Liberty Identity Assurance Framework – Read Me First

Version: 1.0

Editor:

Peter Alterman, Federal PKI Policy Authority
Joan Brennan, IEEE-ISTO
James A. Gross, Wells Fargo
Rob Lockhart, IEEE-ISTO
Richard Trevorah, tScheme Limited
Frank Villavicencio, Citi

Contributors:

Bob Pinheiro, Robert Pinheiro Consulting LLC
David Wasley, Int2
Richard Wilsher, The Zygma Partnership
Stephen P. Sill, General Services Administration

Abstract:

This document relates to the Liberty Identity Assurance Framework [IAF] which has been developed within the Liberty Alliance Identity Assurance Expert Group (IAEG) 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-IAEG members 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.

Filename: liberty-identity-assurance-framework_-_read-me-first-v1.0.pdf

Notice:

Liberty Alliance Project
Licensing Administrator
c/o IEEE-ISTO
445 Hoes Lane
Piscataway, NJ 08855-1331, USA
info@projectliberty.org

Contents

1 Introduction

This document relates to the Liberty Identity Assurance Framework [IAF] which has been developed within the Liberty Alliance Identity Assurance Expert Group (IAEG) 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-IAEG members 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.”

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 to verify they are operating their services in conformance with their proclaimed level(s) of assurance and the stated terms of service.

2 Understanding The Liberty 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 Level Criteria;
2. Service and Credential Assessment Criteria;
3. Accreditation and Certification Model, and;
4. Associated Business Rules.

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 (4) 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.

2.2 Service and Credential Assessment Criteria

The Service and Credential Assessment Criteria section in the IAF 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 Liberty 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.

2.3 Accreditation and Certification Model

The [IAF] uses a phased approach to establish criteria for certification and accreditation, initially focusing on CSPs and the accreditation of those who will assess 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 IAF establishes the requirements that assessors must have in order to perform assessments or audits for Liberty accreditation and defines the rules and requirements for the actual assessments.

2.4 Associated Business Rules

Signatories to these business rules agree that they govern the issuance, use, and validation of credentials issued by IAEG-certified CSPs, the certification of such CSPs, and the accreditation of those who assess CSPs. The Business Rules section of the IAF identifies: how CSPs and relying parties can participate in or be bound by the rules; what the roles and obligations are of the various parties to the rules, i.e., the IAEG, CSPs, relying parties, and assessors; the means of enforcement of and recourse under the rules; and, the general terms of the rules (including Governing Law, severability etc.).

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