

# (PROTO) KANTARA INITIATIVE OVERVIEW AND GLOSSARY

Note to reviewers:

- 1) consider this a 'proof of concept' draft;
- 2) there is no claim as to its completeness in any respect;
- 3) there are many more terms in the Glossary alone that need to be reviewed and (probably mostly) incorporated. This doc as it presently stands has defined only those terms necessary to support the draft as is. Ultimately there will be many terms defined which do not merit inclusion in an overview;
- 4) effort has been made to use language which does not imply an individual person;
- 5) does it actually need to be any more complicated, as an overview? If so, I suggest that specific topic areas be defined and addressed in discrete sections, to be inserted after §5 but before §6, thus ensuring that the Glossary is the final section before Annex A (and any other annexes which are felt necessary).

## 1. SCOPE

This document addresses Kantara Initiative's **Identity Assurance Framework (IAF)** and its principle components (roles, processes, publications and glossary).

## 2. INTRODUCTION

This document provides an Overview of Kantara Initiative's **Identity Assurance Framework (IAF)** [7.4]. It also defines the terms in use within the **IAF** and provides references and links to governing documents, so as to allow interested parties to progress into further detail, as their interest dictates.

Terms in bold are defined in the **GLOSSARY**: numbers shown in this main text after the first use of a defined term relate to its index number within the Glossary and provide a hyper-link to the definition.

## 3. OVERVIEW OF THE IAF

The primary objective of the **IAF** is to provide **Assurance** [7.17] to a range of parties who have an interest in and reliance upon the degree of rigour applied to the management, operation and provisioning of electronic **Identity Proofing** [7.1] and **Credential Management** [7.3] services, as either in-house or out-sourced capabilities.

Through its **IAF**, Kantara Initiative grants **Approvals** for **Credential Services** and **Accreditation** [7.12] to **Assessors** [7.11] which meet the **IAF**'s requirements.

The principle interested parties are organizations which need to have confidence in the asserted identity of persons and other entities with which they interact in their day-to-day operations, known generally as **Relying Parties** [7.26]. By accepting credentials and authentications from **Identity Proofing** and **Credential Management** services which have been **Approved** [7.7] under the **IAF**, those **Relying Parties** will gain **Assurance** that the entities are using credentials which are

31 issued and managed by service providers whose services have been subjected to rigorous assessment by independent  
32 third parties, Kantara’s **Accredited Assessors** [7.13], following the **IAF**’s defined processes and using published and peer-  
33 reviewed **Service Assessment Criteria** [7.9].

34 Additional parties which stand to gain **Assurance** from the **IAF** are:

- 35 1) Other providers of **Credential Services** [7.6];
- 36 2) Identity and Credential Federations, seeking to establish common levels and standards of inter-working &  
37 cooperation;
- 38 3) Regulatory and other oversight bodies;
- 39 4) Standards Development Organizations.

40 Kantara Initiative and its **IAF** are recognized by various authoritative bodies World-wide, which include:

- 41 5) US Federal Identity, Credentialing and Access Management Architecture;
- 42 6) ISO JTC 1 / SC 27 / WG5 (Identity management and privacy technologies);
- 43 7) Australian Government Digital Transformation Agency;
- 44 8) ITU-T SG17 - Security.

45

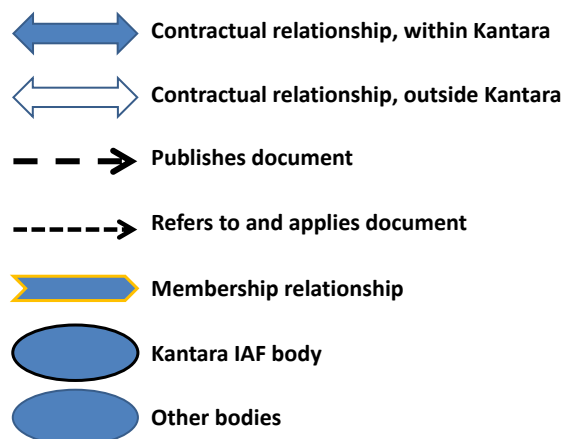
46 The principles of operation of the **IAF** are modelled on those described in ISO/IEC 17065 “Conformity assessment –  
47 Requirements for bodies certifying [...] services” (IS17065), at its latest published edition.

## 48 4. KEY RÔLES AND RELATIONSHIPS

### 49 4.1 General

50 The figures in this section show the principal rôles within the IAF and the relationships between the players in those  
51 rôles. The symbology used is:

#### Key: Relationship symbols



52

53 Each of the entities and roles within these figures is explained below.

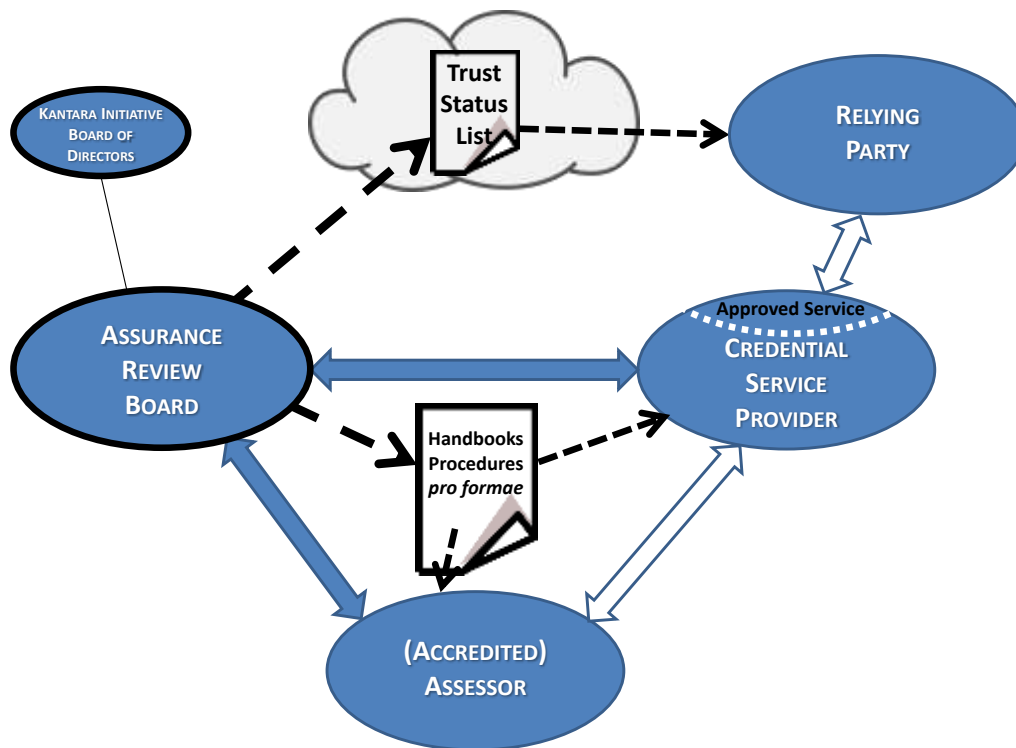
54 **4.2 Kantara Initiative Board of Directors**

55 The Board of Directors (KIBoD) is the Kantara Initiative’s executive body which oversees the entire Kantara organization’s  
56 business. It has final authority with respect to the granting, and other decisions concerning, **Accreditations** and  
57 **Approvals** within the context of the IAF. The KIBoD is also the authoritative source of mandates given to the two  
58 principal entities within the IAF, as described in §4.3 and §4.4. Most participants in the IAF will have little interaction  
59 with the KIBoD itself, but will spend the vast majority of their interactions with one or both of these two entities, as well  
60 as other roles described in the following clauses.

61 The constitution of the KIBoD is beyond the scope of this document. Refer to Kantara Initiative’s website  
62 (<https://kantarainitiative.org/trustees/>) for further information about the KIBoD and its membership.

63 **4.3 Assessment Review Board**

64 Figure 1 focuses on the rôles around the IAF’s **Assessment Review Board (ARB)** [7.18].



65  
66

Figure 1: ARB and related roles

67 The **ARB** receives its operational mandate from the KIBoD and is responsible for the day-to-day management and  
68 operation of the **IAF**. Its principle functions are the accepting and reviewing of applications for **Accreditation** and for  
69 **Approval**, and in making recommendations to the KIBoD for the granting of these qualifications. The **ARB** is also  
70 empowered to reject or request additional supporting information from applicants wherever it feels it has insufficient  
71 information on which to base an y recommendation to the KIBoD.

72 The **ARB** also ensures that contractual arrangements are put in place with Accredited Assessors and Credential Service  
73 Providers to protect Kantara Initiative’s marks, logos, and terms of use.

74 Additionally, the **ARB** is responsible for documenting and publishing its **Accreditation** and **Approval** procedures and  
75 other supporting documents and *pro formae*, for handling enquiries from any parties concerning the **ARB**'s functions,  
76 and for publishing details of those entities which have been granted **Accreditation** or **Approval** in its [Trust Status List](#).

77 The ARB is composed of subject matter experts from a range of fields applicable to the assurance of identity proofing,  
78 credential management and authentication services.

#### 79 **4.4 Relying Party**

80 A **Relying Party** is an entity which places reliance in the fact that the appearance of a **CSP**'s or an **Assessor**'s service in  
81 Kantara's Trust Status List is an indication that that party has been subjected to rigorous and objective review and  
82 evaluation as to its ability to meet defined requirements and to continue its conformity to them, and hence that the  
83 service offered can be relied upon to the stated level of assurance. In the most common usage a **Relying Party** is  
84 considered to be an organizational entity which wants to have a reliable basis for knowing the identity of the **End Users**  
85 with which it enters into some form of transaction. The legal/contractual basis on which such transactions are entered  
86 into is outside the scope of the **IAF**.

87 In other potential usages a **Relying Party** could be an **End User** requiring to be issued with an identity credential which  
88 might allow it to be a participant in such transactions, a **CSP** wishing to find an **Accredited Assessor**, or any other  
89 interested party which wishes to derive confidence from the fact that Kantara Initiative has published an entity's details  
90 in its Trust Status List.

#### 91 **4.5 Accredited Assessor**

92 This is an entity which, organizationally and in terms of the competence of named personnel, has demonstrated to the  
93 **ARB** that it meets the required knowledge and skill qualifications set by the **IAF** (as described in the **IAF**'s applicable  
94 documented procedures etc.) and has been granted **Accreditation**. **Accredited Assessors** must establish a formal  
95 contractual arrangement with Kantara Initiative [through the TMLA ]but the legal/contractual basis on which they  
96 contract with the CSPs they assess is outside the scope of the **IAF**.

97 A grant of **Accreditation** is valid for three years, with annual reviews taking place in the two intervening years.

#### 98 **4.6 Credential Service Provider**

99 This is an entity which, organizationally and in terms of service operation and provision, has demonstrated to the **ARB**  
100 that it meets the applicable criteria set by the **IAF** (as described in the **IAF**'s applicable documented procedures, **Service**  
101 **Assessment Criteria**, etc.) and has been granted **Approval** for the given service. **CSPs** must establish a formal  
102 contractual arrangement with Kantara Initiative [through the TMLA ]but the legal/contractual basis on which they  
103 contract with their **Accredited Assessors** and with **Relying Parties** is outside the scope of the **IAF**.

104 A grant of **Approval** is valid for three years, with annual conformity reviews taking place in the two intervening years.

105

## 4.7 Identity Assurance Work Group

Figure 2 focuses on the rôles around the IAF's **Identity Assurance Work Group (IAWG)** [7.19].

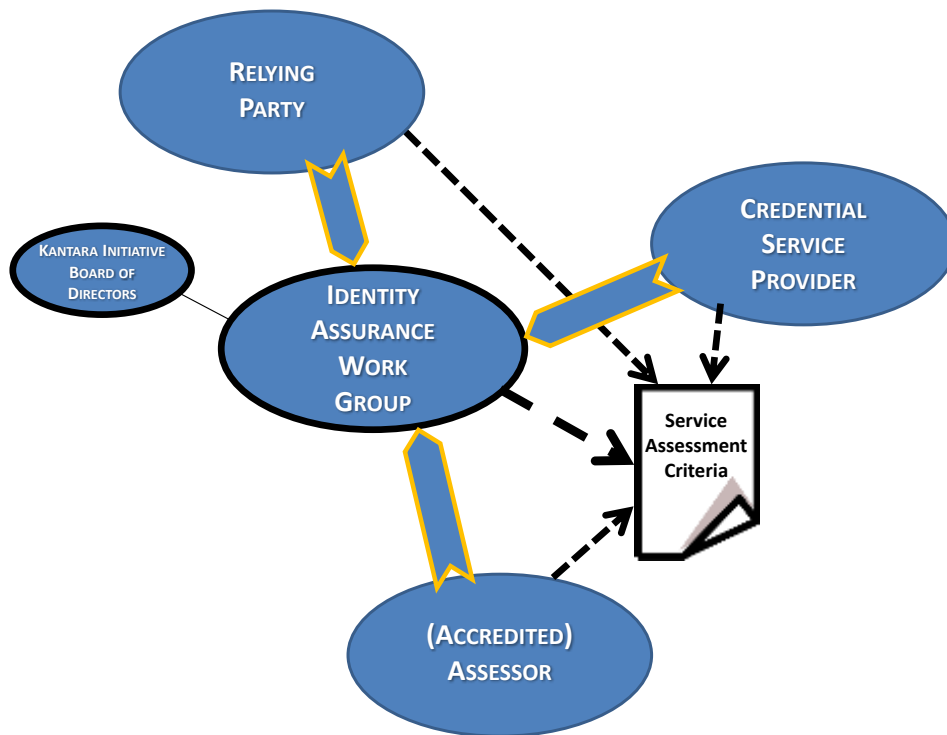


Figure 2: IAWG and related roles

The **IAWG** receives its operational mandate from the KIBoD and is responsible for the **IAF's Service Assessment Criteria**. Its principle functions are the drafting, review and approval of the **SAC** and of any relating documented processes etc. The **IAWG** has established processes which ensure that before being approved for use all SAC and other relevant publications are subject to internal **IAWG** review and, where the subject of review is new or has undergone material change, then public review. Following these reviews the **IAWG** is empowered to approve its own outputs without further reference to the KIBoD.

The **IAWG** is composed of subject matter experts from all perspectives of Kantara Initiative's interested parties: **Credential Service Providers**, **Accredited Assessors** and, importantly, **Relying Parties**. Membership of Kantara Initiative is required and participants are bound by terms and a code of conduct.

## 5. SERVICE APPROVALS

### 5.1 Introduction

Granting **Approvals** to **Credential Services** is the *raison d'être* of Kantara Initiative's **IAF**. Even though **Accreditation** is an equally formally-administered process, it is but a means to an end, that being to ensure that **Assessments** on which **Approvals** are based have been conducted by suitably qualified and competent organizations and persons, thus underpinning the assurance given by the **IAF**.

There are a number of varying perspectives on Approvals which are brought out in the following sections.

## 5.2 Classes of Approval

The IAF supports multiple **Classes of Approval**. Each is distinguished by a principal reference document, such as a specific piece of legislation or standard. These may be generally-applicable or could respond to the needs of a specific sector or domain. Each Class is separately recognized in the IAF's [Trust Status List](#), and is described [here](#).

## 5.3 Full Service versus Component Service Approval

A CSP is not obliged to provide a service which covers the entire life-cycle of credential management functions (which would be a Full Service), and may elect to offer just a sub-set of functionality, which will be referred-to as a Component Service, and indicated as such in the IAF's [Trust Status List](#).

## 5.4 Service Approval Cycle

Service Approvals operate on a triennial (three year) cycle. At the start of each cycle a full 'Triennial' assessment is required. The scope of this assessment will be all of the functionality described for the service, be it a Full Service or a Component Service. In each if the following two years a lesser scope of assessment is required, known as an Annual Conformity review, in which a subset of the applicable criteria are assessed.

There is an available modification to this, in that a very initial assessment may only assess the service in a 'static' sense, i.e. it has yet to commence operations. This is known as a 'Ready To Operate' assessment, and is intended to permit the CSP to show that their service meets the applicable criteria in a conformant manner, but for the fact that it cannot yet be shown to be operating conformantly. After a specified minimum period of time of operations the CSP can then be subjected to a 'Fully Operational Service' (FOS) assessment, which will address those criteria which now have operational records available for the demonstration of conformity. Until the 'FOS' assessment has been successfully concluded, the initial Triennial assessment is not considered concluded and the three-year cycle only then begins.

# 6. PRIMARY DOCUMENTS

The IAF has a number of primary documents, authority for which falls under either the **ARB** or the **IAWG**. All of these documents are available either in the public domain or to members of Kantara Initiative. These documents are:

Document reference: [KIAF-1050](#)

Document title: Overview and Glossary

Approved by: IAWG

Scope: This present document.

Document reference: [KIAF-1340](#)

Document title: Service Assessment Handbook

Approved by: ARB

Scope: Processes and procedures for how the ARB, CSPs and Assessors are required to operate in the performance and review of a service assessment.

## (Proto) Overview and Glossary (KIAF-1050 v0.3z)

- 159 Document reference: [KIAF-1350](#)  
160 Document title: Assessor Accreditation Handbook  
161 Approved by: ARB  
162 Scope: Processes and procedures for how the ARB, and Assessors are required to operate in the  
163 performance and review of an assessor accreditation.
- 164 Document reference: [KIAF-1410](#)  
165 Document title: Commonly-Applicable Service Assessment Criteria  
166 Approved by: IAWG  
167 Scope: Assessment criteria which apply to any service assessment, for any assurance level.
- 168 Document reference: [KIAF-1420](#)  
169 Document title: Operational 63-2 Service Assessment Criteria  
170 Approved by: IAWG  
171 Scope: Assessment criteria which apply to an assessment of a service against NIST SP 800-63 rev.2,  
172 for any assurance level.
- 173 Document reference: [KIAF-1430](#)  
174 Document title: SP 800-63A Service Assessment Criteria  
175 Approved by: IAWG  
176 Scope: Assessment criteria which apply to an assessment of a service against NIST SP 800-63A  
177 (rev.3), for IAL2.
- 178 Document reference: [KIAF-1440](#)  
179 Document title: SP 800-63B Service Assessment Criteria  
180 Approved by: IAWG  
181 Scope: Assessment criteria which apply to an assessment of a service against NIST SP 800-63B (rev.3),  
182 for AAL2.
- 183 Document reference: [KIAF-1610](#)  
184 Document title: Required Assessor Knowledge and Skills  
185 Approved by: ARB  
186 Scope: Requirements to be met by assessors wishing to be Accredited iaw KIAF-1350.

187 Other documents exist but are more focused and specific to particular aspects of the **IAF**, and hence are not considered  
188 to be deserving of mention in this overview. Such documents will be referenced as appropriate in the documents  
189 identified above.

190 Additional information about the **IAF**, and links to the above and other pertinent documents (e.g. various *pro formae*,  
191 etc.) can be found at these web pages:

192 <https://kantarainitiative.org/trust-registry/trust-status-list/>

193 *and others, as deemed relevant to an overview.*

194

## 7. GLOSSARY

The following definitions are for use across Kantara Initiative's **Identity Assurance Framework**. They align to generally-accepted usage in the identity and credential management community and are used within the **IAF** with their given specific meanings. Though there may be commonly-defined and named terms, or similar terms and/or definitions in this Glossary, Kantara Initiative makes no claim as to the value or legitimacy of these definitions in any other situation or context.

Simple principals have been employed in creating them. Firstly, a definition should be able to be expressed in a single sentence, otherwise it is too complicated and/or the definition drafter has done a poor job. Secondly, although notes have been provided in some cases, the definition must not rely on the note to be understood (otherwise the first rule is broken). Thirdly, the definitions are presented in a relational order, respecting the rule wherein no definition may use another defined term unless that term has been previously defined. This ordering has two clear benefits:

- 1) The ordering of terms builds a story as they are read-through in the order presented herein;
- 2) By observing the principal of requiring a used term to be previously defined there is a guarantee of non-circularity.

Some readers may perceive drawbacks, such as:

- 1) Some definitions may be a little vague in view of the desire to observe the referencing rule (above) and a consequence of a very conscious effort to not use a defined term, whatever the immediate convenience it appears to offer; and
- 2) To some, the idea of a non-alphabetic glossary is anathema. For them, and upon the agreement and formalization of these definitions, the definitions could be indexed and a separate Annex could be produced with them in alphabetic order paired with their corresponding relational index reference. (See proto-Annex A: QED!)

Given the draft nature of these definitions, some uncertainty surely exists. Text in [...] is proposed as either optional or additional text (you judge!). The author requests that any attempts at improvement follow the rules above and do not change terms unless it can be proven that they are merely 'links' to enable other definitions to work, i.e. if the term is used within the IAF's documentation suite then it cannot be removed / replaced (except at some cost of editing and republication).

### 7.1 Identity Proofing

the function of collecting evidence [identity attributes] which supports a claim of identity [for a specific entity] and the validation and verification of that evidence so as to determine the veracity (or otherwise) of the claim.

### 7.2 Proven Identity

an identity which has successfully passed the checks made during **Identity Proofing**.

### 7.3 Credential Management

the functions of binding a **Proven Identity** to a credential, of confirming the legitimacy of a credential when it is put to use, and of managing the credential across its life-span.



231

232

*Note - **Credential Management** can also be used in a broader, all embracing, sense, as a convenient term when the distinction is not relevant, to include the **Identity Proofing** function.*

233

234

235

#### 7.4 Identity Assurance Framework

236

Kantara Initiative's [certification scheme | framework] established for the purposes of providing trust and confidence in the provision of [electronic] **Identity Proofing** and **Credential Management** services.

237

238

Abbrv: **IAF**.

239

#### 7.5 Credential Service Provider

240

an organization which provides the functions of a[n electronic] **Identity Proofing** and **Credential Management** service, either in full or as a discrete component (i.e. a sub-set of the functions).

241

242

Abbrv: **CSP**.

243

#### 7.6 Credential Service

244

an **Identity Proofing** and/or **Credential Management** service as offered by a **Credential Service Provider**.

245

#### 7.7 Approval

246

recognition that a **Credential Service** has been subjected to a specific process and has been found to meet the **IAF**'s applicable requirements concerning its operation and provision.

247

248

#### 7.8 Approved Service

249

a **Credential Service** which has been granted **Approval**.

250

#### 7.9 Service Assessment Criteria

251

a formal set of requirements established as the basis on which **Approval** may be granted.

252

Abbrv: **SAC**.

253

#### 7.10 Assessment

254

a process of reviewing a **Credential Service** against **Service Assessment Criteria**.

255

#### 7.11 Assessor

256

an organization (or a representative thereof) which performs **Assessments**.

257

#### 7.12 Accreditation

258

recognition that an **Assessor** has been subjected to a specific process and has been found to meet the **IAF**'s applicable requirements concerning its operation.

259

260

#### 7.13 Accredited Assessor

261

an **Assessor** which has been granted **Accreditation**.

262

263

*Note – some of the IAF's documents will use 'Assessor' instead of 'Accredited Assessor' where it is*

264 contextually evident that the **Assessor** in question must be an **Accredited Assessor** in order to fill the  
265 described role. E.g., the '**Kantara Assessor's Report**' explicitly omits '**Accredited**'.

266

267

#### 268 7.14 Class of Approval

269 **Approval** granted on the basis of an **Assessment** against a [specific | defined] set of **Service Assessment**  
270 **Criteria**.

271 Abbrv: **CoA**.

#### 272 7.15 Statement of Conformity

273 a record of which **Service Assessment Criteria** specifically apply to a **Credential Service** undergoing  
274 **Assessment**, the **Credential Service Provider's** evidence of conformity and the **Accredited Assessor's**  
275 findings, after review of the **Credential Service Provider's** evidence.

276 Abbrv: **SoC**.

#### 277 7.16 Kantara Assessor's Report

278 a record prepared by an **Accredited Assessor**, for a **Credential Service Provider**, documenting their process  
279 and findings following the termination of an **Assessment**.

280 Abbrv: **KAR**.

281

282 *Note – 'termination' is used in preference to 'performance', since the Assessment may not be fully performed,*  
283 *yet a report should be produced on the termination of an Assessment howsoever it concludes.*

#### 284 7.17 Assurance

285 the degree of trust and/or confidence that due process was correctly and competently applied in the case of  
286 an **Approved Service** or an **Accredited Assessor**.

#### 287 7.18 Assurance Review Board

288 the Kantara Initiative body charged with responsibility for reviewing all submissions for **Approval** and for  
289 **Accreditation**, and for related activities and works.

290 Abbr. **ARB**.

#### 291 7.19 Identity Assurance Work Group

292 the Kantara Initiative body charged with responsibility for drafting, reviewing and approving the IAF's **Service**  
293 **Assessment Criteria**, and for related activities and works.

294 Abbr. **IAWG**.

#### 295 7.20 Level of Assurance

296 refer to [NIST SP 800-63 rev.2](#).

297 Abbr. **LoA**.

#### 298 7.21 Assurance Level

refer to [NIST SP 800-63 rev.3](#).

*Note – NIST SP 800-63 rev.3 refers to Identity, Authentication and Federation Assurance Levels, abbreviated to IAL, AAL and FAL respectively.*

## 7.22 Applicant

an entity which presents, or is presented, for **Identity Proofing**.

## 7.23 Subject

an **Applicant** which has had its **Proven Identity** bound to a credential.

*Note – astute readers may observe that an **Applicant** is not considered to have undergone the state-change to **Subject** until binding has occurred. One could consider that an **Applicant** which exists in this ill-defined stasis between Applicant and Subject is a ‘**Proven Applicant**’, since they have a **Proven Identity** which has yet to be made into a useful ‘thing’. Such a formal definition could easily be added if it is felt useful to do so. Conceptually, a ‘**Proven Applicant**’ could be a logical parcel to share around until some other entity chooses to bind it to a ‘something’, so long as the the proofing **Credential Service** can be authenticated as to establish the veracity of any such parcel.*

## 7.24 Claimant

an entity presenting a credential as the basis for proving itself to be the **Subject**.

## 7.25 Authentication

the function of confirming the legitimacy of a **Claimant**[, i.e. that the **Claimant** is indeed the **Subject** which it claims to be].

## 7.26 Relying Party

an entity which chooses to determine its own actions based upon an **Authentication**[ regarding the **Subject** party or that party’s actions].

Abbr. **RP**.

*Note – this is deliberately a very broad definition under which an **RP** could be considered to be, e.g.:*

*i) a regulatory body which sees no need to exercise its regulatory powers so long as the assurances are provided;*

*ii) a **CSP** wishing to secure the services of an **Accredited Assessor**;*

*iii) a consumer of an **Approved Service** (which could be another **CSP** if a component service is under consideration) which wishes to be confident that the provider of the service has been subjected to an independent assessment process against defined criteria.*

*Other forms of **RP** can probably be described but hopefully the point is made.*

*An alternative, narrower, definition would address only the third exemplar, and could be:*

336 “an entity which chooses to determine its own actions based upon **Assurance** regarding an **Approved**  
337 **Service**”.

338 **7.27 End User**

339 a general purpose term for an entity which may require a credential to be bound to it or which may already  
340 have a credential bound to it and which is expected to participate in some form of transaction with a **Relying**  
341 **Party** or with a **Credential Service Provider**, without defining any particular status to the entity.

342

343 **Annex A**

344 The following provides an alphabetically-ordered list of glossarial terms, and their associated (and hyper-linked) index  
345 number.

<b>Term</b>	<b>Index</b>
<b>A</b>	
Accreditation	<a href="#">7.12</a>
Accredited Assessor	<a href="#">7.13</a>
Applicant	<a href="#">7.22</a>
Approval	<a href="#">7.7</a>
Approved Service	<a href="#">7.8</a>
Assessment	<a href="#">7.10</a>
Assessor	<a href="#">7.11</a>
Assurance	<a href="#">7.17</a>
Assurance Level	<a href="#">7.21</a>
Assurance Review Board	<a href="#">7.18</a>
Authentication	<a href="#">7.25</a>
<b>C</b>	
Claimant	<a href="#">7.24</a>
Class of Approval	<a href="#">0</a>
Credential Management	<a href="#">7.3</a>
Credential Service	<a href="#">7.6</a>
Credential Service Provider	<a href="#">7.5</a>
<b>E</b>	
End User	<a href="#">7.27</a>
<b>I</b>	
Identity Assurance Framework	<a href="#">7.4</a>
Identity Assurance Work Group	<a href="#">7.19</a>
Identity Proofing	<a href="#">7.1</a>
<b>K</b>	
Kantara Assessor's Report	<a href="#">7.16</a>
<b>L</b>	
Level of Assurance	<a href="#">7.20</a>
<b>P</b>	
Proven Identity	<a href="#">7.2</a>
<b>R</b>	
Relying Party	<a href="#">7.26</a>
<b>S</b>	
Service Assessment Criteria	<a href="#">7.9</a>
Statement of Conformity	<a href="#">7.15</a>
Subject	<a href="#">7.23</a>

346

347