Document or Set Title: Draft Recommendation: Identity Assurance Framework 1100, 1300, 1400, 1800

Document Status: Open

Originating Work Group: Identity Assurance Working Group

Comment Review Period Closing Dates: July 14, 2012

Submitted to Leadership Council:

Leadership Council Comments:

Reference Key: DocumentSet_ReviewCloseDate_#number

Reference #	Comment Submitted	Status	WG Resolution
1400_14July_03	For all ALn_CM_ASS#030 (Proof of Possession) criteria: I am not sure that the term CLAIMANT (a proxy for the SUBJECT) should be proving possession of the authentication token.	In Process	Ken will look up definition of Applicant, Subject and Claimant and circulate to the list while we come to resolution on what the terms means and how to use them.
1400_14July_06	Assertion Security Validation and Assertion Security The criteria for AL1_CM_ASS#010 and AL2_CM_ASS#010 appear to be more extensive than those being proposed for AL3_CM_ASS#010 and AL4_CM_ASS#010.	CLOSED	**9/6/2012** - Deferred - Requires resolution for the aligning with SP 800-63
1400_14July_07	Credential Issuing In-Person Public Identity Verification The only difference between AL3_ID_IPV#020 Evidence checks and AL4_ID_IPV#030 Evidence checks – primary ID is the title. As the criteria in AL3_ID_IPV#020 (and for	CLOSED – but need to start with this on the next call to update everyone on what we discovered.	**9/6/2012** Rejected - Different philosophy on evidence checks because of the requirements for

	AL2_ID_IPV#020) address, in essence, the Primary ID document I would suggest that the title for AL3_ID_IPV#020 (as well as for AL2_ID_IPV#020) become Evidence checks – primary ID. In addition, I would suggest that the number for AL4_ID_IPV#030 become AL4_ID_IPV#020 (not currently used).		PKI at level 4 Rejected because the comparable criterion doesn't exist at the lower assurance levels?
1400_14July_02	Line 301-302: Currently says, "…defined in Section 2 and in the Identity Assurance Framework: Levels of Assurance document." I do not believe that the reference to the "Identity Assurance Framework: Levels of Assurance" document is required as it is contained in Section 2. As such I would suggest the text become, "…defined in Section 2." I believe that this is also the case for lines 1380-1383 (in section 5).	CLOSED	**08.23.2012** - Accept and change to "at all ALs referred to in section 2."
1400_14July_01	Line 233 – Currently says, "This document sets our normative Kantara requirements …" Should this be, "This document sets **out** normative Kantara requirements …"?	CLOSED	**08.23.2012** – Accept
1100_14July_01	ACCREDITATION) APPLICANT: The specific term is not used in the SAC(1400), RAA(1800), AAS(1300) or LOA(1200). The term APPLICANT is used throughout. The term is defined in AQR(1600) but does not appear in the text. The term APPLICANT is used throughout. The term APPLICANT is applicable to both cases – an assessor or a CSP. I would recommend removing the term (ACCREDITATION) APPLICANT from the Glossary.		
1100_14July_02	ANNUAL CONFORMITY REVIEW (ACR): I would suggest that the focus of the ANNUAL CONFORMITY REVIEW (ACR)		

	should be the Certified Service rather than the Grantee. In my opinion, a Grantee is an organization that, because they have a Certified Service, has been granted the right to use the Kantara Initiative Mark. Based on this I would suggest the following definition for the term ANNUAL CONFORMITY REVIEW (ACR): Review undertaken annually by the ARB (Assurance Review Board) of all Certified Services as a positive check and reminder that their conformity to the appropriate agreement, and therefore the requirements of the AAS(1300), remains their obligation.		
1100_14July_03	APPLICANT: I believe that the SAC(1400) specific definition is the ITU definition of CLAIMANT. In reviewing the criteria in the SAC(1400) it appears that the term SUBJECT should be used rather than APPLICANT. Based on this I would suggest the following definition for the term APPLICANT: An organization which is applying for Kantara Approval or Accreditation.		
1100_14July_04	APPROVED ENCRYPTION: I would recommend that the definition of the term should not be US government specific. Based on this I would suggest the following definition for the term APPROVED ENCRYPTION: Any cryptographic algorithm or method specified by a recognized national technical authority or, in the absence of a national technical authority, an international technical authority		
1100_14July_05	ASSERTION: Why has the definition for the term from the SAML glossary not been used? The existing definition could be used as an example. To remain		

	consistent with SAML I would suggest that “verifier” be changed to “authoritative party” and that “subscriber” be changed to “subject” (the rational for this is discussed in comments about the terms Subject and Subscriber). Based on this I would suggest the following definition for the term ASSERTION: A statement made (by an entity) without accompanying evidence of its validity. For example, a statement from an authoritative party to a relying party that contains identity or other information about a subject.		
1100_14July_06	ASSESSMENT: In order to eliminate some typos and ease of readability I would suggest the following definition for the term ASSESSMENT: A process used to evaluate a credential service, and the provider of that service, for compliance with all applicable requirements specified in one or more Service Assessment Criteria.		
1100_14July_07	ASSURANCE LEVEL (AL): I would suggest that the current definition of the term is too detailed and specific to Credential / Identity Levels of Assurance. As well, I would suggest that including the definition of the levels adds nothing to the definition. The levels are defined in the SAC(1400) or in a separate document and should not be repeated in the glossary. Based on this I would suggest the following definition for the term ASSURANCE LEVEL (AL): A level of confidence which may be relied upon by others that a statement or fact is true. For example, the level of confidence that the individual who uses the credential is the individual to whom the credential was issued		

1100_14July_08	ATTRIBUTE: The term is not used in the SAC(1400), RAA(1800) or AAS(1300) or LOA(1200). The use of the term in the AQR(1600) is not in the same context as the other documents. I would recommend removing the term ATTRIBUTE from the Glossary		
1100_14July_09	AUDIT ORGANIZATION: What is the difference between AUDIT ORGANIZATION and ASSESSOR? Both definitions seem to be the same. I would recommend using ASSESSOR and removing the term AUDIT ORGANIZATION from the Glossary. AUDIT ORGANIZATION is who is doing the assessments today but, in the future, that could change. All that is required to do an assessment is certification by Kantara (it happens that AUDIT ORGANIZATIONS have an easier ability to get certified).		
1100_14July_10	AUTHENTICATION PROTOCOL: I believe that the current definition of the term is at variance to the definition of the concept PROTOCOL that appears in SAML. I would suggest the following definition for the term AUTHENTICATION PROTOCOL to more closely align to the concept of protocol in SAML: A well-specified message exchange process that requests an authentication and the return of a corresponding assertion. For example, requesting authentication of the possession of a token by a claimant with the corresponding assertion of truth. Some authentication protocols include cryptographic keys that are used to protect the entire session		

1100_14July_11	AUTHENTICATION: I believe that the current definition of the term is at variance to the definition that appears in several dictionaries. I would suggest the following definition for the term AUTHENTICATION which I believe is more aligned with the dictionary definition as well as being more applicable to all situations from pseudo anonymous credentials to identity credentials: The process of establishing truth or genuineness to generate an assurance. For example, authentication establishes identity, not what the subject with that identity is authorized to do or what access privileges he or she has.		
1100_14July_12	AUTHORITATIVE PARTY: I propose the following definition for the term AUTHORITATIVE PARTY which appears in the proposed definitions for FEDERATED IDENTITY MANAGEMENT and RELYING PARTY: An organization or individual that is trusted to be an authority on the identity related attributes or roles associated with Subscribers and Subjects. The definition comes from the draft report of the Attribute Management Discussion Group.		
1100_14July_13	CERTIFIED SERVICE: I propose the following definition for the term CERTIFIED SERVICE which appears in the current definition of the terms APPROVAL and APPROVED SERVICE: A service that has been assessed by a Kantara-Accredited Assessor has having met applicable Service Assessment Criteria		

1100_14July_14	CLAIMANT: I believe that the current definition of the term is at variance to the definition in ITU. I would suggest the following definition for the term CLAIMANT to more closely align to the ITU: An entity which is or represents a subject for the purposes of authentication. A claimant includes the functions necessary for engaging in authentication exchanges on behalf of a subject.		
1100_14July_15	CREDENTIAL SERVICE: I believe that the phrase, “the verification of identities (identity proofing),” in the definition of the term does not add anything to the definition. In addition, it will need to be removed in the case of pseudo anonymous credentials as with credentials there is no knowledge of the identity of the subscriber. Based on this I would suggest the following definition for the term CREDENTIAL SERVICE: A type of electronic trust service that supports the issuance of assertions / credentials / tokens, and the subsequent management of those credentials (for example, renewal, revocation, and the provision of related status and authentication services).		
1100_14July_16	CREDENTIAL: I believe that the third sentence of the definition of the term is not needed. In addition, I believe that a CREDENTIAL is issued to a SUBSCRIBER. However, while the SUBSCRIBER may be (and in most cases is) the SUBJECT whose identity needs to be verified, it is not absolutely the case. Also, in the case of pseudo anonymous credentials, there is no knowledge of the identity of the subscriber. Based on this I would suggest the following definition for the		

	term CREDENTIAL: An unique physical or electronic object (or identifier) to be verified when presented in an authentication transaction. A credential can be bound in some way to the subscriber to whom it was issued, or it can be a bearer credential.		
1100_14July_17	ELECTRONIC CREDENTIAL: Why specifically define the term? Is it not a type of CREDENTIAL? The term is not used in the SAC(1400), RAA(1800), AAS(1300) or AQR(1600). It appears in the current definition of the term CREDENTIAL. However, I am proposing a new definition that does not include it. It also appears in LOA(1200) but could be changed to CREDENTIAL. I would recommend removing the term ELECTRONIC CREDENTIAL from the Glossary.		
1100_14July_18	FEDERATED IDENTITY MANAGEMENT: The term is not used in the SAC(1400), RAA(1800), AAS(1300), AQR(1600) or LOA(1200). I would recommend removing the term FEDERATED IDENTITY MANAGEMENT from the Glossary. This being said, I believe that the current definition appears to be a definition of Single Signon. If the term remains in the Glossary I would suggest the following definition: A system that allows organizations that rely upon identity to trust the assertions of identity made by other organizations. That is, Relying Parties can rely upon the assertions made by Authoritative Parties.		
1100_14July_19	IDENTIFER: The term only appears in AL4_ID_IPV#050 Applicant knowledge checks. Its use there is well defined.		

	The term also appears in the definition of other terms in the glossary (IDENTITY and IDENTITY AUTHENTICATION). Its use in the definitions of IDENTITY and IDENTITY AUTHENTICATION has been removed. The term is not used in RAA(1800), AQR(1600) or LOA(1200). The use of the term in AAS(1300) is not applicable. As such, and given it could be used in other contexts where it might be construed to have other meaning, I would recommend that the term IDENTIFER be removed from the Glossary.		
1100_14July_20	IDENTITY ATTRIBUTE: I propose the following definition for the term IDENTITY ATTRIBUTE which appears in the proposed definition for the term IDENTITY: Information — including biological or physiological information — bound to a subject's identity that specifies a characteristic of the subject. The definition, with the exception of the phrase "biological or physiological information", comes from the draft report of the Attribute Management Discussion Group.		
1100_14July_21	IDENTITY AUTHENTICATION: The definition of the term seems to focus on the validity of the relationship between an Identity Attribute (Identifier) and an Identity. It is unclear, in looking in the SAC(1400), about how the definition was determined. The definition of the term does not appear to align with the definition in ITU for entity authentication (ITU states use of the term authentication in an IdM context is taken to mean entity authentication). I would suggest the following definition for the term		

	IDENTITY AUTHENTICATION to more closely align to both the ITU and the definition of the term AUTHENTICATION: The process of establishing confidence in the validity of a subject's claimed identity: that the subject really is who they claim to be. Alternatively, since the terms IDENTITY and AUTHENTICATION have been defined the term IDENTITY AUTHENTICATION can be removed from the glossary.		
1100_14July_22	IDENTITY BINDING: The current definition of the term appears to be an instance (type) of "Level of Assurance". Based on this I would suggest the following definition for the term IDENTITY BINDING: The process of establishing the relationship between a Credential and an Identity.		
1100_14July_23	IDENTITY CONTEXT: I propose the following definition for the term IDENTITY CONTEXT which appears in the proposed definition for the term IDENTITY: The environment or circumstances in which identity information is communicated and perceived. Subjects operate in multiple identity contexts (e.g., legal, social, employment, business, pseudonymous) and may identify themselves differently based on the context. The definition comes from the draft report of the Attribute Management Discussion Group.		
1100_14July_24	IDENTITY: I believe that the current definition of the term is at variance to the definition in ITU. I would suggest the following definition for the term IDENTITY to more closely align to the		

	ITU: The representation of a Subject in the form of one or more information attributes (Identity Attributes) which allow the Subjects to be sufficiently distinguished within context.		
1100_14July_25	RELYING PARTY (RP): I believe that the current definition of the term is at variance to the definition in ITU. I would suggest the following definition for the term RELYING PARTY (RP) to more closely aligns to the ITU: A party that relies upon an assurance(s) (of credential or identity) from another party (Authoritative Party). For example, a party that relies upon an assertion about a subscriber's credentials, in order to grant access to a system. I propose a definition for the term AUTHORITATIVE PARTY elsewhere,		
1100_14July_26	SUBJECT: I believe that the current definition of the term is at variance to the definition of the term PRINCIPAL in the definition in ITU (PRICIPAL appears to be synonymous with SUBJECT). I would suggest the following definition for the term SUBJECT: A party whose identity can be authenticated. A subject and a subscriber can be the same entity.		
1100_14July_27	TOKEN: I do not believe that a CLAIMANT possesses and controls a TOKEN. Rather, I believe that a token is something that a SUBSCRIBER, rather than a CLAIMANT, possesses and controls that they use during authentication. (See discussion of CLAIMANT) Additionally, I believe that a SUBSCRIBER would be issued a TOKEN as they are issued a CREDENTIAL. I am		

	unclear of the difference between TOKEN and CREDENTIAL. I have thought of a TOKEN as a part of or a type of CREDENTIAL. I would suggest the following definition for the term TOKEN: Something that a Subscriber possesses and controls (typically a key or password) that is used to authenticate the Subscriber.		
1100_14July_28	VERIFIER: The term, which appears in the definition of the term ASSERTION and throughout the SAC(1400), has not been defined. I would recommend that it be changed to AUTHORITATIVE PARTY.		
1400_14July_04	The term APPLICANT is used in the criteria in the SAC(1400) when I believe that the term SUBJECT should be used. The use of APPLICANT in sections 1, 2, and 3 as well as line lines 300-306 of section 4 appears to be correct.		
1400_14July_05	The concept of a CLAIMANT needs to be worked into the criteria in the SAC(1400) wherever the term SUBJECT is used. It needs to be determined where a CLAIMANT can be involved and when the SUBJECT must be involved.		
1400_14July_08	SUBJECT: My previous suggestion implied a need to know the true identity of the individual rather than to be able to uniquely distinguish the individual. I would suggest refining my proposed definition of SUBJECT to the following: A party that can be uniquely distinguished (for the purposes of providing service, ensuring accountability, etc. A subject and a subscriber can be the same entity.		

1400_14July_09	SUBSCRIBER: I believe that the current definition of the term assumes an electronic trust service whereas it should refer to all modes of trust services. The credential issued by a trust service could be authenticated manually as well as electronically. I would suggest the following definition for the term SUBSCRIBER: A party that has entered into an agreement to use a trust service. A subscriber and a subject can be the same entity.		
1400_14Jul_10	**Note: Comment received after comment period closed (17 July 2012)** Thanks for the effort. If each sentences could be shorter, it would be much easier for non-native readers. If possible, please break up the long sentences.		
1800_14July_01	Line 65 – Currently says, “This document sets our normative Kantara requirements …” Should this be, “This document sets **out** normative Kantara requirements …”?		
1800_14July_02	Line 73 – a question mark (?) appears after Kantara Initiative Trust		
1800_14July_03	Self-selection of the relevant OP-SAC criteria by the Applicant for Service Component Approval (IAF-1800, page 7, section 3.1.2, lines 117-118) is too ambiguous and open to interpretation. The ARBâ€™s retained rights are only to ask the Applicant to justify their scope of the SoC (IAF-1800, Section 3.1.2, line 119), but not to request modification of		

	it. The references to the relevant criteria (IAF-1100, page 11, definition of Service Component; IAF-1300, page 24, section 6.2 Type of Grant, lines 627-629; and IAF-1400, page 8, section 3.2 Criteria Applicability, lines 219 to 220; and others) should all link to a mapping (probably ideally included in IAF-1800, Rules governing Assurance Assessments) of the relevant OP-SAC criteria for a valid Service Component, such as an Identity Proofing Provider or a Credential Provider.		
1300_14July_01	Line 131 – Currently says, "This document sets our normative Kantara requirements …" Should this be, "This document sets **out** normative Kantara requirements …"?		
1300_14July_02	Section 2 (lines 188-202) – All of these definitions appear in the glossary. As such I would recommend they be removed from this document.		
1300_14July_03	Line 330 – The current text is, "When an Application is granted with conditions …". Would this be better said as, "When a recommendation to grant is conditional …"?		
1300_14July_04	The statement in IAF-1300, Page 6, 1.4 Future Intent, lines 171-174 conflicts with the normative statement in IAF-1300, page 5, section 1.1, lines 128-133. All grey font text should be removed from IAF-1300.		