Federation Operator Guidelines

Version:	**1.0**
Date:	2011-01-30
Editor:	Rich Furr, David Wasley

Contributors:

The full list of contributors can be referenced here:
http://kantarainitiative.org/confluence/x/2wC-Ag

Status: This document is a **Kantara Initiative Recommendation**, created by the IAWG WG (see section 3.8 of the Kantara Initiative Operating Procedures)

Abstract:

The Kantara Initiative Identity Assurance Work Group (IAWG), formed to foster adoption of identity trust services, is developing guidelines and supporting materials for all aspects of federated identity implementation among credential service providers (CSPs) and relying parties (RPs). This document provides guidelines for an Identity Federation, an entity that defines and oversees an organization, which is a collective of cooperating CSPs and RPs. The Federation, typically a legal entity, serves the needs of its participants by establishing standards for a CSP's identity management and a RP's use of identity information it receives. It also serves as an arbiter of compliance with these standards in order that any participant may trust that other participants are complying with Federation standards and rules. A critical component of a Federation is the Federation Operator which manages the services offered by the Federation including

entering into contracts with CSPs, RPs, and vendors, operating a service infrastructure supporting real-time transactions with participants, oversees compliance audits of Federation participants, and maintains records, documents and other resources of the Federation.

Filename: Kantara Initiative_IAWG_FOG_Draft-Recommendation_v1.0.pdf

NOTICE

This document has been prepared by Sponsors of the Kantara Initiative. Permission is hereby granted to use the document solely for the purpose of implementing the Guidelines. No rights are granted to prepare derivative works of these Guidelines. Entities seeking permission to reproduce portions of this document for other uses must contact the Kantara Imitative to determine whether an appropriate license for such use is available.

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

Table of Contents

1 BACKGROUND AND CONTEXT

Trustworthy on-line identity service providers are increasingly accepted by on-line relying parties to provide basic identity and, in some cases, additional relevant information about potential users of their services. With this growth comes the problem of scaling trust models. Individual bi-lateral agreements between identity service providers and relying parties are the conventional way of establishing trust. When there are many hundreds of identity service providers and many thousands of relying parties, a trust broker model becomes more practical.

An identity service provider (IdP)[1] bases identity assertions on the binding of identity information to a physical person and the use of reliable on-line credentials to recognize its identity Subjects. Relying parties (RPs) use that identity information to make an access control decision when the identity Subject wishes to use its services.

An identity federation, for the purposes of this document, is a set of identity service providers and relying parties (a.k.a. on-line service providers) that agree to operate under compatible policies, standards, and technologies in order that end-user identity information provided by IdPs can be understood and trusted by RPs. Such a federation could be an informal collective of entities that have other reasons to trust each other, e.g. a university with multiple campuses or a corporation with multiple subordinate units. However, in general such a federation will include otherwise unaffiliated members and thus will require some sort of trust model and governance framework. Typically governance will involve a federation governing body (FGB) that approves policy, standards and membership requirements on behalf of the member community. If the federation trust model requires that the federation be able to enter into contracts and accept liability for its actions then it should be under the aegis of a legal entity.

The scope of this document does not include requirements on identity Subjects or sources of authority (SOA) for identity attributes. Such requirements may be added at a later time. In general, the federation can place requirements only on entities that are members of the federation.

There are different forms of identity federation, often based on what underlying technology used. ISO x.509 Public Key Infrastructure (PKI) is a very formal, highly structured model for establishing trust between a Certification Authority (CA) and a RP such that the RP will accept and use the content of a PKI certificate to identify a potential user. In that model, trust derives from a primary certification authority (CA) that is recognized by RPs and referred to as the PKI trust anchor (TA). The TA is responsible for ensuring the trustworthiness of all subordinate CAs, i.e., members of the PKI federation. An identity federation based on other technologies must also provide for the

[1] Some federations prefer the term “credential service provider” (CSP). We use the term IdP here to emphasize the broader sense of “identity” that can be asserted to a relying party.

functional role of a “trust anchor” similar to that described in the ISO x.509 PKI framework. The guidelines provided herein are intended to describe principles; how they are implemented in a particular federation may vary.

Whereas a small identity federation might rely on bilateral agreements among members, a large and scalable federation must rely on a support organization that can coordinate essential activities and provide essential services to all members of the federation. These guidelines refer to such an organization as the “Federation Operator” (FO). The FO may be subordinate to the FGB or the two may be one and the same.

The Kantara Initiative formed the Identity Assurance Working Group (IAWG) to foster adoption of consistently managed identity services. The goal is to facilitate trusted identity federation and to promote compatibility and interoperability amongst identity service providers, with a specific focus on the level of trust, or assurance, associated with identity assertions. This document is one product of the IAWG but its principles should apply equally well to identity federations other than that operated by Kantara.

2 FEDERATIONS AND FEDERATION OPERATORS

In this document, the term “Federation” refers to the overall membership, governing body and operational entity(s) that together define, create and support the trust framework upon which federation members rely. Critical elements of the Federation’s role include:

- defining or identifying standards which must be met by all members. These include;
  - policy and operational standards for how identity credentials are issued and managed;
  - standards for the semantics and syntax of information to be exchanged;
  - technology standards for credentials and information exchange;
  - policy standards for how Subject privacy is preserved and how Subject identity information is protected and used;
- entering into interfederation agreements with other Federations which might also require evaluation of comparative policies, translation of semantics or syntax, etc.;

The Federation Operator supports the day-to-day functioning of the Federation. The FO’s roles may include:

- supporting a mechanism whereby Federation member IdPs and RPs can be certain they are interacting with another Federation member;
- ensuring members are certified for compliance or compatibility with Federation standards and providing metadata or other means for reliably conveying the certifications that have been issued to each federation member;
- as necessary, collecting and making available metadata describing members’ infrastructure entities;
- aiding in problem resolution and/or technology compliance testing with or among members;
- enter into contracts for services available to community members;
- serving as the Point of Contact (POC) for concerns or complaints about improper conduct or failure to comply with standards on the part of a federation member;
- other activities or services in support of its community.

In order that the Federation may perform all these roles effectively, it should be a legal entity with resources, staffing and governance that is able to enter into binding contracts and maintain liability for its actions.

These Guidelines are intended to help potential Federations develop a business model and operational plan so that interoperability among Federations might be more readily achieved. These Guidelines are a deliverable of the IAWG.

Most of the principles may be applied regardless of the actual level(s) of assurance which are operational within the Federation. The Kantara Identity Assurance Working Group has developed the Identity Assurance Framework Assurance Levels and the Identity Assurance Framework Service Assessment Criteria which provide a baseline which Federation Operators should use in establishing their internal policies, processes and procedures. Implementation of these policies and procedures should be assessed against the Liberty Alliance/Kantara Service Assessment criteria.

3 BUSINESS PRATICE DOCUMENTATION

The Federation governing body should develop minimum essential documents needed to provide structure, governance and management for the Federation. With guidance from the FGB, the FO should develop and fully document Operating Policies, Processes and Guidelines as guidance and requirements to be met to maintain membership or affiliation with the Federation. Additional documents may be included depending on the needs of the Federation or its members.

Each Federation governing body and/or Federation Operator should:

- Develop an Operating Policy which should
    - define the classes of entities that may participate in the Federation, e.g., voting or non-voting Members, Identity Providers, Service Providers, Subscribers, etc., and their roles in the Federation;
    - include the operational rights and responsibilities of the Federation Members;
    - define the governance principles and structure of the Federation;
    - define a process by which security incidents are handled within the Federation;
    - define expectations for notification to other members and revocation of a member's standing if that member is found to be out of compliance;
    - consider whether “performance guarantees” for the operation and maintenance of FO functions are important and, if so, document what the intended target values are.
- Define and make available to Federation members the policies and procedures under which the Federation Operator must operate and require periodic independent audits of the FO to ensure compliance. These should address
    - procedures for vetting and incorporating new members including records management;
    - personnel requirements for positions in which sensitive information or procedures are handled;
    - infrastructure requirements to ensure security, reliability and robustness;
    - disaster response and recovery;
- Establish the liability structure and provisions under which the Federation should operate.
- Develop a set of documents which specify requirements and/or provide guidance to the various Members regarding the technical, procedural and process related

requirements they must meet to become and remain participating entities in the Federation. These documents should include as a minimum:

- Policy and procedural document(s) which define:
    - the processes used to verify the identity information that will be asserted on behalf of Subscribers;
    - the method and phases of management of the life cycle of the identity credential and any tokens which may be used to host or protect such credentials;
    - the process to resolve any disputes among members of the Federation;
- General security requirements around the sensitivity of relying party applications to include handling of personally identifying information (PII);
- Functional specifications defining the required functionality provided by the Federation and its members, including with respect to enhancements, version upgrades and interoperability;
- Technical specifications that clearly identify and cite:
    - any existing standards, defining the data and attributes included in any identity credentials and the structure of said credentials;
    - the structure and operating requirements of any system used to generate and manage the life cycle of identity credentials;
    - the structure and operations of any tokens used to host and protect identity credentials;
- policies and procedures under which the compliance of Federation members with the policies, processes and specifications of the Federation is assessed and controlled;
- Consider as necessary any requirements for security and software maintenance of service platforms, installation of functional software upgrades, or any other issues that could affect interoperability or trustworthiness of the federation.

- Develop the process by which disputes among and/or between the Members should be resolved.
- Create a set of legal agreements/contracts which bind the Members to the Federation Operating Policies and other governing and management documents.

- Define policies and procedures for certifying, suspending, restoring, revoking, upgrading or downgrading, and terminating a trusted IDP.

3.1 Application Approval

The Federation should have established procedures in place to define and manage the application for membership process. This process should include vetting the *bona fides* of the organization and identifying the proper responsible parties for administrative and operational contacts.

4 ESTABLISHING A NETWORK OF TRUST

Federations can augment or form the basis for trusted identity credentials among its members. Much like the Trust Anchor in a traditional PKI hierarchy, the FGB and FO play critical roles in establishing standards for needed levels of assurance and trustworthiness in credentials and identity assertions. The federation may also wish to establish requirements for how relying parties use and protect identity information they receive in order that IDPs are comfortable providing that information. The FO is responsible for verifying continuing compliance with these standards and rules. Important aspects of this "network of trust" are described below.

4.1 Identity Assurance Policy and Requirements

A fundamental role of the federation is to articulate a framework and set of technical, operational, and policy requirements for its members that establish the basis for trust. For IDPs, this should include identity proofing and credential issuance, credential strength[2] and management, and secure storage and communication of authentication secrets and other sensitive information. Credential strength is a function of credential technology and parameters and should be commensurate with the level of assurance that the IDP asserts, if any. For all parties, it should ensure proper handling of sensitive or confidential information and respect for the privacy of identity Subject information and activities.

4.2 Policy Mapping

Where Members already have established identity management policies, it might be necessary to create a mapping between those policies and the community standard policies. The FO would be responsible for ensuring that this mapping occurs in a reliable and trustworthy process in cooperation with the potential Member. The Federation governing body should approve the results of any such mapping.

If the Federation wishes to be accredited by Kantara, its policies, processes, procedures and technical specifications must be mapped to the requirements defined in the Kantara Service Assessment Criteria for the requisite levels of assurance. Where there may be variance, these must be resolved prior to Kantara accreditation of the Federation.

4.3 Compliance and Audit Review

Audits are the conventional way that a relying party can determine whether it is willing to trust another otherwise unrelated party. The type and scope of an audit may vary as long as it is deemed sufficient. The Federation may wish to establish specific rules about how audits are to be performed both for its members and for its FO.

[2] For example, as defined in [4] or its equivalent.

Typically the FO should undergo audits at defined intervals against its stated policies and procedures in order to assure its Federation Members that it is acting appropriately as the community trust anchor. Federations that certify high assurance IDPs should consider active penetration and integrity testing by a third party as well.

For Kantara accreditation, the Federation must provide the Kantara Management Board an initial certified assessment of its compliance with the provisions of the Kantara Identify Assurance Framework when it applies for certification. Certified Federations will be required to submit follow-up assessments at defined intervals to ensure continued compliance.

Federation Operators should require similar assessments of Federation Members at defined intervals. These assessments would be conducted against the policies, processes and specifications of the Federation or against the mapped policies as defined above.

4.4 Technical Interoperability and Testing

All authentication mechanisms and protocols used within a Federation should be tested to ensure they interoperate properly among Members of the Federation. Where protocols that are used to convey identity information and assurance levels are critical to proper operation of the federation, the FO should define how these protocols can be tested for interoperability, including tests for Relying Party (RP) response to flawed IDP protocol implementation and vice versa. If Federation Member metadata is distributed and installed dynamically, protocols for accomplishing such distribution and rejecting flawed metadata should be tested.

5 NEGOTIATION OF AGREEMENTS

Agreements of Membership should be in place between the Federation and its Members. To the maximum extent possible these should be standardized to ensure all Members are subject to a standard set of rights and responsibilities. These agreements form the basis on which Members can trust each other so essential elements of the Federation trust framework must be consistent across all Members of the Federation.

6 SUMMARY

Identity federations represent communities of interest and promote trust and interoperability among on-line identity service providers and on-line relying parties. The Federation governing body and Federation Operator form the equivalent of a PKI Trust Anchor for the community. This critical role is established through policies and procedures developed in cooperation with the community and verified by qualified independent assessors.

Interoperation of trust and identity credentials between established federations can expand the "web of trust" in important ways, benefiting both federations and identity Subjects. In this way, scalable, trustworthy and secure transactions can be made easier and more flexible for both end-users and relying parties.

7 ACRONYMS

CSP	Credential Service Provider
eID	electronic Identity
FBCA	Federal Bridge Certification Authority
FGB	Federation governing body
FIPS	Federal Information Processing Standard
FO	Federation Operator
HSPD	Homeland Security Policy Directive
IAWG	Identity Assurance Working Group
IDABC	Interoperable Delivery of European eGovernment Services to public Administrations, Business and Citizens
IdM	Identity Management
IdP	Identity Provider
NIH	National Institutes of Health
NIST	National Institute for Science and Technology
OMB	Office of Management and Budget
OTP	One-time use Password
PEGS	Pan-European eGovernment Services
PII	Personally Identifing Information
PKI	Public Key Infrastructure
POC	Point of Contact
RP	Relying Party
SAFE	Secure Access for Everyone (now Signatures and Authentication for Everyone)

8 DEFINITIONS

[Ed. Note: this should be incorporated into the Kantara IAF 1100 Glossary Document http://kantarainitiative.org/confluence/x/e4R7Ag]

Term	Definition
Assessor/Auditor	Provides oversight / ensures compliance
Approved Encryption Method	An algorithm or technique that is either 1) specified in a globally recognized Government Agency Recommendation, or 2) adopted in a globally recognized government Agency Recommendation.
Assurance level	In the context of this document, describes the degree to which a relying party in an electronic business transaction can be confident that the identity information being presented by a IDP actually represents the entity named in it and that it is the represented entity who is actually engaging in the electronic transaction.
Credential	A piece of information attesting to the integrity of certain stated facts[3].
Credential Service Provider	An electronic trust service provider that operates one or more credential services. A CSP can include a Registration Authority. A CSP has limited knowledge of a Subject's broader identity.
Federation	Any alliance or association of organizations which have freely joined together for a common purpose
Federation governing body	Identity federations can take many different forms but all must have some entity that approves policies and standards for the federation. This could be a representative body elected by the membership or any other type of entity that the membership will accept for this purpose.
Federation Operator	An organization that provides day-to-day operational support and management of the federation. The Federation Operator typically is authorized to enter into binding contracts and agreements and to provide support for federation services. The Federation Operator typically reports to the Federation governing body and is recognized by federation members as having certain roles and authority in creating a framework in which on-line identity assertions can be trusted and the privacy of identity information protected[4].
Federation Member	An otherwise independent entity that enters into a contract or

[3] IDABC, eID Interoperability for PEGS, Common specifications for eID interoperability in the eGovernment context, December 2007

[4] InCommon-NIH Interfederation Memorandum of Agreement

	binding agreement with the Federation Operator in order to receive services from the federation.[2] A Member typically will have a role in governance of the federation.
Federation Participant	Similar to Federation Member but may or may not have a role in governance of the Federation.
Identity Management (IdM)	The combination of technical systems, rules, and procedures that define the owner-ship, utilization, and safeguarding of personal identity information. The primary goal of the IdM process is to assign attributes to a digital identity and to connect that identity to an individual incompliance with the Federation Operator's framework.
Identity Provider (IdP)	An entity which provides Subject identities to Relying Parties. There can be various kinds of authentication methods supported by the IdP (e.g. username/password, X.509, OTP…); entities which are capable of creating identities and distributing them to other applications; an entity that manages identity information on behalf of Subjects and provides assertions of Subject identity information to other providers.
Personally Identifiable Information	Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc., either alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.
Registration Authority	A functional entity that accepts requests for registration with the IDP, does identity proofing as required, and creates a record for the Subject in the IDP's identity management system.
Relying Parties	Entities that rely upon an assertion of identity from a IDP. Typically this is used to grant access to on-line services or data on the basis of a valid credential[2]
Resource Provider	A Relying Party which provides systems, applications and infrastructures which leverage the identities provided by a IDP for purposes of granting access to on-line information or data on the basis of the presentation of a valid credential.
Service Assessment Criteria	The Liberty Alliance/Kantara document that provides a framework of baseline policies, requirements (criteria) and rules against which identity trust services can be assessed and evaluated.
Service Provider	A Relying Party to which a Subscriber authenticates using their credential in order to gain access to on-line applications or

	services.[1]
Subscriber	An individual who is the Subject named or identified in a verified identity credential issued to that User[5]

345

[5] SAFE-BioPharma System Documentation Glossary

9 IDENTITY STANDARDS FOR FURTHER REFERENCE

[1] HSPD-12 Policy for a Common Identification Standard for Federal Employees and Contractors
http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html

[2] OMB M-04-04: E-Authentication Guidance for Federal Agencies
http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf

[3] OMB M-06-22: Cost Savings Achieved Through E-Government and Line of Business Initiatives
http://www.whitehouse.gov/omb/memoranda/fy2006/m06-22.pdf

[4] NIST Special Publication 800-63: Electronic Authentication Guideline
http://csrc.nist.gov/publications/nistpubs/800-63-1/sp800-63V1_0_2.pdf

[5] NIST Special Publication 800-53: Recommended Security Controls for Federal Information Systems and Organizations
http://csrc.nist.gov/publications/PubsSPs.html

[6] Federal Information Processing Standard 140-2: **Security Requirements for Cryptographic Modules**
http://csrc.nist.gov/publications/PubsFIPS.html

[7] Federal Information Processing Standard 199: **Standards for Security Categorization of Federal Information and Information Systems**
http://csrc.nist.gov/publications/PubsFIPS.html

[8] X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA)
http://www.cio.gov/fpkipa/documents/FBCA_CP_RFC3647.pdf

[9] X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework
http://www.cio.gov/fpkipa/documents/CommonPolicy.pdf

[10] Citizen and Commerce Class Common Certificate Policy
http://www.cio.gov/fpkipa/documents/citizen_commerce_cp.pdf

[11] Criteria and Methodology For Cross Certification With the U.S. Federal Bridge Certification Authority (FBCA) or Citizen and Commerce Class Common Certification Authority (C4CA)
http://www.cio.gov/fpkia/documents/crosscert_method_criteria.pdf

[12] Level of Assurance Authentication Context Profiles for SAML 2.0, DRAFT, 24 March 2009;
http://www.oasis-open.org/committees/download.php/31807/sstc-saml-loa-authncontext-profile-draft-02-diff.pdf

[13] Kantara Initiative Identity Assurance Framework: Assurance Levels, V1.0
http://kantarainitiative.org/confluence/pages/viewpageattachments.action?pageId=41025670&highlight=Kantara+IAF-1200-Levels+of+Assurance.doc - Documents-attachment-Kantara+IAF-1200-Levels+of+Assurance.doc

[14] Kantara Initiative Identity Assurance Framework Service Assessment Criteria, V1.0

http://kantarainitiative.org/confluence/pages/viewpageattachments.action?pageId=41025670&highlight=Kantara+IAF-1200-Levels+of+Assurance.doc - Documents-attachment-Kantara+IAF-1200-Levels+of+Assurance.doc