Identity Assurance Framework: Overview

Version: . **2.0**

Date: 2010-04-08

Editor: Colin Soutar, CSC on behalf IAWG

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 comprises several documents that detail the levels of assurance, and the certification program that bring the Framework to the marketplace. The IAF comprises primary documents such as this 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 two secondary documents: 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; and the Assessor Qualifications and Requirements which provides an

overview of the requirements which applicant assessors must fulfill in order to become Kantara-Accredited Assessors.

This present document provides an overview of the IAF documents and program.

Filename: Kantara IAF-1000-Overview.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

This document relates to the Kantara Initiative Identity Assurance Framework [IAF] which has been developed within the Kantara Initiative Work Group (IAWG) and corresponding public special interest groups with input from members of the global financial services, government, healthcare, IT, and telecommunications sectors.

This document is intended to enable non-IAWG participants to understand and familiarize themselves with the IAF and thus be a starting point for industry professionals who want to learn more and possibly conform to the IAF.

1.1 Intended Audience

The intended audience for this document encompasses users of electronic identity credentials, entities that rely upon these electronic credentials, credential service providers who issue these electronic credentials, and assessors who review the business processes of credential service providers. This audience typically includes managers and decision makers responsible for developing strategies for managing access to online resources based on trustworthy identification of potential users, as well as providers of trustworthy online identity credentials.

Other audiences might include potential subjects of online identity services and IT auditors who may be asked to evaluate online identity service providers.

The reader should have a basic understanding of technical and practical issues regarding identity and online identity credentials as discussed in such forums, documents, and specifications as the EAP Trust Framework ([EAPTrustFramework]), the US E-Authentication Federation Credential Assessment Framework ([CAF]), and the [CABForum].

1.2 Overview

In order to conduct any sort of business in an online world, entities (which include people, organizations, applications, machines, etc.) need to be able to identify themselves remotely and reliably. However, in most cases, it is not sufficient for the typical electronic credential (usually a basic userID/password pair or a digital certificate) to simply make the assertion that “I am who I say I am ... believe me.” A relying party needs to be able to know to some degree that the presented electronic identity credential truly represents the individual referred to in the credential. In the case of self-issued credentials, this is generally difficult. However, most electronic identity credentials are issued by Credential Service Providers (CSPs), often referred to as identity providers (IdPs): your workplace network administrator, your social networking service or online game administrator, a government entity, or a trusted third party. You may have multiple credentials from multiple providers ... most people do.

There are four main roles involved in making this online exchange trustworthy:

1. Entities who are the subjects of identity credentials issued by a CSP, variously referred to as “subjects” or “credential holders”;
2. CSPs who are providers of identity services and issuers of electronic identity credentials;
3. Auditors or assessors who review the business processes and operating procedures that CSPs follow; and
4. Entities that rely upon the credentials issued by CSPs, referred to as “relying parties (RPs).”

Different CSPs follow different policies, rules, and procedures for issuing electronic identity credentials. In the business world, the more trustworthy the credential, the more stringent are the rules governing identity proofing, credential management, and the kinds of credentials issued. But while different CSPs follow their own rules, more and more end users (i.e., subjects) and relying parties (e.g., online services) wish to trust existing credentials and not issue yet another set of credentials for use to access one service. This is where the concept of identity federation becomes important. Federated identity provides CSPs, subjects, and relying parties with a common set of identity trust conventions that transcend individual identity service providers, users, or networks, so that a relying party will know it can trust a credential issued by CSP-1 at a level of assurance comparable to a common standard, which will also be agreed upon by CSP-2, CSP-3, and CSP-4. In this context, an assurance level describes the degree to which a relying party in an electronic exchange can, after performing certain tests to authenticate (validate) the origin of the exchange, be confident that the identity information being presented by a CSP actually represents the entity referred to in it and that it is the represented entity which is actually engaging in the exchange.

Identity federation offers many advantages to organizations, including recognized cost and time savings, ability to assure and monitor privacy and security, auditability to meet increasing global compliance demands, and the ability to minimize use and retention of personally identifiable information (PII). The opportunity, and its potential benefits, have been well-documented by early federated identity deployers and users, who recognized identity federation as a logical approach that unlocks a myriad of electronic business and online interactive opportunities which appeal to the end user’s need for simplicity and high level of service.

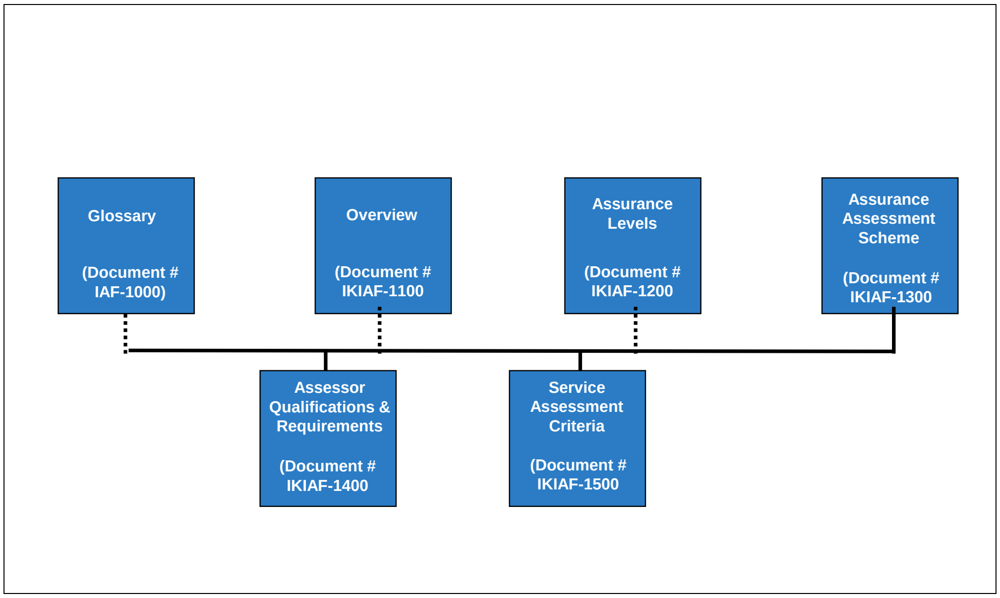
The IAF provides a means to enable relying parties to understand the trustworthiness of electronic identity credentials by other parties at commonly agreed levels of assurance. The IAF specifies the verification and proofing checks that CSPs carry out on entities, the way that CSPs run their services, and how the CSPs, themselves, are assessed by accredited assessors to verify they are operating their services in conformance with their proclaimed level(s) of assurance and the stated terms of service.

The IAF is designed to be generic and thereby commensurate with a wide array of programs spanning the adopted four Assurance Levels, ranging from: open government programs operating at lower or medium assurance levels; to medium to high assurance applications such as access to patient electronic health records; to very-high assurance programs for defence, such as the Transglobal Secure Collaboration Program, where additional specificity may be provided by the Program, depending on particular business rules and process.

2 UNDERSTANDING THE KANTARA INITIATIVE IDENTITY ASSURANCE FRAMEWORK

The [IAF] is a standardized approach that defines processes and procedures for CSPs, relying parties, and operators of federated identity networks (Federation Operators) to trust each other's credentials at known levels of assurance. The main components of the IAF are:

1. Assurance Levels;
2. Glossary;
3. Assurance Assessment Scheme (AAS);
4. Service Assessment Criteria, and;
5. Assessor Qualifications and Requirements.
6. Associated Profiles



2.1 Assurance Level Criteria

Assurance levels are the levels of trust associated with a credential as measured by the associated technology, processes, and policy and practice statements. The IAF defers to the guidance provided by the U.S. National Institute of Standards and Technology (NIST) Special Publication 800-63 version 1.0.2 [NIST800-63] which outlines four levels of assurance, ranging in confidence level from low to very high. The level of assurance provided is measured by the strength and rigor of the identity verification and proofing process, the credential's strength, and the management processes the CSP applies to it. The IAF then goes on to describe the service assessment criteria at each assurance level.

On the relying party side, these same four assurance levels address increasing levels of risk. For each Assurance Level, the IAF defines commensurate risk mitigation measures appropriate for the level of trust that may be assumed in the identity credentials. These four levels have been adopted by the U.K. government, the Government of Canada, and the U.S. Federal Government for categorizing required electronic identity trust levels for providing electronic government services.

A summary of the IAF's approach to assurance levels is provided in the Assurance Level document.

2.2 Glossary

The Glossary document of the IAF provides a brief summary of commonly used terms that are used across IAF documents. It presents readers with a baseline understanding of how terms are used to enable better understanding of the programs and processes being discussed. As terms and usage can vary from industry to industry, it is recommended reading for anyone wanting a strong baseline understanding of the Identity Assurance Framework.

2.3 Assurance Assessment Scheme

The Assurance Assessment Scheme (AAS) portion of the IAF defines the phased approach used to establish criteria for certification and accreditation, initially focusing on CSPs and the accreditation of the assessors who will certify and evaluate them. The goal of this phased approach is to provide, initially, federations and Federation Operators with the means to certify their members for the benefit of inter-federation and to streamline the certification process for the industry. It is anticipated that follow-on phases will target the development of criteria for certification of federations, themselves, as well as best practices guidelines for relying parties.

The AAS establishes the requirements that assessors must have in order to perform assessments or audits, thus earning the associated Kantara Initiative Mark. It also defines the rules and requirements they will use when performing the actual assessments on CSPs vying to earn the associated Kantara Initiative Mark(s) for Kantara Initiative accreditation.

2.4 Service Assessment Criteria

The Service Assessment Criteria (SAC) document establishes baseline criteria for organizational conformity, identity-proofing services, credential strength, and credential management services against which all CSPs will be evaluated. The IAF also establishes a protocol for publishing updates, as needed, to account for technological advances and preferred practice and policy updates.

These criteria set out the requirements that identity services and their CSPs must meet at each assurance level within the IAF in order to receive Kantara Initiative accreditation.

CSPs can determine the assurance levels 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 assurance level are the basis for assessing and approving electronic trust services.

Note that the Service Assessment Criteria defines Common Organization Criteria (CO-SAC) that must be conformed to by a CSP, as well as Credential Management (CM-SAC) and ID Proofing Criteria (ID-SAC). A CSP must demonstrate conformity to the CO-SAC and at least one of the CM-SAC and ID-SAC to attain the Kantara recognition mark.

2.5 Assessor Qualifications and Requirements

The Assessor Qualifications and Requirements document outlines the requirements which applicant assessors must fulfill in order to become Kantara-Accredited Assessors. These requirements will be used to validate applicants' suitability by the Assessment Review Board (ARB), according to the processes described in the Assurance Assessment Scheme.

2.6 Associated Profiles

In addition to the generic IAF documents described above, particular implementation of the IAF may require ancillary specifications, relating to, for example, jurisdictional privacy principles or operational conditions. These ancillary specifications will be defined in IAF Profiles, and will be associated with the IAF certification process for that particular implementation.

3 REFERENCES

3.1 Informative

[CABForum] See the CA/Browser Forum website at http://www.cabforum.org/

[CAF] Louden, Chris; Spencer, Judy; Burr, Bill; Hawkins, Kevin; Temoshok, David; Cornell, John; Wilsher, Richard G.; Timchak, Steve; Sill, Stephen; Silver, Dave; Harrison, Von; eds., "E-Authentication Credential Assessment Framework (CAF)," E-Authentication Initiative, Version 2.0.0 (March 16, 2005). http://www.cio.gov/eauthentication/documents/CAF.pdf

[EAPTrustFramework] "Electronic Authentication Partnership Trust Framework" Electronic Authentication Partnership, Version 1.0. (January 6, 2005) http://eap.projectliberty.org/docs/Trust_Framework_010605_final.pdf

[IAF] Cutler, Russ, eds. "Liberty Identity Assurance Framework," Version 1.1, Liberty Alliance Project (21 June, 2008). http://www.projectliberty.org/liberty/content/download/4315/28869/file/liberty-identity-assurance-framework-v1.1.pdf

[NIST800-63] Burr, William E., Dodson, Donna F., Polk, W. Timothy, eds., "Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology," Version 1.0.2, National Institute of Standards and Technology, (April, 2006). http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

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