Identity Assurance Framework: Glossary

Version: 2.0

Date: 2010-04-24

Editor: Joni Brennan, IEEE-ISTO

Contributors:

The full list of contributors can be referenced here:
http://kantarainitiative.org/confluence/display/idassurance/IAF+2.0+Contributors

Abstract:

The Kantara Initiative Identity Assurance Work Group (IAWG) was formed to foster adoption of identity trust services. The primary deliverable of the IAWG is the Identity Assurance Framework (IAF), which is comprised of many different documents that detail the levels of assurance and the certification program that bring the Framework to the marketplace. The IAF is comprised of a set of documents that includes an Overview publication, the IAF Glossary, a summary Assurance Levels document, and an Assurance Assessment Scheme (AAS), which encompasses the associated assessment and certification program, as well as several subordinate documents, among them the Service Assessment Criteria (SAC), which establishes baseline criteria for general organizational conformity, identity proofing services, credential strength, and credential management services against which all CSPs will be evaluated. This document provides a Glossary of terms used throughout these documents.

Filename: **Kantara** IAF-1100-Glossary.doc

Notice:

55 ## Contents

56

59

60

1 INTRODUCTION

Kantara Initiative formed the Identity Assurance Work Group (IAWG) to foster adoption of consistently managed identity trust services. Utilizing initial contributions from the e-Authentication Partnership (EAP), the US E-Authentication Federation, and Liberty Alliance, the IAWG's objective is to create a Framework of baseline policy requirements (criteria) and rules against which identity trust services can be assessed and evaluated. The goal is to facilitate trusted identity federation and to promote uniformity and interoperability amongst identity service providers, with a specific focus on the level of trust, or assurance, associated with identity assertions. The primary deliverable of the IAWG is the Identity Assurance Framework (IAF).

The IAF leverages the EAP Trust Framework [EAPTrustFramework] and the US E-Authentication Federation Credential Assessment Framework ([CAF]) as baselines in forming the criteria for a harmonized, best-of-breed, industry-recognized identity assurance standard. The IAF is a Framework supporting mutual acceptance, validation, and life cycle maintenance across identity federations. The IAF is comprised of a set of documents which includes an Overview publication, the IAF Glossary, a summary Assurance Levels document, and an Assurance Assessment Scheme (AAS) document, which encompasses the associated assessment and certification program, in addition to several subordinant documents. The present document provides a Glossary of Terms used throughout the IAF documents.

2 IDENTITY ASSURANCE FRAMEWORK GLOSSARY

TERM	**DEFINITION**
AAS	See Assurance Assessment Scheme
Accreditation	The process used to achieve formal recognition that an organization has agreed to the operating rules defined in the AAS (Assurance Assessment Scheme) and is competent to perform assessments using the Service Assessment Criteria.
AL	See *Assurance Level*
Annual Conformity Review (ACR)	Review undertaken annually by the ARB (Assurance Review Board) of all Grantees as a positive check and reminder that their conformity to the appropriate agreement, and therefore the requirements of the AAS, remains their obligation.
Applicant	An individual or person acting as a proxy for a machine or corporate entity who is the subject of an identity proofing process.
Approval	The process by which the ARB accepts the compliance of a certified service and the CSP responsible for that service commits to upholding the Rules as defined in the AAS.
Approved encryption	Any cryptographic algorithm or method specified in a FIPS or a NIST recommendation or equivalent, as established by a recognized national technical authority. Refer to http://csrc.nist.gov/cryptval/.
Approved service	A certified service which has been granted an approval by the Kantara Initiative Board of Trustees.
Assertion	A statement from a verifier to a relying party that contains identity or other information about a subscriber.
Assessment	A process used to evaluate an electronic trust service and the service provider using the requirements specified by one or more Service Assessment Criteria for compliance with all applicable requirements.
Assessor	A person or corporate entity who performs an assessment.
Assurance Level (AL)	A degree of certainty that a claimant has presented a credential that refers to the claimant's identity. Each assurance level expresses a degree of confidence in the process used to establish the identity of the individual to whom the credential was issued and a degree of confidence that the individual who uses the

	credential is the individual to whom the credential was issued. The four assurance levels are: • Level 1: Little or no confidence in the asserted identity's validity • Level 2: Some confidence in the asserted identity's validity • Level 3: High confidence in the asserted identity's validity • Level 4: Very high confidence in the asserted identity's validity
Assurance Review Board (ARB)	The Assurance Review Board (ARB) is a sub-committee of the Board of Trustees, and is the operational authoritative body of the Kantara Identity Assurance Framework Assurance Assessment Scheme (AAS) certification program. It has delegated authority from the Kantara Initiative Board of Trustees (KIBoT) to undertake assessments of all types of applications for a Grant of Rights of Use of the Kantara Initiative Mark and shall make recommendations to the KIBoT for the award or denial of such Grants.
Assurance Assessment Scheme (AAS)	A program which defines the process for assessing the operating standards of certain players in the Identity and Credential Assurance Management space against strict criteria, and grants to candidates of the Scheme the right to use the Kantara Initiative Mark, a symbol of trustworthy identity and credential management services, at specified Assurance Levels.
Attack	An attempt to obtain a subscriber's token or to fool a verifier into believing that an unauthorized individual possesses a claimant's token.
Attribute	A property associated with an individual.
Audit Organization	An organization which undertakes assessments of entities and their services to establish their conformity to or compliance with specific standards or other widely-recognized criteria. Specifically, in the context of the AAS, entities providing credentialing or identity management services which are claiming conformance to the IAF.
(Accreditation) Applicant	An Audit Organization applying to Kantara Initiative for accreditation under the AAS.
Authentication	Authentication simply establishes identity, not what that identity is authorized to do or what access privileges he or she has.

Authentication protocol	A well-specified message exchange process that verifies possession of a token to remotely authenticate a claimant. Some authentication protocols also generate cryptographic keys that are used to protect an entire session, so that the data transferred in the session is cryptographically protected.
Authorization	Process of deciding what an individual ought to be allowed to do.
Bit	A binary digit: 0 or 1.
CAP	Credential Assessment Profile.
Certification	The ARB's affirmation that a particular credential service provider can provide a particular credential service at a particular assurance level based on a certification report from an accredited assessor.
Claimant	A party whose identity is to be verified.
Certification Body	An organization which has been deemed competent to perform assessments of a particular type. Such assessments may be formal evaluations or testing and be based upon some defined set of standards or other criteria.
Certified service	An electronic trust service which has been assessed by a Kantara-accredited assessor and found to be compliant with the applicable SACs.
Credential	An object to be verified when presented in an authentication transaction. A credential can be bound in some way to the individual to whom it was issued, or it can be a bearer credential. Electronic credentials are digital documents that bind an identity or an attribute to a subscriber's token.
Credential management	A service that supports the lifecycle of identity credentials from issuance to revocation, including renewal, status checks, and authentication services.
Credential service	A type of electronic trust service that supports the verification of identities (identity proofing), the issuance of identity related assertions/credentials/tokens, and the subsequent management of those credentials (for example, renewal, revocation, and the provision of related status and authentication services).
Credential Service Provider (CSP)	An electronic trust service provider that operates one or more credential services. A CSP can include a Registration Authority.
CSP	See *Credential Service Provider*.

Cryptographic token	A token for which the secret is a cryptographic key.
Electronic credentials	Digital documents used in authentication that bind an identity or an attribute to a subscriber's token.
Electronic Trust Service (ETS)	A service that enhances trust and confidence in electronic transactions, typically but not necessarily using cryptographic techniques or involving confidential material such as PINs and passwords.
Electronic Trust Service Provider (ETSP)	An entity that provides one or more electronic trust services.
ETS	See *Electronic Trust Service*.
ETSP	See *Electronic Trust Service Provider*.
Federal Information Processing Standards (FIPS)	Standards and guidelines issued by the National Institute of Standards and Technology (NIST) for use government-wide in the United States. NIST develops FIPS when the U.S. Federal government has compelling requirements, such as for security and interoperability, for which no industry standards or solutions are acceptable.
Federated identity management	A system that allows individuals to use the same user name, password, or other personal identification to sign on to the networks of more than one enterprise in order to conduct transactions.
Federation Operator	An individual or group that defines standards for its respective federation, or trust community and evaluates participation in the community or network to ensure compliance with policy, including the ability to request audits of participants for verification.
FIPS	See *Federal Information Processing Standards*.
Grant Category	One of the specific purposes for which the Kantara Initiative Mark may be used by a third party, being one of: Approved Service; Accredited Assessor; Service Approval Authority (future work focus); or Certified Federation Operator.
Grant (of Rights of Use)	The Granting, by the Kantara Initiative Board of Trustees (KIBoT) or another authoritative body to which the KIBoT has given a delegated authority (itself via a Grant), to use of the Kantara Initiative Mark for a specific Grant Category.
Grantee	An organization to which a Grant of Rights of Use of the Kantara

	Initiative Mark has been awarded.
IAWG	See *Identity Assurance Work Group*.
Identification	Process of using claimed or observed attributes of an individual to infer who the individual is.
Identifier	Something that points to an individual, such as a name, a serial number, or some other pointer to the party being identified.
Identity	A unique name for a single person. Because a person's legal name is not necessarily unique, identity must include enough additional information (for example, an address or some unique identifier such as an employee or account number) to make a unique name.
Identity Assurance Work Group (IAWG)	The multi-industry Kantara Initiative partnership working on enabling interoperability among public and private electronic identity authentication systems to foster the adoption of trusted on-line identity services.
Identity Assurance Framework (IAF)	The body of work that collectively defines the industry-led self-regulatory Framework for electronic trust services in the United States and around the globe, as operated by the Kantara Initiative. The Identity Assurance Framework includes documents which contain descriptions of criteria, rules, procedures, and processes.
Identity authentication	Process of establishing an understood level of confidence that an identifier refers to an identity. It may or may not be possible to link the authenticated identity to an individual.
Identity binding	The extent to which an electronic credential can be trusted to be a proxy for the entity named in it.
Identity Proofing	The process by which identity related information is validated so as to identify a person with a degree of uniqueness and certitude sufficient for the purposes for which that identity is to be used.
Identity Proofing policy	A set of rules that defines identity proofing requirements (required evidence, format, manner of presentation, validation), records actions required of the registrar, and describes any other salient aspects of the identity proofing function that are applicable to a particular community or class of applications with common security requirements. An identity proofing policy is designed to accomplish a stated assurance level.
Identity Proofing service provider	An electronic trust service provider which offers, as a standalone service, the specific electronic trust service of identity proofing. This service provider is sometimes referred to as a Registration

	Agent/Authority (RA).
Identity Proofing practice statement	A statement of the practices that an identity proofing service provider employs in providing its services in accordance with the applicable identity proofing policy.
Information Security Management Systems (ISMS)	A system of management concerned with information security. The key concept of ISMS is the design, implement, and maintain a coherent suite of processes and systems for effectively managing information security, thus ensuring the confidentiality, integrity, and availability of information assets and minimizing information security risks.
Issuer	Somebody or something that supplies or distributes something officially.
Kantara-approved assessor	A body that has been granted an accreditation to perform assessments against Service Assessment Criteria, at the specified assurance level(s).
Kantara-accredited service	A service which has applied for accreditation and completed a certified assessment at the specified assurance level(s).
Kantara Initiative Board of Trustees	The Kantara Initiative Board of Trustees (KIBoT) is comprised of trustee-level members of the Kantara Initiative, who have the responsibility of reviewing ARB recommendations and awarding the Kantara Initiative Mark to applying assessors and CSPs.
Kantara Initiative Mark	A symbol of trustworthy identity and credential management services at specified Assurance Levels, awarded by the Kantara Initiative Board of Trustees.
Kantara Trust Status List	Online record of Accredited Assessors and Certified Services, maintained on the Kantara Initiative website, listing organizations and services that have received the Kantara Initiative Mark and the associated assurance levels achieved.
Level of Assurance (LOA)	See *Assurance Level*.
Network	An open communications medium, typically the Internet, that is used to transport messages between the claimant and other parties.
OID	Object identifier.
Password	A shared secret character string used in authentication protocols. In many cases the claimant is expected to memorize the password.
Practice statement	A formal statement of the practices followed by an authentication

	entity (e.g., RP, CSP, or verifier) that typically defines the specific steps taken to register and verify identities, issue credentials, and authenticate claimants.
Public key	The public part of the asymmetric key pair that is typically used to verify signatures or encrypt data.
Public key infrastructure (PKI)	A set of technical and procedural measures used to manage public keys embedded in digital certificates. The keys in such certificates can be used to safeguard communication and data exchange over potentially unsecure networks.
Registration	An entry in a register, or somebody or something whose name or designation is entered in a register.
Relying Party (RP)	An entity that relies upon a subscriber's credentials, typically to process a transaction or grant access to information or a system.
Role	The usual or expected function of somebody or something, or the part somebody or something plays in a particular action or event.
SAC	See *Service Assessment Criteria*.
Security	A collection of safeguards that ensures the confidentiality of information, protects the integrity of information, ensures the availability of information, accounts for use of the system, and protects the system(s) and/or network(s) used to process the information.
Service Assessment Criteria (SAC)	A set of requirements levied upon specific organizational and other functions performed by electronic trust services and service providers. Services and service providers must comply with all applicable criteria to qualify for Kantara Initiative approval and earn the Kantara Initiative Mark.
Signatory	A party that opts into and agrees to be bound by the AAS-defined agreements according to the specified procedures.
Specified service	The electronic trust service which, for the purposes of an AAS assessment, is the subject of criteria set out in a particular SAC, or in an application for assessment, in a grant of an approval or other similar usage as may be found in various IAWG documentation.
Subject	An entity that is able to use an electronic trust service subject to agreement with an associated subscriber. A subject and a subscriber can be the same entity.
Subscriber	A party that has entered into an agreement to use an electronic trust service. A subscriber and a subject can be the same entity.

Threat	An adversary that is motivated and capable to violate the security of a target and has the capability to mount attacks that will exploit the target's vulnerabilities.
Token	Something that a claimant possesses and controls (typically a key or password) that is used to authenticate the claimant's identity.
Verification	Establishment of the truth or correctness of something by investigation of evidence.

84

85

Revision History

1. 8May2008 – Identity Assurance Framework Version 1.0 Initial Draft
    a. Released by Liberty Alliance
    b. Revision and scoping of Initial Draft release
2. 23JUNE 2008 – Identity Assurance Framework Version 1.1 Final Draft
    a. Released by Liberty Alliance
    b. Inclusion of comments to Final Draft
3. 1OCTOBER2009 – Identity Assurance Framework Version 1.1 Final Draft
    a. Documents contributed to Kantara Initiative by Liberty Alliance
4. XAPRIL2010 – Identity Assurance Framework Version 2.0
    a. Released by Kantara Initiative
    b. Significant scope build
    c. Original Identity Assurance Framework all inclusive document broken in to a set of documents with specific focus:
        i. Kantara IAF-1000-Overview
        ii. Kantara IAF-1100-Glossary
        iii. Kantara IAF-1200-Levels of Assurance
        iv. Kantara IAF-1300-Assurance Assessment Scheme
        v. Kantara IAF-1400-Service Assessment Criteria
        vi. Kantara IAF-1600-Assessor Qualifications and Requirements