifier to perform authentication of an entity.

71 **3.2.2 authoritative source**: A repository which is recognized as being an accurate and up-to-date
72 source of information.

73 **3.2.3 credential service provider (CSP)**: A trusted actor that issues and/or manages credentials.

74 **3.2.4 entity authentication assurance (EAA)**: A degree of confidence reached in the authentication
75 process that the entity is what it is, or is expected to be (this definition is based on the 'authentication
76 assurance' definition given in [b-ITU-T X.1252]).

77 NOTE – The confidence is based on the degree of confidence in the binding between the entity and the identity
78 that is presented.

79 **3.2.5 identifier**: One or more attributes that uniquely characterize an entity in a specific context.

80 **3.2.6 identity information verification**: A process of checking identity information and credentials
81 against issuers, data sources or other internal or external resources with respect to authenticity, validity,
82 correctness and binding to the entity.

83 **3.2.7 identity proofing**: The process by which the registration authority (RA) captures and verifies
84 sufficient information to identify an entity to a specified or understood level of assurance.

85 **3.2.8 man-in-the-middle attack**: An attack in which an attacker is able to read, insert and modify
86 messages between two parties without their knowledge.

87 **3.2.9 mutual authentication**: The authentication of identities of entities which provides both entities
88 with assurance of each other's identity.

89 **3.2.10 phishing**: A scam by which an email user is duped into revealing personal or confidential
90 information which the scammer can then use illicitly.

91 **3.2.11 registration authority (RA)**: A trusted actor that establishes and/or vouches for the identity of
92 an entity to a credential service provider (CSP).

93 **3.2.12 relying party (RP)**: Actor that relies on an identity assertion or claim.

94 **3.2.13 salt**: A non-secret, often random value that is used in a hashing process.

95 NOTE – It is also referred to as sand.

96 **3.2.14 shared secret**: A secret used in authentication that is known only to the entity and the verifier.

97 **3.2.15 time stamp**: This is a reliable time variant parameter which denotes a point in time with respect
98 to a common reference.

99 **3.2.16 transaction:** A discrete event between an entity and service provider that supports a business or
100 programmatic purpose.

101 **3.2.17 trust framework:** A set of requirements and enforcement mechanisms for parties exchanging
102 identity information.

103 **3.2.18 trusted third party (TTP):** An authority or its agent, trusted by other actors with respect to
104 specified activities (e.g., security-related activities).

105 NOTE – A trusted third party is trusted by an entity and/or a verifier for the purposes of authentication.

106 **3.2.19 validity period:** The time period during which an identity or credential may be used in one or
107 more transactions.

108 **3.2.20 verification:** The process of checking information by comparing the provided information with
109 previously corroborated information.

110 **3.2.21 verifier:** The actor that corroborates identity information.

111 NOTE – The verifier can participate in multiple phases of the EAAF and can perform credential verification
112 and/or identity information verification.

113 **4 Abbreviations and acronyms**

114 This Recommendation uses the following abbreviations and acronyms:

115	AL	Assurance Level (syn. Level of Assurance (LoA))
116	CA	Certification Authority
117	CSP	Credential Service Provider
118	EAA	Entity Authentication Assurance
119	EAAF	Entity Authentication Assurance Framework
120	ICT	Information and Communication Technology
121	IdM	Identity Management
122	IP	Internet Protocol
123	LoA	Level of Assurance (syn. AL)
124	LoAs	Levels of Assurance (syn. ALs)
125	MAC	Media Access Control
126	NPE	Non-Person Entity
127	PDA	Personal Digital Assistant
128	PII	Personally Identifiable Information
129	PIN	Personal Identification Number
130	RA	Registration Authority
131	RP	Relying Party
132	SAML	Security Assertion Markup Language
133	TCP/IP	Transmission Control Protocol/Internet Protocol

134	TLS	Transport Layer Security
135	TPM	Trusted Platform Module
136	TTP	Trusted Third Party
137	URL	Uniform Resource Locator

138 **5 Conventions**

139 This Recommendation applies the following verbal forms for the expression of provisions:

- 140 a) "shall" indicates a requirement
- 141 b) "should" indicates a recommendation
- 142 c) "may" indicates a permission
- 143 d) "can" indicates a possibility and a capability.

144 **6 Levels of assurance**

145 {KI.6#01: [KI-SAC] provides criteria at four Assurance Levels which share the descriptions and explanations offered in this
 146 section. Indeed, much of the broad material in this section is taken verbatim from [b-OMB], and other parts of this text
 147 addressing specific LoAs are based on Kantara input during the drafting process, drawn from [KI-LoA]. Therefore the
 148 Kantara IAF is consistent with the concept of, and expectations of rigour associated with, the LoA described in this section.
 149 Furthermore, §6.6 and §6.7 are derived largely from Kantara input.}

150 This entity authentication assurance framework (EAAF) defines four levels of assurance (LoA) for
 151 entity authentication. Each LoA describes the degree of confidence in the processes leading up to and
 152 including the authentication process itself, thus providing assurance that the entity that uses a particular
 153 identity is in fact the entity to which that identity was assigned. For the purposes of this
 154 Recommendation, an LoA is a function of the processes, management activities and technical controls
 155 that have been implemented by a credential service provider (CSP) for each of the EAAF phases based
 156 on the criteria set forth in clause 10. Entity authentication assurance (EAA) is affected by management
 157 and organizational considerations, but this Recommendation does not provide explicit normative criteria
 158 for these considerations. An entity can be a human or a non-person entity (NPE).

159 *«source text excised»*

160 LoA1 is the lowest level of assurance, and LoA4 is the highest level of assurance specified in this
 161 Recommendation. Determining which LoA is appropriate in a given situation depends on a variety of
 162 factors. The determination of the required LoA is based mainly on risk: the consequences of an
 163 authentication error and/or misuse of credentials, the resultant harm and impact, and their likelihood of
 164 occurrence. Higher LoAs shall be used for higher perceived risk.

165 The EAAF provides requirements and implementation guidance for each of the four LoAs. In particular,
 166 it provides requirements for the implementation of processes for the following phases:

- 167 a) enrolment (e.g., identity proofing, identity information verification, registration)
- 168 b) credential management (e.g., credential issuance, credential activation)
- 169 c) authentication.

170 It also provides guidance regarding management and organizational considerations (e.g., legal
 171 compliance, information security management) that affect entity authentication assurance.

172

Table 6-1 – Levels of assurance²

Level	Description
1 – Low	Little or no confidence in the claimed or asserted identity
2 – Medium	Some confidence in the claimed or asserted identity
3 – High	High confidence in the claimed or asserted identity
4 – Very high	Very high confidence in the claimed or asserted identity

173 This framework contains requirements to achieve a desired LoA for each entity authentication assurance
 174 framework phase. The overall LoA achieved by an implementation using this framework will be the
 175 level of the phase with the lowest LoA.

176 **6.1 Level of assurance 1 (LoA1)**

177 At LoA1, there is minimal confidence in the claimed or asserted identity of the entity, but some
 178 confidence that the entity is the same over consecutive authentication events. This LoA is used when
 179 minimum risk is associated with erroneous authentication. There is no specific requirement for the
 180 authentication mechanism used; only that it provides some minimal assurance. A wide range of
 181 available technologies, including the credentials associated with higher LoAs, can satisfy the entity
 182 authentication assurance requirements for this LoA. This level does not require use of cryptographic
 183 authentication methods (e.g., cryptographic-based challenge-response protocol).

184 For example, LoA1 may be applicable for authentication in which an entity presents a self-registered
 185 username or password to a service provider's website to create a customized page, or transactions
 186 involving websites that require registration for access to materials and documentation, such as news or
 187 product documentation.

188 For example, at LoA1, a media access control (MAC) address may satisfy a device authentication
 189 requirement. However, there is little confidence that another device will not be able to use the same
 190 MAC address.

191 **6.2 Level of assurance 2 (LoA2)**

192 At LoA2, there is some confidence in the claimed or asserted identity of the entity. This LoA is used
 193 when moderate risk is associated with erroneous authentication. Single-factor authentication is
 194 acceptable. Successful authentication shall be dependent upon the entity proving, through a secure
 195 authentication protocol, that the entity has control of the credential. Controls should be in place to
 196 reduce the effectiveness of eavesdroppers and online guessing attacks. Controls shall be in place to
 197 protect against attacks on stored credentials.

198 For example, a service provider might operate a website that enables its customers to change their
 199 address of record. The transaction in which a beneficiary changes an address of record may be
 200 considered an LoA2 authentication transaction, as the transaction may involve a moderate risk of
 201 inconvenience. Since official notices regarding payment amounts, account status, and records of
 202 changes are usually sent to the beneficiary's address of record, the transaction additionally entails
 203 moderate risk of unauthorized release of PII. As a result, the service provider should obtain at least some
 204 authentication assurance before allowing this transaction to take place.

² LoA is a function of the processes, management activities, and technical controls that have been implemented by a CSP for each of the EAAF phases based on the criteria set forth in clause 10.

205 **6.3 Level of assurance 3 (LoA3)**

206 At LoA3, there is high confidence in the claimed or asserted identity of the entity. This LoA is used
207 where substantial risk is associated with erroneous authentication. This LoA shall employ multifactor
208 authentication. Any secret information exchanged in authentication protocols shall be cryptographically
209 protected in transit and at rest (although LoA3 does not require the use of a cryptographic-based
210 challenge-response protocol). There are no requirements concerning the generation or storage of
211 credentials; they may be stored or generated in general purpose computers or in special purpose
212 hardware.

213 For example, a transaction in which a company submits certain confidential information electronically
214 to a government agency may require an LoA3 authentication transaction. Improper disclosure could
215 result in a substantial risk for financial loss. Other LoA3 transaction examples include online access to
216 accounts that allow the entity to perform certain financial transactions, or use by a third party contractor
217 of a remote system to access potentially sensitive client personal information.

218 **6.4 Level of assurance 4 (LoA4)**

219 At LoA4, there is very high confidence in the claimed or asserted identity of the entity. This LoA is used
220 when high risk is associated with erroneous authentication. LoA4 provides the highest level of entity
221 authentication assurance defined by this Recommendation. LoA4 is similar to LoA3, but it adds the
222 requirements of in-person identity proofing for human entities and the use of tamper-resistant hardware
223 devices for the storage of all secret or private cryptographic keys. Additionally, all PII and other
224 sensitive data included in authentication protocols shall be cryptographically protected in transit and at
225 rest.

226 For example, services where there is a potential high risk for harm or distress in the case of an
227 authentication failure may require LoA4 protection. The responsible party needs full assurance that the
228 correct entity provided certain critical information, and the responsible party may even be criminally
229 liable for any failure to verify the information. Finally, approval of a transaction involving high risk of
230 financial loss may be an LoA4 transaction.

231 *«source text excised»*

232 **6.5 Selecting the appropriate level of assurance**

233 Selection of the appropriate LoA should be based on a risk assessment of the transactions or services for
234 which the entities will be authenticated. By mapping impact levels to LoAs, parties to an authentication
235 transaction can determine what LoA they require and can procure services and place reliance on assured
236 identities accordingly. Table 6-2 indicates possible consequences and impacts of authentication failure
237 at the various LoAs.

238

Table 6-2 – Potential impact at each level of assurance

Possible consequences of authentication failure	Potential impact of authentication failure by LoA			
	1	2	3	4
Inconvenience, distress or damage to standing or reputation	Min*	Mod	Sub	High
Financial loss or agency liability	Min	Mod	Sub	High
Harm to the organization, its programs or public interests	N/A	Min	Mod	High
Unauthorized release of sensitive information	N/A	Mod	Sub	High
Personal safety	N/A	N/A	Min Mod	Sub High
Civil or criminal violations	N/A	Min	Sub	High
* Min=Minimum; Mod=Moderate; Sub=Substantial; High=High.				

239 Determination of what constitutes minimum, moderate, substantial, and high risk depends on the risk
 240 criteria defined by the organization using this Recommendation for each of the possible consequences.
 241 Additionally, it is possible to have multiple impact scenarios (e.g., consequences could include harm to
 242 the organization, as well as, unauthorized release of sensitive information). In multiple impact scenarios,
 243 the highest LoA corresponding to the consequences should be used.

244 Each LoA shall be determined by the strength and rigour of the controls and processes for each phase of
 245 the EAAF that the CSP applies to the provision of its service. The EAAF establishes a need for
 246 operational service assurance criteria at each LoA for CSPs. Service assurance criteria are introduced in
 247 clause 11, but specific requirements are out of scope for this Recommendation.

248 There may be other business related factors to take into account, beyond the scope of security, when
 249 using the results of the risk assessment to determine the applicable LoA. Such business factors may
 250 include:

- 251 a) the organization's approach to managing residual risk;
- 252 b) the organization's appetite for accepting risk in terms of the impacts shown in Table 6-2;
- 253 c) the business objectives for the service (e.g., a service with the business objective of driving
 254 uptake may be better served by a lower LoA using a credential such as a password, if the
 255 organization has processes in place to mitigate fraud and is comfortable accepting the risk of
 256 fraud).

257 The risk assessment of a transaction may be conducted as a part of an organization's overall information
 258 security risk assessment (e.g., ISO/IEC 27001) and should focus on the specific need for security in the
 259 transactions being contemplated. The risk assessment shall address risk related to EAA. The results of
 260 the risk assessment shall be compared to the four LoAs. The LoA that best matches the results of the
 261 risk assessment shall be selected.

262 Where multiple classes of transactions are envisaged, it is possible that a different LoA applies to each
 263 transaction or to groups of transactions. In other words, multiple LoAs may be accepted by a single
 264 organization, according to the specific transaction in question.

265 **6.6 LoA mapping and interoperability**

266 Different domains may define LoAs differently. These LoAs will not necessarily support a one-to-one
267 mapping to the four LoAs described in this framework. For example, one domain may adopt a four-level
268 model, and another domain may adopt a five-level model. The various criteria for the different
269 authentication models must be separately defined and widely communicated.

270 In order to achieve interoperability between different LoA models, each domain shall explain how its
271 mapping scheme relates to the LoAs defined in this Recommendation by:

- 272 a) developing a well-defined entity authentication assurance methodology, including well defined
273 categories of LoAs; and
- 274 b) widely publishing this methodology so that organizations wishing to enter into federation-type
275 agreements with them can clearly understand each other's processes and terminology.

276 The LoA methodology shall take into account and clearly define LoAs in terms of a risk assessment that
277 specifies and quantifies:

- 278 a) expected threats;
- 279 b) impacts (i.e., min, mod) should threats become reality;
- 280 c) identification of threats that must be controlled at each LoA;
- 281 d) recommended security technologies and processes for use in implementing controls at each
282 LoA, such as specifying a credential to be carried on a hardware device (e.g., smart card) or
283 specifying requirements for the generation and storage of credentials;
- 284 e) criteria for determining the equivalence of different combinations of authentication factors
285 taking into account both identity proofing and associated credentials.

286 One approach to address the issue of mapping/bridging between different LoA models may be to use the
287 four-level model defined in this document and map other n-level models against it. This method would
288 allow identity federations using different models for authentication assurance to map against the four-
289 level model. Mappings shall define how un-mapped LoAs will be handled, which may be to simply
290 ignore them or to effectively map them to the next lowest level (since there could be no basis for
291 assuming a higher LoA if it had not been specifically determined beforehand).

292 **6.7 Exchanging authentication results based on the 4 LoAs**

293 Actors participating in an authentication transaction (e.g., CSPs, RPs) may need to exchange
294 information to complete the transaction or activity.

295 The range of actions includes, but is not limited to, the following:

- 296 a) allowing an RP to express its expectations for the LoA at which an entity should be
297 authenticated;
- 298 b) allowing an entity or CSP to indicate the actual LoA in its responses;
- 299 c) allowing an entity or CSP to advertise those LoAs for which it has been certified capable of
300 meeting the requirements associated with that LoA.

301 Actors participating in an authentication transaction shall agree on the protocol, semantics, format and
302 structure of the information to be exchanged. The RP may need to specify if it will accept any
303 authentication response other than that exactly requested.

304 While digital certificates are an established way to convey information concerning the assurance of
305 related credentials, metadata is increasingly being used as a method to communicate what assurance

306 requirements the exchanging parties have. A 'Context Class', such as a 'Security Assertion Markup
307 Language (SAML) Authentication Context Class' in the form of a uniform resource locator (URL), is a
308 well-known mechanism for parties to express those classes concerning authentication assurance in
309 authentication requests and assertions. For example, a typical assertion from an identity provider might
310 convey information such as "This user is John Doe; he has an email address of john.doe@example.com,
311 and he was authenticated into this system using a password mechanism."

312 The remainder of this framework addresses the structure within which processes and requirements for
313 services are established and the threats and impacts relating to entity authentication. It concludes with an
314 overview of the need for service assurance criteria against which services may be assessed to ensure that
315 the appropriate LoA is assigned to achieve adequate credential services.

316 **7 Actors**

317 The actors involved in the EAAF include entities, CSPs, RAs, RPs, verifiers and TTPs. These actors
318 may belong to a single organization or separate organizations. There may be a variety of relationships
319 and capabilities provided by a number of organizations including shared or interacting components,
320 systems and services.

321 {KI.7#01: There are many ways to view and describe the elements of a broad identity assurance framework and the various
322 roles within it, any of which may be fulfilled by a discrete entity, or by a single entity fulfilling two or more of those roles,
323 depending upon the nature of the entity and the business and process models they employ. This section can be
324 accommodated by CSPs wishing to show conformity to [KI-SAC], according to how they define their service and the set of
325 (Kantara) criteria which they intend to fulfil. [X.1254] does not develop specific criteria to the level which is accomplished
326 in [KI-SC] and therefore the disposition of source requirements to the actors defined hereafter is not as precise as may be the
327 case with [KI-SAC]. Furthermore, the term 'CSP' is used within Kantara Very broadly and inclusively, and terms which
328 define a sub-set of the full functionality covered by [KI-SAC] are not generally used, e.g. an 'RA' is considered to be a
329 functional sub-set of a 'CSP'. }

330 **7.1 Entity**

331 An entity can have its identity authenticated. The ability to authenticate an entity depends on a number
332 of factors. In the context of this framework, the ability to authenticate an entity implies that the entity
333 has been registered and issued the appropriate credentials by a CSP and that an authentication protocol
334 has been specified. During authentication, the entity may attest to its own identity. It is also possible that
335 there is a separate party representing the entity for the purposes of authentication.

336 **7.2 Credential service provider**

337 A credential service provider (CSP) issues and/or manages credentials or the hardware, software and
338 associated data that can be used to produce credentials. Passwords and biometric data are examples of a
339 credential that may be issued and managed by a CSP. Smart cards containing private keys are an
340 example of hardware and associated data (that can be used to produce credentials) that may be issued
341 and managed by a CSP. A CSP may also issue and manage data that can be used to authenticate
342 credentials. If passwords are used as credentials, this data may be the values of one-way functions of the
343 passwords. If credentials are based on digitally-signed information, CSPs may produce public key
344 certificates that can be used by verifiers. The credentials that are issued and supported, as well as the
345 safeguards that are implemented by the CSP, are key factors in determining which LoA will be reached
346 during a particular authentication transaction (see also clause 10.3).

347 Every entity shall be issued one or more credentials, or the means to produce credentials, to enable later
348 authentication. Credentials, or the means to produce credentials, are typically only issued after
349 successful completion of an enrolment process, at the end of which the entity is registered.

350 **7.3 Registration authority**

351 A Registration Authority (RA) establishes and/or vouches for the identity of an entity to a CSP. The RA
352 shall be trusted by the CSP to execute the processes related to the enrolment phase and register entities
353 in a way that allows later assignment of credentials by the CSP.

354 Each RA shall perform some form of identity proofing and identity information verification according
355 to a specified procedure. In order to differentiate the entity from other entities, an entity is typically
356 assigned one or more identifiers, which will allow the entity to be recognized later in the applicable
357 context.

358 **7.4 Relying party**

359 An RP is an actor that relies on an identity claim or assertion. The relying party may require an
360 authenticated identity for a variety of purposes, such as account management, access control,
361 authorization decisions, etc. The relying party may itself perform the operations necessary to
362 authenticate the entity, or it may entrust these operations to a third party.

363 **7.5 Verifier**

364 The verifier is an actor that corroborates identity information. The verifier can participate in multiple
365 phases of EAA and can perform credential verification and/or identity information verification.

366 **7.6 Trusted third party**

367 A TTP is an authority or its agent, trusted by other actors with respect to certain activities (e.g., security-
368 related activities). For this framework, a TTP is trusted by an entity and/or a verifier for the purposes of
369 authentication. Examples of TTPs for the purposes of entity authentication include certification
370 authorities (CAs) and time-stamping authorities.

371 **8 Entity authentication assurance framework phases**

372 This clause provides a description of the phases and processes of EAA. Although some EAA models
373 may differ from the structure of this model, conformance to this model requires that functional
374 capabilities fully meet the requirements set out in this framework. This framework is technology neutral.

375 Organizations adopting this framework shall establish policies, procedures and capabilities that provide
376 the necessary supporting processes and fulfil requirements set forth in this framework. These will vary
377 according to the role chosen by a particular organization and, for instance, the LoAs at which an
378 organization provides credentials. For example, an organization may be subject to:

- 379 a) requirements for particular actions on behalf of the organization or its representatives related to
380 particular LoAs;
- 381 b) requirements for external or third party assessment of an organization's operational capability
382 within the EAAF;
- 383 c) policies, actions and capabilities necessary to establish the trustworthiness of the processes,
384 services and capabilities provided by organizations adopting the framework.

385 {KI.8#01: In providing for the Approval of a CSP, be it for a Full or a Component service, the Kantara IAF aligns to all of
386 the above requirements, specifically: with regard to §8 a) and c) above, [KI-SAC] sets out requirements which CSPs must
387 fulfill prior to being granted a Kantara Approval and [KI-AAS] in concert with [KI-RAA] defines the processes involved;
388 regarding §8 b), Approval is recommended after review of a report from a Kantara-Accredited Assessor (accredited
389 according to [KI-AAS] and [KI-AQR]), who executes a third-party assessment and reports on their findings as to whether
390 conformity exists (also following processes defined in [KI-AAS] and [KI-RAA]).}

391 8.1 Enrolment phase

392 The enrolment phase consists of four processes: application and initiation, identity proofing, identity
 393 verification, and record-keeping/recording. These processes may be conducted entirely by a single
 394 organization, or they may consist of a variety of relationships and capabilities provided by a number of
 395 organizations including shared or interacting components, systems and services.

396 {KI.8.1#01: The required processes differ according to the rigour required by the applicable LoA. In the
 397 case of an entity enrolling under LoA1, these processes are minimal (e.g., an individual may click a
 398 "new user" button on a webpage and create a username and password). In other cases, enrolment
 399 processes may be extensive.

400 {AL*_ID_IDV#000}

401 {KI.8.1#02: For example, enrolment at LoA4 requires an in-person meeting between the entity and the
 402 RA, as well as extensive identity proofing.

403 {AL4_ID_IDV#000}

404 8.1.1 Application and initiation

405 {KI.8.1.1#01: The enrolment phase is initiated in a variety of ways. For instance, it may be initiated
 406 pursuant to a request made by entities seeking to obtain a particular credential themselves (e.g., when a
 407 new user of a website wishes to obtain a username and password). It is equally possible that the
 408 enrolment process is initiated by a third party on behalf of the entity or by the CSP itself
 409 (e.g., government-issued identification card, employee badge). For example, at higher LoAs,
 410 applications may be accepted only where the entity has been sponsored by a third party.

411 {Refer to the definitions of 'Subject' and 'Subscriber' in [KI-GLOSS], which encompass these concepts.}

412 {KI.8.1.1#02: In any event, the initiation process of the enrolment phase for humans may involve the
 413 completion of an application form. This form should record sufficient information to ensure the entity
 414 may be identified uniquely within a context (e.g., by recording the full name, date and place of birth).

415 {AL*_CO_NUI#020, AL*_ID_POL#010, AL*_ID_POL#020, AL*_CM_CRN#030}

416 *«source text excised»*

417 {KI.8.1.1#03: CSPs shall set forth the terms under which enrolment is provided and under which the
 418 services associated with that enrolment shall be used.

419 {AL*_CO_NUI#020}

420 {KI.8.1.1#04: The terms of services associated with the enrolment may be established pursuant to a trust
 421 framework.

422 {AL*_ID_IDV#010}

423 {KI.8.1.1#05: Where appropriate, liability disclaimers or other legal provisions shall be accepted by, or
 424 on behalf of, the entity prior to continuation of the enrolment processes.

425 {AL*_CO_NUI#040}

426 8.1.2 Identity proofing and identity information verification

427 Identity proofing is the process of capturing and verifying sufficient information to identify an entity to
 428 a specified or understood level of assurance. Identity information verification is the process of checking
 429 identity information and credentials against issuers, data sources or other internal or external resources
 430 with respect to authenticity, validity, correctness and binding to the entity. Depending on the context, a
 431 variety of identity information (e.g., government identity cards, driver's licences, biometric information,

432 machine-based attestation, birth certificates) issued or approved by authoritative sources may fulfil
433 identity proofing requirements.

434 {KI.8.1.2#01: The actual identity information presented to fulfil identity proofing requirements varies
435 with the LoA. Such requirements may also be influenced by the class and context of identity proofing
436 being performed (e.g. in-person, remote, current relationship or affiliation) or by a specific framework
437 or federation within they are determined.

438 {AL*_CO_NUI#0120, AL*_CO_NUI#020, AL*_ID_IDV#010,
439 AL*_ID_IPV#010, AL1/2/3_ID_RPV#010, AL2/3_ID_CRV#010, AL2/3/4_ID_AFV#000, AL2/3/4_ID_AFV#010}

440 {KI.8.1.2#02: Identity proofing may include the physical checking of presented identity documents to
441 detect possible fraud, tampering or counterfeiting. Identity proofing may also include checking to ensure
442 the identity is used in other contexts (i.e., verified from other RAs). The identity proofing requirements
443 shall be more stringent the higher the LoA. Also, the identity proofing process shall be more stringent
444 for entities asserting or claiming an identity remotely (e.g., via an online channel) than locally (e.g., in
445 person with the RA).

446 { AL*_CO_NUI#020, AL*_ID_IPV#020,
447 AL1/2/3_ID_IPV#020, AL4_ID_IPV#030, AL4_ID_IPV#040, AL4_ID_IPV#050,
448 AL1/2/3_ID_RPV#020, AL2/3_ID_CRV#020, AL2/3/4_ID_AFV#020}

449 The stringency of identity proofing requirements is based on the objectives that must be met for each
450 LoA.

451 {KI.8.1.2#03: At LoA1, the only objective is to ensure the identity is unique within the intended context.
452 The identity should not be associated with two different entities.

453 {AL1_ID_POL#010, AL1_ID_POL#020}

454 {KI.8.1.2#04: At LoA2, there are two objectives. First, the identity shall be unique in the context.

455 {AL2_ID_POL#010, AL2_ID_POL#020}

456 {KI.8.1.2#05: Second, the entity to which the identity pertains shall exist objectively, which means the
457 identity is not fictitious or intentionally fabricated for fraudulent purposes.³ For example, human
458 identity proofing at LoA2 may include checking birth and death registers to ensure some provenance
459 (although it does not prove that the entity in possession of a birth certificate is the entity to which the
460 birth certificate relates).

461 {AL2_ID_IPV#020, AL2_ID_RPV#020, AL2_ID_CRV#020, AL2_ID_AFV#020}

462 «source text excised»

463 {KI.8.1.2#06: LoA3 includes the objectives of LoA1 and LoA2, as well as the objective of verifying the
464 identity information through one or more authoritative sources, such as an external database. Identity
465 information verification shows that the identity is in use and links to the entity. However, there is no
466 assurance that identity information is in the possession of the real or rightful owner of the identity.

467 {AL3_ID_POL#010, AL3_ID_POL#020, AL3_ID_IPV#020, AL3_ID_RPV#020, AL3_ID_CRV#020, AL3_ID_AFV#020}

468 {KI.8.1.2#07: For humans, LoA4 adds one additional objective to LoA3 by requiring entities to be
469 witnessed in person to help protect against impersonation.

470 {AL4_ID_POL#010, AL4_ID_POL#020, AL4_ID_IPV#030, AL4_ID_IPV#040, AL4_ID_IPV#050

471 NOTE – this clause is a very indirect assertion that only in-person proofing is permitted at AL4,
472 which is explicitly stated by AL4_ID_IDV#000}

³ This does not preclude the use of pseudonyms.

473 {KI.8.1.2#08: Identity proofing processes at a higher LoA shall include the processes of the lower LoAs.
474 For example, LoA3 identity proofing assumes that LoA1 and LoA2 identity proofing controls have been
475 satisfied.

476 {NOTE – Whilst this is a generally correct statement, it ignores the fact that, even within [X.1254], there
477 are contradictions to this generality, e.g. not allowing pseudonyms at higher ALs, or only allowing in-
478 person proofing at AL4. Certainly within [KI-SAC], some criteria either become inapplicable at higher
479 ALs or are introduced at higher ALs, hence the normative phrasing of this clause is not consistent with
480 actual requirements in [X.1254] or [KI-SAC], although the latter makes no such explicit claim and readily
481 distinguishes when the general rule is not applicable. }

482

483

484

Table 8-1 – Applying identity proofing objectives to the LoAs

LoA	Description	Objective	Controls	Method of processing ⁴
LoA1 – low	Little or no confidence in the claimed or asserted identity	Identity is unique within a context	Self-claimed or self-asserted	Local or remote
LoA2 – medium	Some confidence in the claimed or asserted identity	Identity is unique within context and the entity to which the identity pertains exists objectively	Proof of identity through use of identity information from an authoritative source	Local or remote
LoA3 – high	High confidence in the claimed or asserted identity	Identity is unique within context, entity to which the identity pertains exists objectively, identity is verified, and identity is used in other contexts	Proof of identity through use of identity information from an authoritative source + identity information verification	Local or remote
LoA4 – very high	Very high confidence in the claimed or asserted identity	Identity is unique within context, entity to which the identity pertains exists objectively, identity is verified, and identity is used in other contexts	Proof of identity through use of identity information from multiple authoritative sources + identity information verification + entity witnessed in person ⁵	Local only

485 {NOTE - The foregoing text and mappings are considered to have addressed the requirements summarized in the
486 table above and hence no further mapping within the table itself is felt necessary or helpful. }

487 Required LoA controls to protect against threats to enrolment shall be determined by the use of controls
488 listed in clause 10.1.2.

489 {KI.8.1.2#09: Any implementation of the EAAF relies on (a subset of) the identity information and
490 sources that are available to prospective entities and/or to the RA.

491 The reliability and accuracy of these credentials, identity information and sources determine the actual
492 assurance provided by the enrolment phase. Consequently, implementers of the EAAF shall carefully
493 consider the assurance provided by the identity (management) infrastructures that are used by the
494 different sources and issuers when deciding which credentials, identity information and/or sources to
495 rely on for identity proofing and identity information verification purposes. Any implementation of the
496 EAAF shall involve the publication of a document (e.g., identity proofing policy as described in clause

⁴ Remote identity proofing is accomplished over a network and therefore involves not being able to physically see the entity whereas local identity proofing is accomplished in a manner that requires physically seeing the entity.

⁵ The witnessed in-person control applies only to human entities.

497 10.1.2.1) which provides an overview of the identity information, sources and/or issuers that are relied
 498 upon in support of the enrolment phase.

499 {AL*_CO_NUI#020, AL2/3/4_ID_POL#030, AL2/3/4_ID_POL#040, AL2/3/4_ID_IDV#010}

500 8.1.3 Record-keeping/recording

501 {KI.8.1.3#01: This is the process of concluding the enrolment of an entity. It is the record-keeping
 502 process of the enrolment phase in which a record of the enrolment is created. This record shall include
 503 the information and documentation that was collected (and may be retained), information about the
 504 identity information verification process, the results of these steps, and other pertinent data. A decision
 505 is then rendered and recorded to accept, deny or refer the enrolment for further examination or other
 506 follow up.

507 {AL*_CO_NUI#050, AL2/3/4_CO_SER#010, AL*_CM_CSM#010, AL2/3/4_ID_IDC#020, AL2/3/4_ID_VRC#010,
 508 AL2/3/4_ID_VRC#020, AL2/3/4_ID_VRC#030, AL2/3/4_CM_CRN#090, AL2_CM_CRN#095, AL3/4_CM_SER#010}

509 8.1.4 Registration

510 {KI.8.1.4#01: Registration is a process in which an entity requests to use a service or resource. Although
 511 the registration process is generally considered as a part of an enrolment process, such that it is
 512 performed at the end of the enrolment phase, it may also be performed at a later time. Unlike other
 513 processes in enrolment that are likely to be necessary only once, registration may be necessary when an
 514 entity requests access to each service or resource for the first time.

515 {NOTE – Kantara does not consider there to be any distinction between enrollment and registration – it
 516 uses the latter term to refer to the steps involved in accepting an application, performing identity proofing
 517 and vetting, issuing credentials, recording the facts of those actions and entering the details of the subject
 518 and their credential into a registry. Use of that credential is either explicitly enabled or would be the
 519 subject of an authentication service offered to a party relying on the previously-issued credential, such
 520 determinations being dependent on the nature of the service being submitted to Kantara for assessment and
 521 Approval.}

522 8.2 Credential management phase

523 The credential management phase comprises all processes relevant to the lifecycle management of a
 524 credential, or the means to produce credentials, which enables the user to participate in an activity or
 525 context. The credential management phase may involve some or all of the following processes: creation
 526 of credentials, issuance of credentials or of the means to produce credentials, activation of credentials or
 527 the means to produce credentials, storage of credentials, revocation and/or destruction of credentials or
 528 of the means to produce credentials, renewal and/or replacement of credentials or the means to produce
 529 credentials, and record-keeping. Some of these processes depend on whether the credential is carried on
 530 a hardware device.

531 {NOTE – The sub-clauses to this section are somewhat bereft of hard requirements, hence the referenced
 532 tags from [KI-SAC] are more a collective grouping than a one-to-one or one-to-many mapping at a discrete
 533 level.}

534 8.2.1 Credential creation

535 {KI.8.2.1#01: The credential creation process encompasses all necessary processes to create a credential,
 536 or the means to produce a credential, for the first time. These processes may include pre-processing,
 537 initialization, and binding.

538 {§5.*.2.1 deals with this topic, for each AL.}

539 8.2.1.1 Credential pre-processing

540 {KI.8.2.1.1#01: Some credentials, or the means to produce credentials, require pre-processing before
541 issuance, such as personalization where a credential is customized to the entity's identity.
542 Personalization can take many different forms depending on the credential. For instance, the
543 personalization of a smart card that holds credentials may involve printing (on the outside of the card) or
544 writing (to the card's chip) the name of the entity to which the card will be issued. There are also
545 credentials that do not require personalization, such as passwords.

546 { [KI-SAC] does not explicitly address pre-processing/personalization of credentials. However,
547 the following criteria address the characteristics required of various credentials and tokens,
548 which, by design, must be conducted prior to initialization and binding:
549 AL*_CM_CRN#040, AL2/3/4_CM_CRN#050, AL2_CM_CRN#055, AL2/3/4_CM_CRN#060, AL2/3/4_CM_CRN#070,
550 AL4_CM_CRN#075, AL3/4_CM_CRN#080 }

551 8.2.1.2 Credential initialization

552 {KI.8.2.1.2#01: Credential initialization encompasses all steps to ensure that a means to produce a
553 credential will later be able to support the functionalities that it is expected to support. For instance, a
554 smart card chip might be required to calculate the cryptographic key pairs necessary to later support the
555 generation of digital signatures. Similarly, a smart card might be issued in a "locked" state that requires
556 a PIN during the activation process.

557 {AL3/4_CM_SKP#010, AL3/4_CM_SKP#010 }

558 8.2.1.3 Credential binding

559 {KI.8.2.1.3 #01: Binding is the process of establishing an association between a credential, or the means
560 to produce a credential, and the entity to which it will be issued. How binding is accomplished and the
561 confidence in the binding association varies with the LoA. For instance, in an online scenario when
562 binding an entity's persistent pseudonymous identifier to the entity's customer record, a first time
563 "activation code" may be carried through the binding process in a session-only encrypted cookie over a
564 secured channel. Alternatively, the activation code may be requested at the end of the process once the
565 entity-to-persistent identifier binding step has been completed, in order to bind the persistent identifier
566 to the customer record.

567 {AL*_CM_CRN#010, AL2/3/4_CM_CRN#020, AL*_CM_CRN#030 }

568 8.2.2 Credential issuance

569 {KI.8.2.2#01: Credential issuance is the process of providing or otherwise associating an entity with a
570 particular credential, or the means to produce a credential. The complexity of this process varies with
571 the LoA required. Higher LoAs, will require secure delivery of a hardware device (e.g., a smart card)
572 that holds a credential and may require in-person delivery of the device. In the case of lower LoAs, the
573 issuance process might be as simple as sending a password or PIN to the entity's physical or email
574 address.

575 {AL2/3/4_CM_CRD#010, AL2/3_CM_CRD#016, AL3/4_CM_CRD#017, AL3_CM_CRD#018 }

576 «source text excised»

577 8.2.3 Credential activation

578 {KI.8.2.3#01: Credential activation is the process whereby a credential, or the means to produce
579 credentials, is made ready for use. The activation process may involve a variety of measures depending
580 on the credential. For instance, a credential, or the means to produce credentials, may have been
581 "locked" after its initialization until the moment of issuance to the entity to prevent interim misuse. In
582 such cases, activation may involve the "unlocking" of the credential (e.g., use of a password).

583 A credential, or the means to produce credentials, can also be re-activated after a suspension where its
 584 validity has been temporarily stopped.
 585 {AL3/4_CM_CRD#020, AL2/3/4_ID_IDC#030}

586 **8.2.4 Credential storage**

587 Credential storage is the process whereby credentials, or the means to produce credentials, are securely
 588 stored in a way that protects against their unauthorized disclosure, use, modification or destruction.
 589 Credential storage involves the entity associated with a credential and actions required to prevent the
 590 unauthorized use of a credential.

591 Credential storage does not necessarily include protection of information used to check that a credential
 592 is legitimate, if that information is not part of the credential. The protection of information, such as
 593 tables of hashed passwords required for authentication, is required at higher LoAs.

594 **8.2.5 Credential suspension, revocation and/or destruction**

595 Revocation is the process whereby the validity of a credential is permanently ended. Suspension is a
 596 related process whereby the validity of a credential is temporarily stopped.

597 {KI.8.2.5#01: Revocation may be appropriate in many different instances. Revocation shall occur in the
 598 following instances:

- 599 a) a credential, or a means to produce a credential, has been reported lost, stolen or otherwise
 600 compromised;
- 601 b) a credential has expired;
- 602 c) the basis for a credential no longer exists (e.g., when an employee leaves her employer);
- 603 d) a credential has been used for unauthorized purposes; or
- 604 e) a different credential has been issued to replace the credential in question.

605 {AL2/3/4_CO_NUI#020 a), AL2_CM_RVP#010, AL2_CM_RVP#020, AL2_CM_RVP#040, AL2_CM_RVP#045,
 606 AL2/3/4_CM_RVR#010, AL2/3/4_CM_RVR#020, AL2/3/4_CM_RVR#030, AL2/3/4_CM_RVR#040,
 607 AL2_CM_RVR#050, AL2/3/4_CM_SRR#010}

608 {KI.8.2.5#02: The time frame between notice of an event requiring revocation and the completion of the
 609 revocation process is determined by organizational policy. At higher LoAs, the time period permitted
 610 for revocation is usually shorter. Some credentials, such as those held on smart cards, can be physically
 611 destroyed upon revocation. However, the information associated with the credential cannot always be
 612 destroyed.

613 {AL2/3/4_CO_NUI#020 a), AL2_CM_RVP#030}

614 **8.2.6 Credential renewal and/or replacement**

615 Renewal is the process whereby the life of an existing credential is extended. Replacement is the process
 616 whereby an entity is issued a new credential, or a means to produce a credential, to replace a previously
 617 issued credential that has been revoked. An example of a replacement credential is when a CSP sends a
 618 temporary password to the entity's email address that enables the entity to create a new password after
 619 providing the temporary password. Another example is a PIN unlock code, which should be treated as if
 620 it were a PIN. The rigorousness of the processes for the renewal and replacement of credentials varies
 621 according to the LoA.

622 8.2.7 Record-keeping

623 {KI.8.2.7#01: Appropriate records shall be maintained throughout the lifecycle of a credential. At a
624 minimum, records shall be kept to document the following information:

- 625 a) the fact that a credential has been created
- 626 b) the identifier of the credential (where applicable)
- 627 c) the entity to which the credential has been issued (where applicable)
- 628 d) the status of the credential (where applicable).

629 Records shall be kept for every (applicable) process involved in the credential management phase.

630 {AL*_#CO_NUI#050, AL*_CM_CSM#010, AL2/3/4_CM_RVP#050, AL2/3/4_ID_VRC#030}

631 Where credentials are issued to human entities, the keeping of records is likely to involve the processing
632 of PII. See Appendix I.

633 8.3 Entity authentication phase

634 In the entity authentication phase, the entity uses its credential to attest its identity to an RP. The
635 authentication process is concerned solely with the establishment (or not) of confidence in the claim or
636 assertion of identity, and it has no bearing on, or relationship with, the actions the relying party may
637 choose to take based upon the claim or assertion.

638 8.3.1 Authentication

639 {KI.8.3.1#01: The authentication process includes the use of a protocol to demonstrate possession and/or
640 control of a credential in order to establish confidence in an identity. Authentication protocol
641 requirements vary depending on the applicable LoA. For example, for a lower LoA, authentication may
642 involve use of a password. At higher LoAs, authentication may involve using a cryptographic-based
643 challenge-response protocol. Multifactor authentication is required at higher LoAs. Not all
644 authentication factors provide the same strength, and multiple factors are used to increase assurance. See
645 clause 10.

646 {AL*_CM_CSM#040, AL2_CM_RVP#020, AL2_CM_RVP#030, AL2/3/4_CM_ASS#010, AL2/3/4_CM_ASS#015,
647 AL3/4_CM_ASS#018, AL2/3/4_CM_ASS#020, AL2/3/4_CM_ASS#030, AL2/3/4_CM_ASS#035,
648 AL2/3/4_CM_ASS#040, AL2/3/4_CM_AGC#010, AL4_CM_AGC#020, AL2/3/4_CM_MFA#010, AL*_CM_CRN#035}

649 {NOTE – the criteria found in [KI-SAC] §5.2/3/4.6.4, i.e. the AL2/3/4_CM_VAS series are not mapped because they are
650 more directly related to communication protocols between the CSP and its RPs,
651 rather than the broader aspects of entity authentication }

652 8.3.2 Record-keeping

653 {KI.8.3.2#01: Monitoring and record-keeping of events in the authentication phase may be necessary for
654 a variety of purposes, such as service provision, compliance, accountability and/or legal requirements.

655 {AL*_CM_CSM#010, AL2/3/4_CM_RVP#060}

656 {KI.8.3.2#02: These records shall be managed in a manner that takes into account the need for protection
657 and minimization of PII. See also Appendix I.

658 {AL*_CM_CSM#010, AL2/3/4_CM_RVP#060}

659 9 Management and organizational considerations

660 EAA does not come from technical factors alone, but also from regulations, contractual agreements and
661 consideration of how the service provision is managed and organized. A technically rigorous solution

662 without competent management and operation can fall short of its potential for providing security in the
663 provision of EAA.

664 This clause is informative and describes organizational and management considerations that affect EAA.
665 It does not provide specific criteria for each LoA. Specific criteria and conformance assessment for
666 management and organizational considerations are outside of the scope of this Recommendation, but
667 should be provided within a trust framework.

668 9.1 Service establishment

669 {KI.9.1#01: Service establishment addresses both the legal status of the service provider and the status
670 of the functional service provision. For instance, knowing that the provider of identity management and
671 authentication services is a registered legal entity gives confidence that the CSP is a bona fide enterprise
672 in the jurisdiction within which it operates. This becomes more significant when service components are
673 operated by different legal entities (e.g., registration as a separate function).

{AL*_CO_ESM#010, AL*_CO_ESM#030}

675 {KI.9.1#02: Although the basic requirements are the same for all LoAs, the higher LoAs should have
676 greater dependency on the service provision being complete and reliable. For instance, at LoA3 and
677 above, greater assurance about the service provision should also be taken from knowledge of its
678 corporate ties and understanding of the level of independence it is permitted in its operations.

{AL3/4_CO_ESM#060, AL3/4_CO_ESM#070}

680 9.2 Legal and contractual compliance

681 {KI.9.2#01: All EAAF actors should understand and comply with any legal requirements incumbent on
682 them in connection with the operation and delivery of the service. This has implications including, but
683 not limited to, the types of information that may be sought, how identity proofing is conducted, and
684 what information may be retained. Handling of PII is a particular legal concern (see [Annex A Appendix I](#)
685 (per Erratum 1 (05/2013))). Account should be taken of all jurisdictions within which actors operate.

{AL*_CO_ESM#030, AL*_CO_ESM#050, AL*_CO_ESM#055}

687 {KI.9.2#02: At LoA2 and higher, specific policy and contractual requirements should also be identified.

{AL*_CO_NUI#010, AL*_CO_NUI#020, AL2/3/4_CO_NUI#025, AL*_CO_NUI#030, AL*_CO_NUI#040,
689 AL*_CO_NUI#050, AL2/3/4_CO_NUI#070}

690 9.3 Financial provisions

691 {KI.9.3#01: Where long-term availability of services is a consideration in both an entity's and relying
692 parties' expectations, financial stability should be shown as sufficient to ensure the continued operation
693 of the service and to underwrite the degree of liability exposure being carried. For LoA1 services and
694 reliance, such provisions are unlikely to be a consideration, whereas services supporting more
695 significant transactions at LoA2 and higher should address such needs.

{AL2/3/4_CO_ESM#040}

697 9.4 Information security management and audit

698 {KI.9.4#01: At LoA2 and higher, EAAF actors should have in place documented information security
699 management practices, policies, approaches to risk management and other recognized controls, so as to
700 provide assurance that effective practices are in place.

{AL2/3/4_CO_ISM#010, AL2/3/4_CO_ISM#020, AL2/3/4_CO_ISM#030, AL2/3/4_CO_ISM#040,
702 AL2/3/4_CO_ISM#050, AL2/3/4_CO_ISM#060, AL2/3/4_CO_ISM#070, AL2/3/4_CO_ISM#100,
703 AL2/3/4_CO_OPN#020, AL2/3/4_CO_OPN#030, AL2/3/4_CO_OPN#040, AL2/3/4_CO_OPN#050,

704 AL2/3/4_CO_OPN#060, AL2/3/4_CO_OPN#070}

705 {KI.9.4#02: For LoA3 and above, a formal information security management system (e.g., [b-ISO/IEC
706 27000-series]) should be used.
707 {AL3/4_CO_ISM#120}
708 {NOTE – [X.1254] refers explicitly to IS27000, which is an overview of the IS27001-series; [IS29115] refers to the
709 “IS27000-series”; however, each is incorrectly expressed, since the only *formal* basis for an information security
710 management system is IS27001, to which [KI-SAC] correctly refers.}

711 {KI.9.4#03: Depending on the agreements for legal, contractual, and technical compliance, actors should
712 ensure that parties are abiding by their commitments and may provide an avenue for redress in the event
713 that they are not.
714 {AL2/3/4_CO_ESC#010, AL2/3/4_CO_ESC#020}

715 {KI.9.4#04: At LoA2 and higher, this assurance should be supported by security audits, both internal and
716 external, and the secure retention of records of significant events, including those audits. An audit can
717 be used to check that parties' practices are in line with what has been agreed. Dispute resolution services
718 may be used for disagreements.
719 {AL2/3/4_CO_ISM#080}
720 {NOTE – Kantara does not explicitly require external audits and neither does IS27001. A previous requirement in [KI-SAC]
721 for external review which existed when [X.1254] was being drafted was later removed,
722 since it was considered that a Kantara Assessment served that purpose.}

723 9.5 External service components

724 {KI.9.5#01: When an organization is dependent upon third parties for parts of its service, how it directs
725 the actions of these parties and oversees them will contribute to the overall assurance of the service
726 provision. The nature and extent of the arrangements should be proportional to the required LoA and to
727 the information security management system being applied. At LoA1, such assurance should have
728 minimal effect, but from LoA2 and up, these measures contribute to the overall assurance being given.
729 {AL2/3/4_CO_ESC#010, AL2/3/4_CO_ESC#020}

730 9.6 Operational infrastructure

731 {KI.9.5#01: To enable large-scale networks of trust, a trust framework may be used. In a trust
732 framework, the actors support the information flow between one another. Depending on the agreements,
733 additional actors may be called on to ensure that all actors are abiding by commitments and may provide
734 an avenue for redress in the event that they are not.
735 {These criteria could again be called-up: AL2/3/4_CO_ESC#010, AL2/3/4_CO_ESC#020.
736 Additionally, a community which requires Kantara Approval by its members would place some assurance that
737 ‘actors are abiding by commitments’, through Kantara’s Approvals and its oversight (e.g. US-FICAM).
738 Such measures fall outside of the scope of [KI-SAC].}

739 9.7 Measuring operational capabilities

740 Policy makers set out the technical and contractual requirements for trust frameworks. Technical
741 requirements might include, for example, product version levels, system configuration, settings and
742 protocols, while contractual requirements might be geared towards fair information practices. As they
743 establish these requirements, policy makers should include criteria by which potential trust framework
744 entities can be measured. Rather than developing the criteria themselves, policy makers may wish to
745 draw on standard criteria that experts have already elaborated, such as this Recommendation. The more
746 policy makers use standard criteria across different trust frameworks, the easier it will be for entities to

747 understand and apply the criteria consistently. Moreover, named sets of criteria can serve as shorthand
748 to indicate different degrees or types of rigour in requirements or capabilities at various LoAs.

749 {NOTE – this can be equated to the Kantara profiling paradigm, which falls outside the scope of [KI-SAC].}

750 10 Threats and controls

751 This clause describes threats to each phase of the EAAF and provides required controls for each LoA.

752 10.1 Threats to, and controls for, the enrolment phase

753 10.1.1 Enrolment phase threats

754 Table 10-1 identifies and describes threats to the enrolment phase.

755 **Table 10-1 – Threats to the enrolment phase**

Threat	Examples
Impersonation	Some examples of impersonation are when an entity illegitimately uses another entity's identity information « <i>source text excised</i> ».
Impersonation (From [IS29115].)	Some examples of impersonation are when an entity illegitimately claims another entity's identity by using a forged driver's license describing an individual who doesn't exist « <i>source text excised</i> ».

756 10.1.2 Required LoA controls to protect against enrolment phase threats

757 Table 10-2 identifies the required controls for the enrolment phase according to LoA.

758 **Table 10-2 – Enrolment phase controls for each LoA**

Threats	Controls	Required controls			
		LoA1	LoA2	LoA3	LoA4
Impersonation	IdentityProofing: PolicyAdherence	#1	#1	#1	#1
	IdentityProofing: In Person				#2
	IdentityProofing: AuthoritativeInformation	#3	#4	#5	#6

759 NOTE – In the above table, the identifiers #1 – #6 correspond to the specific controls required to provide
760 protection at each LoA. Each of these controls is described in detail in clause 10.1.2.1. Boxes in the table with a
761 diagonal line indicate that the respective control is not applicable at the indicated LoA.

762 10.1.2.1 Controls against enrolment phase threats

763 The following controls against enrolment phase threats correspond to #1 – #6 listed in Table 10-2.

764 IdentityProofing: PolicyAdherence

765 {KI.10.1.2.1#01: #1. Publish the identity proofing policy, and perform all identity proofing in accordance
766 with the published identity proofing policy.

767 {AL2/3/4_ID_POL#030, AL2/3/4_ID_POL#040

768 NOTE – [KI-SAC] does NOT require such publication at AL1;

769 AL4_CM_CPP#020}

770 {KI.10.1.2.1#02: #2. In-person identity proofing shall be used for humans.

771 {AL4_ID_IDV#000}

772 IdentityProofing: AuthoritativeInformation

773 {KI.10.1.2.1#03: #3. Identity information may be self-claimed or self-asserted.

774 {AL1_ID_IPV#010, AL1_ID_RPV#010}

775 #4. The following controls apply:

- 776 • all controls from #3.
- 777 {NOTE – this is manifestly wrong, since self-assertions are permitted only at AL1, originating from OMB M-04-04
- 778 and being mimicked in CD29003, at the time of this mapping.
- 779 Observance of #2 is not an effective preclusion of this.}

780 In addition:

- 781 • The entity shall provide identity information from at least one policy-compliant authoritative
- 782 source of identity information.

783 a) For humans

784 i) In person:

- 785 • {KI.10.1.2.1#03: Ensure that the entity is in possession of an identification
- 786 document from at least one policy-compliant authoritative source that bears a
- 787 photographic image of the holder that matches the appearance of the entity; and
- 788 {AL2_ID_IPV#010}

- 789 • {KI.10.1.2.1#04: ensure that the presented identification document appears to be a
- 790 genuine document, properly issued and valid at the time of application.

791 {AL2_ID_IPV#020, AL2_ID_SCV#010}

792 ii) Not in person:

- 793 • {KI.10.1.2.1#05: The entity shall provide evidence that he/she is in possession of
- 794 policy-compliant, personal identity information. (Examples of acceptable identity
- 795 information might include a driver's licence or a passport); and
- 796 {AL2_ID_RPV#010, AL2_ID_CRV#010, AL2_ID_AFV#010, AL2_ID_IDC#010}

- 797 • {KI.10.1.2.1#06: the existence and validity of the evidence provided shall be
- 798 confirmed in accordance with policy requirements.

799 {AL2_ID_RPV#020, AL2_ID_CRV#020, AL2_ID_AFV#020, AL2_ID_IDC#010, AL2_ID_SCV#010}

800 «source text excised»

801 #5. The following controls apply:

- 802 • {KI.10.1.2.1#07: all controls from #4.

803 {NOTE – This erroneously permits self-assertion at AL3, by inheritance from #3.

804 Observance of #2 is not an effective preclusion of this. See previous comment.

805 Therefore, the following requirements for evidence, as set out in §10.1.2.1 #4 a) i) and ii) (above),

806 apply here wrt AL3 tags.}

807 {AL3_ID_IPV#010, AL3_ID_RPV#010, AL3_ID_CRV#010, AL3_ID_AFV#010, AL3_ID_IDC#010, AL2_ID_SCV#010}

808 In addition:

809 {NOTE – although this states ‘in addition’, inclusion below of AL3 tags accomplishes both the requirements of #4 controls

810 AND these additional requirements (because of the way [KI-SAC] re-states all applicable requirements).}

811 a) For humans

- 812 i) {KI.10.1.2.1#08: In person:
- 813 • Verify the accuracy of contact information listed in the identification document by
- 814 using it to contact the entity.
- 815 • Verify at least one identification document (e.g., document attesting to birth,
- 816 marriage or immigration) against registers of the relevant authoritative source.
- 817 • Corroborate personal information against applicable authoritative information
- 818 sources and (where possible) sources from other contexts, which are sufficient to
- 819 ensure a unique identity; and
- 820 • verify information previously provided by, or likely to be known only by, the
- 821 entity.

822 {AL3_ID_IPV#020, AL3_ID_SCV#010}

- 823 ii) {KI.10.1.2.1#09: Not in person:
- 824 • Ensure check by a trusted third party of the entity's assertion/claim to the current
- 825 possession of an LoA3 (or higher) credential from an authoritative source; and/or
- 826 • verify information previously provided by, or likely to be known only by, the
- 827 entity.
- 828 {AL3_ID_RPV#020, AL3_ID_CRV#020, AL3_ID_AFV#020, AL3_ID_IDC#010, AL3_ID_SCV#010}

829 «source text excised»

830 #6. The following controls apply:

- 831 • {KI.10.1.2.1#10: all controls from #5.
- 832 {NOTE – This erroneously permits self-assertion at AL4, by inheritance from #3, through #4.
- 833 Observance of #2 is not an effective preclusion of this. See previous comment.
- 834 In addition, this erroneously allows remote proofing at AL4, which should never be permitted.
- 835 Therefore, the following requirements for evidence, as set out in §10.1.2.1 #4 a) i) and ii) (above),
- 836 apply here wrt AL4 tags, except that **only those addressing in-person proofing are cited**, in keeping with accepted
- 837 principles.}
- 838 {AL4_ID_IPV#010, AL4_ID_SCV#010}

839 In addition:

840 {NOTE – although this states ‘in addition’, inclusion below of **in-person** AL4 tags accomplishes both the requirements of #5

841 controls AND these additional requirements (because of the way [KI-SAC] re-states all applicable requirements).}

- 842 a) {KI.10.1.2.1#11: For humans
- 843 – The entity shall provide identity information from at least one additional policy-
- 844 compliant authoritative source.
- 845 {AL4_ID_IPV#030, AL4_ID_IPV#040, AL4_ID_IPV#050, AL4_ID_SCV#010}

846 «source text excised»

847

848

849 **10.2 Threats to, and controls for, the credential management phase**850 **10.2.1 Credential management threats**

851 Table 10-3 lists threats to the credential management phase.

Table 10-3 – Credential management threats

Threat	Examples
CredentialCreation: Tampering	An attacker alters information as it passes from the enrolment process to the credential creation process.
CredentialCreation: UnauthorizedCreation	An attacker causes a CSP to create a credential based on a fictitious entity.
CredentialIssuance: Disclosure	A credential created by the CSP for an entity is copied by an attacker as it is transported from the CSP to the entity during credential establishment.
CredentialActivation: Unauthorized Possession	An attacker obtains a credential that does not belong to him/her, and, by masquerading as the rightful entity, causes the CSP to activate the credential.
CredentialActivation: Unavailability	<ol style="list-style-type: none"> 1. The entity associated with a credential, or the means to generate the credential, is not in the usual location and is unable to adequately authenticate its identity to the CSP. 2. Delivery of a credential, or the means to generate the credential, is delayed, and activation within the prescribed period is not possible.
CredentialStorage: Disclosure	Credentials stored in a system file are revealed. For example, a stored record of usernames and passwords is accessed by an attacker.
CredentialStorage: Tampering	The file that maps usernames to credentials is compromised so that the mappings are modified, and existing credentials are replaced by credentials to which the attacker has access.
CredentialStorage: Duplication	An attacker uses stored information to create a duplicate credential (e.g., by duplicating a smart card that can generate the credential) that can be used by an unauthorized entity.
CredentialStorage: DisclosureByEntity	The entity keeps a written record of the username and password in a place that can be accessed by others.
CredentialRevocation: DelayedRevocation	The dissemination of revocation information is not timely leading to a threat of entities with revoked credentials still being able to authenticate before the credential verifier updates the latest revocation information.
CredentialRevocation: UseAfterDecommissioning	<p>User accounts are not deleted when employees leave a company leading to possible misuse of the old accounts by unauthorized persons.</p> <ul style="list-style-type: none"> – A credential stored in a hardware device is used after its cryptographic keys have been revoked.
CredentialRenewal: Disclosure	Credential renewed by the CSP for an entity is copied by an attacker as it is transported.
CredentialRenewal: Tampering	A new credential created by an entity is modified by an attacker as it is being submitted to the CSP to replace an expired credential.

Table 10-3 – Credential management threats

Threat	Examples
CredentialRenewal: UnauthorizedRenewal	An attacker is able to take advantage of a weak credential renewal protocol to extend the credential validity period for a current entity. An attacker fools the CSP into issuing a new credential for a current entity, and the new credential binds the current entity's identity to a credential provided by the attacker. <i>«source text excised»</i>
CredentialRecordkeeping: Repudiation	An entity asserts or claims that a legitimate credential is fraudulent or contains incorrect information in order to falsely deny having used the credential.

852

853 **10.2.2 Required LoA controls to protect against credential management phase threats**

854 Table 10-4 identifies the required controls against credential management threats according to the LoA.

Table 10-4 – Credential management controls for each LoA

Threats	Controls	Required controls			
		LoA1	LoA2	LoA3	LoA4
CredentialCreation: Tampering	AppropriateCredentialCreation	#1	#1	#2	#2
	HardwareOnly	/	/	/	#3
	StateLocked	/	/	/	#4

Table 10-4 – Credential management controls for each LoA

Threats	Controls	Required controls			
		LoA1	LoA2	LoA3	LoA4
CredentialCreation: UnauthorizedCreation	TrackedInventory	#5	#5	#5	#5
CredentialIssuance: Disclosure	AppropriateCredentialIssuance	#6	#7	#7	#8
CredentialActivation: UnauthorizedPossession CredentialActivation: Unavailability	ActivatedByEntity	#9	#9	#10	#11
CredentialStorage: Disclosure CredentialStorage: Tampering CredentialStorage: Duplication CredentialStorage: DisclosureByEntity	CredentialSecureStorage	#12	#13	#14	#15
CredentialRevocation: DelayedRevocation CredentialRevocation: UseAfterDecommissioning	CredentialSecureRevocation &Destruction	#16	#16	#16	#16
CredentialRenewal: Disclosure CredentialRenewal: Tampering CredentialRenewal: UnauthorizedRenewal	CredentialSecureRenewal	#17	#17	#18	#19
CredentialRecordkeeping: Repudiation	RecordRetention	#20	#20	#21	#21

855 NOTE – In the above table, the identifiers #1-#21 correspond to the specific controls required to provide
856 protection at each LoA. Each of these controls is described in detail in clause 10.2.2.1. Boxes in the table with a
857 diagonal line indicate that the respective control is not applicable at the indicated LoA.

858 10.2.2.1 Controls against credential management phase threats

859 The following controls against credential management phase threats correspond to the numbers #1-#21
860 listed in Table 10-4.

861 AppropriateCredentialCreation

862 #1. The following controls apply:

- 863 • {KI.10.2.2.1#01: Formalized and documented processes shall be used for credential creation.
864 {AL1/2_CO_NUI#010, AL1/2_CO_NUI#020, AL2_CO_NUI#025, AL2_CO_ISM#010, AL1/2_CM_CRN#010}}

865 {KI.10.2.2.1#02: Prior to finalizing the binding of a credential to an entity, the CSP must have adequate
866 assurance that the credential is bound and remains bound to the correct entity.

867 {NOTE – [KI-SAC] does not directly address binding at issue at AL1 & 2. At ALs 3 & 4 CM_CRN#080 addresses this for
868 PKI credentials. The following requirement ensures binding only at any change of user info.}
869 {AL2/3/4_CM_IDP#010}

870 #2. The following controls apply:

- 871 • {KI.10.2.2.1#03: all controls from #1.

872 {AL3/4_CO_NUI#010, AL3/4_CO_NUI#020, AL3/4_CO_NUI#025, AL3/4_CO_ISM#010,
873 AL3/4_CM_CRN#010, AL3/4_CM_CRN#080, AL3/4_CM_IDP#010}

874 In addition:

875 • Credential binding shall provide protection against tampering by either using:

876 a) {KI.10.2.2.1#04: digital signatures; or

877 {AL3/4_CM_CRN#080}

878 b) {KI.10.2.2.1#05: at LoA4, the mechanisms described in StateLocked for credentials held on a
879 hardware device.

880 {NOTE – This is poorly stated, since #2 applies at ALs 3 & 4 (see Table 10-4), yet #4 is AL4 only.
881 Therefore, this clause should be interpreted with the amendment inserted by this Editor.}

882 HardwareOnly

883 {KI.10.2.2.1#06: #3. Credentials shall be contained on a hardware security module.⁶

884 {AL4_CM_CRN#060}

885 StateLocked

886 {KI.10.2.2.1#07: #4. Credentials held on a hardware device shall be put in a locked state at the end of the
887 creation process.

888 {NOTE – [KI-SAC] has no such explicit requirement.}

889 TrackedInventory

890 {KI.10.2.2.1#08: #5. If a credential, or the means to produce credentials, is held on a hardware device, the
891 hardware device shall be kept physically secure and the inventory tracked. For example, non-
892 personalized smart cards should be stored in a secure place and their serial numbers recorded to protect
893 against theft and subsequent attempts to create unauthorised credentials.

894 {NOTE – [KI-SAC] has no such explicit requirement.
895

896 AppropriateCredentialIssuance

897 {KI.10.2.2.1#09: #6. Formalized and documented processes shall be used for credential issuance.

898 {NOTE – there is no such requirement in [KI-SAC] at AL1.
899 This would not stop a CSP conforming to this [X.1254] requirement,
900 if they chose to document and operate against such processes.}

901 #7. The following controls apply:

902 • {KI.10.2.2.1#10: all controls from #6.

903 {AL2/3_CM_CPP#010, AL2/3_CM_CPP#030}

904 In addition:

905 • {KI.10.2.2.1#11: The issuance process shall include a mechanism to ensure that a credential is
906 provided to the correct entity or an authorized representative. If the credential is not delivered in
907 person, a mechanism shall be used to check that the delivery address exists and is legitimately
908 associated with the entity.

909 {AL2/3_CM_CRD#015, AL2/3_CM_CRD#016, AL3_CM_CRN#020}

⁶ The boundary of a hardware security module is defined in ISO/IEC 19790:2012.

910 #8. The following controls apply:

- 911 • {KI.10.2.2.1#12: all controls from #7, subject to the limitation that only delivery in-person shall
- 912 be permitted.

913 {NOTE – ‘all controls’ would anticipate remote (i.e. non in-person) delivery, which is not permitted at AL4, to which this

914 control relates. The following mapping observes that limitation}

915 {AL4_CM_CPP#020, AL4_CM_CPP#030, AL4_CM_CRD#015}

916 In addition:

- 917 • {KI.10.2.2.1#13: If a credential is not delivered in person, then it shall be delivered using a secure
- 918 channel and the entity or an authorized representative of the entity shall sign a receipt
- 919 acknowledging receipt of the credential.

920 {AL4_CM_CRN#020}

921 ActivatedByEntity

922 {KI.10.2.2.1#14: #9. A procedure shall exist to ensure that a credential, or the means to generate a

923 credential, is activated only if it is under the control of the intended entity. There are no specific

924 requirements for this procedure.

925 {NOTE – there is no such requirement in [KA-SAC] at AL1. Further, it is assumed that ‘activation’ relates to enabling use

926 of the credential once it is delivered to the subject, NOT its use for the purposes of an authentication of the subject.}

927 {AL2_CM_CRD#010, AL2_CM_CRD#015, AL2_CM_CRD#016}

928 {KI.10.2.2.1#15: #10. A procedure shall exist to ensure that a credential, or the means to generate a

929 credential, is activated only if it is under the control of the intended entity. This procedure shall prove

930 that the entity is bound to the activation of a credential (e.g., challenge-response protocol).

931 {AL3_CM_CRD#010, AL3_CM_CRD#015, AL3_CM_CRD#016, AL3_CM_CRD#020}

932 #11. A procedure shall exist to ensure that a credential, or the means to generate a credential, is

933 activated only if it is under the control of the intended entity. This procedure shall:

- 934 a) {KI.10.2.2.1#16: prove that the entity is bound to the activation of a credential (e.g., challenge-
- 935 response protocol), and

936 {AL4_CM_CRD#010, AL4_CM_CRD#015, AL4_CM_CRD#020}

- 937 b) {KI.10.2.2.1#17: allow activation only within a period of time determined by policy.

938 {NOTE – [KI-SAC] has no such provision.}

939 CredentialSecureStorage

940 #12. The following controls apply:

- 941 • {KI.10.2.2.1#18: Credentials based on shared secrets shall be protected by access controls that
- 942 limit access to only those administrators and applications that require access; and

943 {AL1_CO_SCO#020}

- 944 • {KI.10.2.2.1#19: Protection policy for stored credentials shall be described in the documentation
- 945 associated with the use of those credentials that is made available to entities.

946 {NOTE – the provisions of CO_CPP#010/015 do not exist in [KI-SAC] at AL1.}

947 #13. The following controls apply:

- 948 • {KI.10.2.2.1#20: all controls from #12.

949 {AL2_CO_SCO#020, AL2_CM_CPP#010}

950 In addition:

- 951 • {KI.10.2.2.1#21: Such shared secret files shall not contain the plaintext passwords or secrets; an
 952 alternative method may be used to protect the shared secret.
 953 {AL2_CO_SCO#020, AL2_CO_SCO#030}
- 954 #14. The following controls apply:
- 955 • {KI.10.2.2.1#22: all controls from #13.
 956 {AL3_CO_SCO#020, AL3_CO_SCO#030, AL3_CM_CPP#010}
- 957 In addition:
- 958 • {KI.10.2.2.1#23: Shared secrets shall be protected by access controls that limit access to only
 959 those administrators and applications that require access. Such shared secrets shall be encrypted.
 960 The encryption key for the shared secret shall itself be encrypted and stored in a cryptographic
 961 module (hardware or software). The encryption key for the shared secret shall be decrypted only
 962 as immediately required for an authentication operation; and
 963 {AL3_CO_SCO#020}
- 964 • {KI.10.2.2.1#24: Entities or authorized representatives of entities shall be required to
 965 acknowledge that they understand these requirements and agree to protect credentials in
 966 accordance with these requirements.
 967 {NOTE – [KI-SAC] has no such requirement}
- 968 #15. The following controls apply:
- 969 • {KI.10.2.2.1#25: all controls from #14.
 970 {AL4_CO_SCO#020, AL4_CO_SCO#030, AL4_CM_CPP#010, AL4_CO_OPN#020}
- 971 In addition:
- 972 • {KI.10.2.2.1#26: Entities or authorized representatives of entities shall be required to sign a
 973 document acknowledging that they understand the requirements for the storage of credentials
 974 and agree to protect credentials accordingly.
 975 {NOTE – [KI-SAC] has no such requirement}
- 976 CredentialSecureRevocation&Destruction
- 977 #16. {KI.10.2.2.1#27: CSPs shall revoke or destroy (if possible) credentials (including those based on
 978 shared secrets) within a specific time period for each LoA as defined by organizational policy.
 979 {AL2/3_CM_CPP#010, AL2/3/4_CM_RVP#010 e), AL2/3/4_CM_RVP#030}
 980 {NOTE – [KI-SAC] has no such requirement at AL1.}
- 981 CredentialSecureRenewal
- 982 #17. The following controls apply:
- 983 • {KI.10.2.2.1#28: The CSP shall establish suitable policies for the renewal and replacement of
 984 credentials.
 985 {AL2_CM_CPP#010}
 986 {NOTE – [KI-SAC] has no such requirement at AL1.}
- 987 • {KI.10.2.2.1#29: Proof-of-possession of the unexpired current credential shall be demonstrated by
 988 the entity prior to the CSP allowing renewal and/or replacement.
 989 {AL1/2_CM_RNR#020}
- 990 • {KI.10.2.2.1#30: Passwords shall meet minimum CSP policy requirements for password strength
 991 and re-use.

SAC mapping – ISO/IEC 29115 / ITU-T X.1254 – Entity authentication assurance framework

- 992 {AL2_CM_CPP#010}
- 993 {NOTE – [KI-SAC] has no such requirement at AL1.}
- 994 {NOTE – this is not mapped to [KI-SAC] controls which require specific password characteristics / entropy, since none are
- 995 stated here – it requires only that policy is met, and defining one and having a C(r)SP accomplishes that.}
- 996 • {KI.10.2.2.1#31: After expiry of the current credential, renewal shall not be permitted.
- 997 {AL2_CM_RNR#030 b)}
- 998 • {KI.10.2.2.1#32: All interactions shall occur over a protected channel such as SSL/TLS (shaded
- 999 text from [IS29115]).
- 1000 {AL2_CM_RNR#030 d)}
- 1001 #18. The following controls apply:
- 1002 • {KI.10.2.2.1#33: all controls from #17.
- 1003 {AL3_CM_CPP#010, AL3_CM_RNR#020, AL3_CM_RNR#030 b, d)}
- 1004 In addition:
- 1005 • {KI.10.2.2.1#34: They will perform an LoA2 identity proofing in accordance with clause 10.1.2.1
- 1006 (IdentityProofing: PolicyAdherence, IdentityProofing: AuthoritativeInformation).
- 1007 {NOTE – [KI-SAC] has no such requirement and the rationale for this seems flawed: Controls from #17 (applied at AL3)
- 1008 require that the subject be authenticated. Since this would be based on initial IdPV at AL3,
- 1009 why repeat now but at a lower level of assurance??}
- 1010 #19. The following controls apply:
- 1011 • {KI.10.2.2.1#35: all controls from #17.
- 1012 {AL4_CM_CPP#020, AL4_CM_RNR#020, AL4_CM_RNR#030 b, d)}
- 1013 In addition:
- 1014 • {KI.10.2.2.1#36: The will perform an LoA3 identity proofing in accordance with clause 10.1.2.1
- 1015 (IdentityProofing: PolicyAdherence, IdentityProofing: AuthoritativeInformation).
- 1016 {NOTE – [KI-SAC] has no such requirement and the rationale for this seems flawed: Controls from #17 (applied at AL4)
- 1017 require that the subject be authenticated. Since this would be based on initial IdPV at AL4,
- 1018 why repeat now but at a lower level of assurance??}
- 1019 RecordRetention
- 1020 #20. {KI.10.2.2.1#37: A record of the registration, history and status of each credential (including
- 1021 revocation) shall be maintained by the CSP. The duration of retention shall be specified in the CSP
- 1022 policy.
- 1023 {AL2_CM_CPP#010, AL2_CM_RNR#050}
- 1024 {NOTE – [KI-SAC] has no such requirements at AL1.}
- 1025 #21. The following controls apply:
- 1026 • {KI.10.2.2.1#38: all controls from #20; and
- 1027 {AL3_CM_CPP#010, AL4_CM_CPP#020, AL3/4_CM_RNR#050}
- 1028 • {KI.10.2.2.1#39: formalized and documented procedures shall be developed for the chain of
- 1029 custody for each record.
- 1030 {AL3/4_CO_ISM#010, AL3/4_CO_ISM#120}

1031 **10.3 Threats to, and controls for, the authentication phase**1032 **10.3.1 Authentication phase threats**

1033 Threats to the authentication phase include both threats associated with the use of credentials during
 1034 authentication and general threats to authentication. General threats to authentication include, but are not
 1035 limited to: malicious software (e.g., viruses, Trojans, keystroke loggers), social engineering (e.g.,
 1036 shoulder surfing, theft of hardware devices and pins); user errors (e.g., weak passwords, failure to
 1037 protect authentication information), false repudiation, unauthorized interception and/or modification of
 1038 authentication data during transmission, denial of service, and procedural weaknesses. With the
 1039 exception of the use of multifactor authentication, controls for general threats to authentication are
 1040 beyond the scope of this Recommendation. This clause focuses on the threats associated with the use of
 1041 credentials for authentication, describes those threats and lists controls for each type of threat.

1042 Except for the requirement to use multifactor authentication for LoAs 3 and 4, it is not appropriate to
 1043 delineate specific controls in terms of LoA for the authentication phase. Some controls may not be
 1044 appropriate for all contexts. For example, controls for the authentication of users accessing online
 1045 magazine subscriptions are probably different from controls for medical doctors accessing patient
 1046 records. Therefore, it is recommended that, as the risk and consequence of exploitation grows more
 1047 severe, the CSP should consider security in depth (i.e., layering controls appropriate to the operational
 1048 environment, the application, and the LoA). It is up to the system designer, based on risk analysis, to
 1049 make the decisions as to how, when, and in what combination to use these controls.

1050 There are many threats to credentials used for authentication. Table 10-5 lists some broad categories of
 1051 threats to the use of credentials and provides specific examples to illustrate the threats.

Table 10-5 – Summary of threats to the use of credentials in the authentication phase

Threat	Examples
General threats	General threats to authentication include many categories of threat common to any type of ICT. Some examples include keystroke loggers, social engineering, and user errors. Except for the use of multifactor authentication, controls against these threats are beyond the scope of this Recommendation. Note that multifactor authentication does not protect against all possible general threats.
OnlineGuessing	An attacker performs repeated logon attempts by guessing possible values of the credential.
OfflineGuessing	Secrets associated with credential generation are exposed using analytical methods outside the authentication transaction. Password cracking often relies upon brute force methods, such as the use of dictionary attacks. With dictionary attacks, an attacker uses a program to iterate through all of the words in a dictionary (or multiple dictionaries in different languages), computes the hash value for each word, and checks the resultant hash value against the database. The use of rainbow tables is another password cracking method. Rainbow tables are pre-computed tables of clear text/hash value pairs. Rainbow tables are quicker than brute-force attacks because they use reduction functions to decrease the search space. Once generated or obtained, rainbow tables can be used repeatedly by an attacker.

Table 10-5 – Summary of threats to the use of credentials in the authentication phase

Threat	Examples
CredentialDuplication	The entity's credential, or the means to generate credentials, has been illegitimately copied. An example would be the unauthorized copying of a private key.
Phishing	An entity is lured to interact with a counterfeit verifier, and tricked into revealing his or her password or sensitive personal data that can be used to masquerade as the entity. An example is when an entity is sent an email that redirects him or her to a fraudulent website and asks the user to log in using his or her username and password.
Eavesdropping	An attacker listens passively to the authentication transaction to capture information which can be used in a subsequent active attack to masquerade as the entity.
ReplayAttack	An attacker is able to replay previously captured messages (between a legitimate entity and an RP) to authenticate as that entity to the RP.
SessionHijack	An attacker is able to insert himself or herself between an entity and a verifier subsequent to a successful authentication exchange between the latter two parties. The attacker is able to pose as an entity to the relying party or vice versa to control session data exchange. An example is when an attacker is able to take over an already authenticated session by eavesdropping on or predicting the value of authentication cookies used to mark HTTP requests sent by the entity.
ManInTheMiddle	The attacker positions himself or herself between the entity and relying party so that he or she can intercept and alter the content of the authentication protocol messages. The attacker typically impersonates the relying party to the entity and simultaneously impersonates the entity to the verifier. Conducting an active exchange with both parties simultaneously may allow the attacker to use authentication messages sent by one legitimate party to successfully authenticate to the other.
CredentialTheft	A device that generates or contains credentials is stolen by an attacker.
SpoofingAndMasquerading	Spoofing and masquerading refer to situations in which an attacker impersonates another entity in order to allow the attacker to perform an action he would otherwise not be able to perform (e.g., gain access to an otherwise inaccessible asset). This may be done by making use of the credential(s) of an entity or otherwise posing as an entity (e.g., by forging a credential). Some examples are when an attacker impersonating an entity spoofs one or more biometric characteristics by creating a "gummy" finger that matches the pattern of the entity; an attacker spoofs a MAC address by having its device broadcast a MAC address that belongs to another device that has permissions on a particular network; or an attacker poses as a legitimate software publisher responsible for downloading on-line software applications and/or updates.

1052 **10.3.2 Required LoA controls to protect against threats to the use of credentials**

1053 Table 10-6 identifies the required controls to counter credential use threats according to LoA.

Table 10-6 – Summary of controls for threats to the use of credentials according to LoA

Threats	Controls	Required controls				
		LoA*	LoA1	LoA2	LoA3	LoA4
General**	MultiFactorAuthentication	/	/	/	#1	#1
OnlineGuessing	StrongPassword CredentialLockOut DefaultAccountUse AuditAndAnalyze	#2 #3 #4 #5	/	/	/	/
OfflineGuessing	HashedPasswordWithSalt	#6	/	/	/	/
CredentialDuplication	AntiCounterfeiting	#7	/	/	/	/
Phishing	DetectPhishingFromMessages AdoptAntiPhishingPractice MutualAuthentication	#8 #9 #10	/	/	/	/
Eavesdropping	NoTransmitPassword EncryptedAuthentication DifferentAuthenticationParameter	#11 #12 #13	/	/	/	/
ReplayAttack	DifferentAuthenticationParameter Timestamp PhysicalSecurity	#13 #14 #15	/	/	/	/
SessionHijacking	EncryptedSession FixProtocolVulnerabilities CryptographicMutualHandshake	#16 #17 #18	/	/	/	/
ManInTheMiddle	MutualAuthentication EncryptedSession	#10 #16	/	/	/	/
CredentialTheft	CredentialActivation	#19	/	/	/	/
SpoofingAndMasquerading	CodeDigitalSignature LivenessDetection	#20 #21	/	/	/	/
LoA* – These controls should be applied as determined necessary by a risk assessment.						
General** – Not all of the general threats can be resisted by multifactor authentication.						

1054 NOTE – In the above table, the identifiers #1-#21 correspond to the specific controls required to provide
1055 protection at each LoA. Each of these controls is described in detail in clause 10.3.2.1.

1056 10.3.2.1 Controls against threats to the use of credentials in the authentication phase

1057 The following controls against threats to the use of a credential during the authentication phase
1058 correspond to the numbers #1-#21 listed in Table 10-6.

1059 MultiFactorAuthentication

1060 {KI.10.3.2.1#01: #1. Two or more credentials implementing different authentication factors shall be used
1061 (e.g., something you have combined with something you know).

1062 {AL3/4_CM_MFA#010, AL3/4_CM_ASS#010}

- 1063 StrongPassword
- 1064 {KI.10.3.2.1#02: #2. Use of strong passwords (e.g., complex, non-dictionary strings that contain mixtures
1065 of upper case, lower case, numeric and special characters) shall be enforced.
1066 {AL1_CM_CTR#020 a), AL1_CM_CRN#040 a) b) i), AL1_CM_ASS#010 g) ii), AL1_CM_VAS#060}
- 1067 CredentialLockout
- 1068 {KI.10.3.2.1#03: #3. A lockout or slowdown mechanism shall be used after a certain number of failed
1069 password attempts.
1070 {AL1_CM_AS#035}
- 1071 DefaultAccountUse
- 1072 {KI.10.3.2.1#04: #4. Default account names and password (e.g., manufacturer's settings) shall not be used.
1073 {AL*_CM_CRN#030, AL1/2_CM_CRN#040 a), AL3/4_CM_CRN#040}
1074 {NOTE – CRN#040 is not applicable at AL4, since PINS/password are disallowed.}
- 1075 AuditAndAnalyze
- 1076 {KI.10.3.2.1#05: #5. An audit trail of failed logins shall be used to analyse for patterns of online password
1077 guessing attempts.
1078 {AL2/3/4_CO_SER#010}
1079 {NOTE – [KI-SAC] has no such requirements at AL1.}
- 1080 HashedPasswordWithSalt
- 1081 {KI.10.3.2.1#06: #6. Hashed passwords with salt shall be used to deter brute force and rainbow table
1082 attacks.
1083 {AL2/3_CO_SCO#030}
1084 {NOTE – [KI-SAC] has no such requirements at AL1.}
1085 {NOTE – Such a control is not relevant at AL4, since crypto mechanisms over-rule.}
- 1086 Anticounterfeiting
- 1087 {KI.10.3.2.1#07: #7. Anti-counterfeiting measures (e.g., holograms, microprint) shall be used on devices
1088 holding credentials.
1089 {NOTE – [KI-SAC] has no such explicit requirement – even references to FIPS 140-2 / IS19790 are insufficient,
1090 since these docs have no such explicit statements.}
- 1091 DetectPhishingFromMessages
- 1092 {KI.10.3.2.1#08: #8. Controls shall be implemented that are specifically designed to detect phishing
1093 attacks (e.g., Bayesian filters, IP blacklists, URL-based filters, heuristics and fingerprinting schemes).
1094 {AL2/3/4_CO_ISM#030, AL2/3/4_CM_CTR#030}
1095 {NOTE – [KI-SAC] has no such requirements at AL1.}
1096 {NOTE – this is broad and specific controls should derive from it
1097 – this could be accommodated through preparation of a profile }
- 1098 AdoptAntiPhishingPractice
- 1099 {KI.10.3.2.1#09: #9. (correcting [X.1254]) Practices such as disabling images, disabling hyperlinks from
1100 untrusted sources and providing visual cues in email clients shall be used to protect entities against
1101 phishing attacks.
1102 {AL2/3/4_CO_ISM#030, AL2/3/4_CM_CTR#030}
1103 {NOTE – [KI-SAC] has no such requirements at AL1.}
1104 {NOTE – this is broad and specific controls should derive from it

1105 – this could be accommodated through preparation of a profile}

1106 MutualAuthentication

1107 {KI.10.3.2.1#10: #10. (correcting [X.1254]) Mutual authentication shall be used.
 1108 {AL2/3/4_CO_SCO#010, AL2/3/4_CM_ASS#010, AL*_CM_VAS#060}
 1109 {NOTE – [KI-SAC] has no CO_SCO#010 requirements at AL1 ([29115] intends that this applies to all).}

1110 NoTransmitPassword

1111 {KI.10.3.2.1#11: #11. Authentication mechanisms that do not transmit passwords over the network shall
 1112 be used (e.g., Kerberos protocol).
 1113 {AL*_CO_SCO#020}
 1114 {NOTE – this is not precisely the same control requirement, but its effect is equivalent,
 1115 to the extent that encryption can protect.}

1116 EncryptedAuthentication

1117 {KI.10.3.2.1#12: #12. If authentication exchange over a network is necessary, the data shall be encrypted
 1118 prior to transit.
 1119 {AL2/3/4_CM_ASS#010, AL*_CM_VAS#060}

1120 DifferentAuthenticationParameter

1121 {KI.10.3.2.1#13: #13. A different authentication parameter shall be used for each authentication
 1122 transaction (e.g., one-time password, session credential).
 1123 {AL2_CM_CTR#028, AL*_CM_VAS#080, AL*_CM_VAS#090}

1124 Timestamp

1125 {KI.10.3.2.1#14: #14. Each message shall be time-stamped with a non-forgeable time stamp.
 1126 {AL2/3/4_CO_SCO#010 b)}

1127 PhysicalSecurity

1128 {KI.10.3.2.1#15: #15. Physical security mechanisms shall be used (i.e., tamper evidence, detection and
 1129 response).
 1130 {NOTE – [KI-SAC] has no such explicit requirement – even references to FIPS 140-2 / IS19790 are insufficient,
 1131 since these docs have no such explicit statements.}

1132 EncryptedSession

1133 {KI.10.3.2.1#16: #16. Encrypted sessions shall be used.
 1134 {AL2/3/4_CO_SCO#010}

1135 FixProtocolVulnerabilities

1136 {KI.10.3.2.1#17: #17. Platform patches to fix protocol vulnerabilities (e.g., TCP/IP) shall be used.
 1137 {AL2/3/4_CO_ISM#050 b)}

1138 CryptographicMutualHandshake

1139 {KI.10.3.2.1#18: #18. A mutual handshake exchange based on cryptography (e.g., TLS) shall be used.
 1140 {AL2/3/4_CO_SCO#010 a)}

1141 CredentialActivation

1142 {KI.10.3.2.1#19: #19. An activation feature shall be required to use the credential (e.g., entering a PIN or
 1143 biometric information into the hardware device containing the credential).

1144 {AL2/3/4_ID_IDC#030 b) , AL3/4_CM_CRN#050 c) , AL3/4_CM_CRN#060 b), AL3/4_CM_CRD#020,
 1145 AL4_CM_CRD#030, AL3/4_CM_CRN#070 b), AL4_CM_CRN#075 c)}
 1146 {NOTE – though commonplace in AL1 services (e.g. use of a PIN), [KI-SAC] tends to ignore at AL1 and increment across
 1147 the ALs in a number of specific ways.}

1148 CodeDigitalSignature

1149 {KI.10.3.2.1#20: #20. Digital signatures shall be verified against a trusted source to counter the
 1150 downloading of software that has been modified by unauthorized parties.
 1151 {NOTE – [KI-SAC] has no such explicit requirement.}}

1152 LivenessDetection

1153 {KI.10.3.2.1#21: #21. Liveness detection techniques shall be used to identify the use of artificial biometric
 1154 characteristics (e.g., forged fingerprints).
 1155 {NOTE – [KI-SAC] has no such explicit requirement.}}

1156 **11 Service assurance criteria**

1157 {KI.11#01: Trust framework operators that seek to comply with this framework shall establish specific
 1158 criteria fulfilling the requirements of each LoA that they intend to support and shall assess the CSPs that
 1159 claim compliance with the framework against those criteria.
 1160 {Kantara IAF accomplishes this at its latest release status, most specifically the AAS, RAA and SAC.}}

1161 {KI.11#02: Likewise, CSPs shall determine the LoA at which their services comply with this framework
 1162 by evaluating their overall business processes and technical mechanisms against specific criteria.
 1163 {AL_CO_ISM#010, AL_CO_ISM#030}
 1164 {NOTE – Granting of a Kantara Approval is evidence of a CSP’s successful compliance with this requirement.}}

1165

1166

1167

Bibliography

1168 *Note – this first part of the bibliography relates only to the –generated content of this document.*

1169 [IS29115] ISO/IEC 29115:2012, *Entity authentication assurance framework* (see also
1170 [X.1254]).

1171 <http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=45138>

1172 [KI-GLOSS] Kantara Initiative K-IAF-1100 v2.1bis, *Glossary*.

1173 <[https://kantarainitiative.org/confluence/download/attachments/41649275/Kantara IAF-1100 Glossary v2-0.pdf](https://kantarainitiative.org/confluence/download/attachments/41649275/Kantara%20IAF-1100%20Glossary%20v2-0.pdf)>

1174 [KI-LoA] Kantara Initiative K-IAF-1200 v2.0, *Levels of Assurance*.

1175 <[https://kantarainitiative.org/confluence/download/attachments/41649275/Kantara IAF-1200 Levels of
1176 Assurance v2-0.pdf](https://kantarainitiative.org/confluence/download/attachments/41649275/Kantara%20IAF-1200%20Levels%20of%20Assurance%20v2-0.pdf)>

1177 [KI-SAC] Kantara Initiative K-IAF 1400 v4.0bis, *Service Assessment Criteria*.

1178 <[https://kantarainitiative.org/confluence/download/attachments/41649275/Kantara%20IAF-
1179 1400%20Service%20Assessment%20Criteria%20v4-
1180 0bis.pdf?version=1&modificationDate=1413503746000&api=v2](https://kantarainitiative.org/confluence/download/attachments/41649275/Kantara%20IAF-1400%20Service%20Assessment%20Criteria%20v4-0bis.pdf?version=1&modificationDate=1413503746000&api=v2)>

1181 [SP800-63-2] NIST Special Pub 800-63 (2014), *Electronic Authentication Guideline Version
1182 v2*.

1183 <http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf>

1184 [X.1254] Recommendation ITU-T X.1254 (2012), *Entity authentication assurance
1185 framework* (see also [IS29115]).

1186 <http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf>

1187 *Note – this second part of the bibliography consists of references cited in the original ITU-T
1188 Recommendation [X.1254].*

1189 [b-ITU-T X.1252] Recommendation ITU-T X.1252 (2010), *Baseline identity management terms and
1190 definitions*.

1191 [b-ITU-T Y.2702] Recommendation ITU-T Y.2702 (2008), *Authentication and authorization
1192 requirements for NGN release 1*.

1193 [b-ITU-T Y.2720] Recommendation ITU-T Y.2720 (2009), *NGN identity management framework*.

1194 [b-ITU-T Y.2721] Recommendation ITU-T Y.2721 (2010), *NGN identity management requirements
1195 and use cases*.

1196 [b-ITU-T Y.2722] Recommendation ITU-T Y.2722 (2010), *NGN identity management mechanisms*.

1197 [b-ISO/IEC 9798] ISO/IEC 9798:2010, *Information technology – Security techniques – Entity
1198 authentication*.

1199 [b-ISO/IEC 18014-2] ISO/IEC 18014-2:2009, *Information technology – Security techniques – Time-
1200 stamping services – Part 2: Mechanisms producing independent tokens*.

1201 [b-ISO/IEC 19790] ISO/IEC 19790:2012, *Information technology – Security techniques – Security
1202 requirements for cryptographic modules*.

1203 [b-ISO/IEC 19792] ISO/IEC 19792:2009, *Information technology – Security techniques – Security
1204 evaluation of biometrics*.

SAC mapping – ISO/IEC 29115 / ITU-T X.1254 – Entity authentication assurance framework

1205	[b-ISO/IEC 27000]	ISO/IEC 27000:2012, <i>Information technology – Security techniques – Information security management systems – Overview and vocabulary.</i>
1206		
1207	[b-ISO/IEC 27001]	ISO/IEC 27001:2005, <i>Information technology – Security techniques – Information security management system – Requirements.</i>
1208		
1209	[b-ISO/IEC 29100]	ISO/IEC 29100:2011, <i>Information technology – Security techniques – Privacy framework.</i>
1210		
1211	[b-ISO/IEC 29101]	ISO/IEC 29101, <i>Information technology – Security techniques – Privacy architecture framework.</i>
1212		
1213	[b-ISO/IEC 24760-1]	ISO/IEC 24760-1:2011, <i>Information technology – Security techniques – A framework for identity management – Part 1: Terminology and concepts.</i>
1214		
1215	[b-ISO/IEC 19790]	ISO/IEC 19790:2012, <i>Information technology – Security techniques – Security requirements for cryptographic modules.</i>
1216		
1217	[b-NIST SP800-36]	NIST Special Pub 800-36 (2003), <i>Guide to Selecting Information Technology Security Products.</i>
1218		
1219		http://csrc.nist.gov/publications/nistpubs/800-36/NIST-SP800-36.pdf
1220	[b-NIST SP800-63]	NIST Special Pub 800-63 (2006), <i>Electronic Authentication Guideline Version 1.0.2.</i>
1221		
1222		http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf
1223	[b-AGGPKI]	<i>Australian Government Gatekeeper Public Key Infrastructure.</i>
1224		http://www.gatekeeper.gov.au/
1225	[b-DuD]	Van Alsenoy B., and De Cock, D. (2008), <i>'Due processing of personal data in eGovernment? A Case Study of the Belgian electronic identity card'</i> , <i>Datenschutz und Datensicherheit</i> , Vol.32, No.3, pp.178-183.
1226		
1227		
1228	[b-EoI]	New Zealand Standard: <i>Evidence of Identity Standard Version 2.0, 2009.</i>
1229		http://www.dia.govt.nz/EoI/pdf/EoIv2.0.pdf
1230	[b-ENISA]	ENISA, <i>Mapping (Interoperable Delivery of European e-government services to public Administrations, Businesses and Citizens) IDABC Authentication Assurance Levels to SAML v2.0.</i>
1231		
1232		
1233	[b-IAF]	<i>Kantara Initiative Identity Assurance Framework v2.0.</i>
1234		http://kantarainitiative.org/confluence/display/GI/Identity+Assurance+Framework
1235	[b-MOV]	Menezes, A., van Oorschot, P., and Vanstone, S. (1997), <i>'Handbook of Applied Cryptography'</i> , pp. 3-4.
1236		
1237		http://www.cacr.math.uwaterloo.ca/hac/
1238	[b-NeAF]	<i>The National e-Authentication Framework.</i>
1239		http://www.finance.gov.au/e-government/security-and-authentication/authentication-framework.html
1240	[b-OECD]	OECD (2007), <i>OECD Recommendation on Electronic Authentication and OECD Guidance for Electronic Authentication.</i>
1241		
1242		http://www.oecd.org/dataoecd/32/45/38921342.pdf
1243	[b-OMB]	OMB Memorandum M-04-04, <i>E-Authentication Guidance for Federal agencies</i> , December 16, 2003.
1244		
1245		http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf

1246 [b-PEA] Industry Canada (2004), *Principles for Electronic Authentication: A Canadian*
1247 *Framework*.
1248 <http://strategis.ic.gc.ca/epic/site/ecic-ceac.nsf/en/h_gv00240e.html>