Identity Assurance Framework: Assurance Levels

Version: draft 0.5

Date: 2009-12-31

Editor: Joni Brennan, IEEE-ISTO
Britta Glade

Contributors:

This document is a draft and not in final release form. The full list of contributors will be added prior to the final release of this document.

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 overviews the four Levels of Assurance, on which the IAF is based, as posited by the U.S. Federal Government and described in OMB M-04-04 [M-04-04] and NIST Special Publication 800-63 [NIST800-63]. These are further described in this document.

Filename: Kantara IAF-1200-Levels of Assurance.doc

Notice:

Implementation or use of certain elements of this document may require licenses under third party intellectual property rights, including without limitation, patent rights. The Participants of and any other contributors to the Specification are not and shall not be held responsible in any manner for identifying or failing to identify any or all such third party intellectual property rights. This Specification is provided "AS IS," and no Participant in Kantara Initiative makes any warranty of any kind, expressed or implied, including any implied warranties of merchantability, non-infringement of third party intellectual property rights, and fitness for a particular purpose. Implementers of this Specification are advised to review Kantara Initiative's website (http://www.kantarainitiative.org/) for information concerning any Necessary Claims Disclosure Notices that have been received by the Kantara Initiative Board of Trustees.

Contents

1 INTRODUCTION 4
2 ASSURANCE LEVELS 5
2.1 Assurance Level Policy Overview....................5
2.2 Description of the Four Assurance Levels....................6
2.2.1 Assurance Level 1 7
2.2.2 Assurance Level 2 7
2.2.3 Assurance Level 3 7
2.2.4 Assurance Level 4 7

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 policies requirements (criteria) and rules against which identity trust services can be assessed and evaluated. The goal is to facilitate trusted identity federation and to promote uniformity and interoperability amongst identity service providers, with a specific focus on the level of trust, or assurance, associated with identity assertions. The primary deliverable of IAWG is the Identity Assurance Framework (IAF).

The IAF 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. The present document presents an overview of the Assurance Levels.

2 ASSURANCE LEVELS

2.1 Assurance Level Policy Overview

Assurance Levels (ALs) are the levels of trust associated with a credential as measured by the associated technology, processes, and policy and practice statements controlling the operational environment. The IAF defers to the guidance provided by the U.S. National Institute of Standards and Technology (NIST) Special Publication 800-63 version 1.0.1 [NIST800-63] which outlines four levels of assurance, ranging in confidence level from low to very high. Use of ALs is determined by the level of confidence or trust (i.e. assurance) necessary to mitigate risk in the transaction.

An assurance level (AL) describes the degree to which a relying party in an electronic business transaction can be confident that the identity information being presented by a CSP actually represents the entity named in it and that it is the represented entity who is actually engaging in the electronic transaction. ALs are based on two factors:

- The extent to which the identity presented by a CSP in an identity assertion can be trusted to actually belong to the entity represented. This factor is generally established through the identity proofing process and identity information management practices.

- The extent to which the electronic credential presented to a CSP by an individual can be trusted to be a proxy for the entity named in it and not someone else (known as identity binding). This factor is directly related to the integrity and reliability of the technology associated with the credential itself, the processes by which the credential and its verification token are issued, managed, and verified, and the system and security measures followed by the credential service provider responsible for this service.

Managing risk in electronic transactions requires authentication and identity information management processes that provide an appropriate level of assurance of identity. Because different levels of risk are associated with different electronic transactions, IAWG has adopted a multi-level approach to ALs. Each level describes a different degree of certainty in the identity of the claimant.

The IAWG ALs enable subscribers and relying parties to select appropriate electronic identity trust services. IAWG uses the ALs to define the Service Assessment Criteria (SAC) to be applied to electronic identity trust service providers when they are demonstrating compliance through the Assurance Assessment Scheme (AAS) certification and assurance program. Relying parties (RPs) should use the assurance level descriptions to map risk and determine the type of credential issuance and authentication services they require. Credential service providers (CSPs) should use the levels to determine what types of credentialing electronic identity trust services they are capable of providing currently and/or aspire to provide in future service offerings.

2.2 Description of the Four Assurance Levels

The four ALs describe the degree of certainty associated with an identity assertion. The levels are identified by both a number and a text label. The levels are defined as shown in Table 2-1:

Table 2-1. Four Assurance Levels

Level	Description
1	Little or no confidence in the asserted identity's validity
2	Some confidence in the asserted identity's validity
3	High confidence in the asserted identity's validity
4	Very high confidence in the asserted identity's validity

The choice of AL is based on the degree of certainty of identity required to mitigate risk mapped to the level of assurance provided by the credentialing process. The degree of assurance required is determined by the relying party through risk assessment processes covering the electronic transaction system. By mapping impact levels to ALs, relying parties can then determine what level of assurance they require. Further information on assessing impact levels is provided in Table 2-2:

Table 2-2 Potential Impact at Each Assurance Level

Potential Impact of Authentication Errors	**Assurance Level***			
	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 govt. agency 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	Sub High
Civil or criminal violations	N/A	Min	Sub	High

**Min=Minimum; Mod=Moderate; Sub=Substantial; High=High*

The level of assurance provided is measured by the strength and rigor of the identity proofing process, the credential's strength, and the management processes the service provider applies to it. The IAWG has established service assessment criteria at each AL for electronic trust services providing credential management services. These criteria are described in the Service Assessment Criteria document.

CSPs can determine the AL at which their services might qualify by evaluating their overall business processes and technical mechanisms against the Service Assessment Criteria. The service assessment criteria within each AL are the basis for assessing and approving electronic trust services.

2.2.1 Assurance Level 1

At AL1, there is minimal confidence in the asserted identity. Use of this level is appropriate when no negative consequences result from erroneous authentication and the authentication mechanism used provides some assurance. A wide range of available technologies and any of the token methods associated with higher ALs, including PINS, can satisfy the authentication requirement. This level does not require use of cryptographic methods.

The electronic submission of forms by individuals can be Level 1 transactions when all information flows to the organization from the individual, there is no release of information in return and the criteria for higher assurance levels are not triggered.

2.2.2 Assurance Level 2

At AL2, there is confidence that an asserted identity is accurate. Moderate risk is associated with erroneous authentication. Single-factor remote network authentication is appropriate. Successful authentication requires that the claimant prove control of the token through a secure authentication protocol. Eavesdropper, replay, and online guessing attacks are prevented. Identity proofing requirements are more stringent than those for AL1 and the authentication mechanisms must be more secure, as well.

2.2.3 Assurance Level 3

AL3 is appropriate for transactions requiring high confidence in an asserted identity. Substantial risk is associated with erroneous authentication. This level requires multi-factor remote network authentication. Identity proofing procedures require verification of identifying materials and information. Authentication must be based on proof of possession of a key or password through a cryptographic protocol. Tokens can be “soft,” “hard,” or “one-time password” device tokens. Note that both identity proofing and authentication mechanism requirements are more substantial.

2.2.4 Assurance Level 4

AL4 is appropriate for transactions requiring very high confidence in an asserted identity. This level provides the best practical remote-network authentication assurance, based on proof of possession of a key through a cryptographic protocol. Level 4 is similar to Level 3 except that only “hard” cryptographic tokens are allowed. High levels of cryptographic assurance are required for all elements of credential and token management. All sensitive data transfers are cryptographically authenticated using keys bound to the authentication process.

2.2.5 Identity Assurance Levels Illustrated

A summary chart with the levels of assurance, examples, and assessment criteria, is below in Table 2-3. Table 2-3 serves the purpose of purely to illustrating the Assurance Levels and should be considered example only. In all instances determination of the Assurance Levels must be made by the application owner. Additionally, it is worth noting that previous versions of this document included specific scenario examples, however feedback indicates that the generic table 2-3 shall adequately serve to illustrate the Assurance Levels.

Table 2-3 Identity Assurance Levels Illustrated

Assurance Level	Example	Assessment Criteria – Organization	Assessment Criteria – Identity Proofing	Assessment Criteria – Credential Management
AL 1	Registration to a news website	Minimal Organizational criteria	Minimal criteria - Self assertion	PIN and Password
AL 2	Change of address of record by beneficiary	Moderate organizational criteria	Moderate criteria - Attestation of Govt. ID	Single factor; Prove control of token through authentication protocol
AL 3	Access to an online brokerage account	Stringent organizational criteria	Stringent criteria – stronger attestation and verification of records	Multi-factor auth; Cryptographic protocol; "soft", "hard", or "OTP" tokens
AL 4	Dispensation of a controlled drug or $1mm	Stringent organizational criteria	More stringent criteria – stronger attestation and verification	Multi-factor auth w/hard tokens only; crypto protocol w/keys bound to auth process