Disposition of Comments for a Draft Recommendation Review Period

Document or Set Title: Identity Assurance Framework: Federation Operator Guidelines

Document Status: Draft Recommendation

Originating Work Group: Identity Assurance Work Group

Comment Review Period Closing Dates: 20 September 2010

Submitted to Leadership:

Leadership Council Comments:

Reference Key: FOG_20SEPT_#01

Reference #	Comment Submitted	WG Resolution
FOG_20SEPT_#01	Introduction, p. 4 The name Federation Operator (FO) seems loaded with ambiguities. The "identity federation" is something distinct from the Federation Operator. An operator seems more like a process than a distinct entity. There are many places in the document where the word 'federation' is used and it is not clear whether the term refers to the FO or the identity federation or something else. I would suggest looking at other possible names to eliminate these ambiguities. Possibilities might include: • Identity system manager • Identity federation manager • Identity system coordinator • Identity federation enabler • Etc. Any of these could be condensed into a three-letter acronym that would be unambiguous throughout the document.	"Federation" is a collective structure with a set of rules and standards. The FO is the organization that manages and provides support services to the Federation. Text suggested in document. Modified text: *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.* *...* *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 federation governing body or the two may be one and the same.* **Disposition: Addressed**
FOG_20Sept_#02	Has Kantara gone through this document with an eye towards making sure it is compatible with the federal National Strategy for Trusted	NSTIC is pretty high level. Our approach seems consistent with

	Identities in Cyberspace (NSTIC),www.nstic.ideascale.com? It appears that NSTIC will establish the environment in which Federation Operators will need to function.	that document. The NSTIC implementation plan may provide more guidance on this matter. **Disposition: Future**
FOG_20Sept_#03	P 4, line 83 I would add 'overseeing enforcement' as an additional function of an FO. People will only trust an identity federation if they know there are mechanisms to detect and remove entities that do not play by the rules.	What we have today is periodic audits. Typically there is no single point at which to monitor in "real time" the behavior of a federation member. Modified text: *The FO's roles may include ... 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;* **Disposition: Addressed**
FOG_20Sept_#04	P. 6, line 124 I would recommend adding an item that indicates the FO will include specific performance guarantees. In order to build and maintain trust the FO will need to ensure interoperability across certain environments, the ability to maintain correct operation across version upgrades, compatibility with various standards, ability to support a set of identity functions, limitations on the time a given operation will require to become effective, etc. These will need to be part of a list of specific performance guarantees offered by the FO.	Text added - see line 136, 156 and 168. Typically most of these would be in the membership contract. Modified text: *consider whether "performance guarantees" for the operation and maintenance of FO functions are important and, if so, document what the intended target values are.* *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:* *...* *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 structure and operating requirements of any system used to generate and manage the life cycle of identity credentials;*

		Disposition: Addressed
FOG_20Sept_#05	P. 7, line 157 Consider adding additional bulleted items to the list. • Use cases demonstrating proper application of federation operator resources to solve real-world problems • Workflow diagrams illustrating proper sequencing of federation operator capabilities • An analysis of tools and methods available (required?) to detect fraud, error or misuse of identity federation capabilities • References to the laws and governance under which the FO operates • Policies and procedures for creating, suspending, restoring, revoking, upgrading or downgrading, and terminating a trusted identity	Most of this seems too detailed for the document at hand. The last bullet seems relevant. Modified text: *Define policies and procedures for certifying, suspending, restoring, revoking, upgrading or downgrading, and terminating a trusted CSP.* **Disposition: Addressed**
FOG_20Sept_#06	In general I feel that the document does not deal at all adequately with the need for an FO to be able to detect and correct incidents, errors, fraud, malfeasance, etc. In order to establish trust an FO will need to be able to ensure its potential customers that it knows how to keep its house in order. Nothing will provide this assurance more powerfully than to demonstrate how the FO can strongly detect and rapidly & completely correct misdeeds in its identity environment.	A topic for long discussion. It would be non trivial and expensive to implement if possible at all. Perhaps more discussion of this concern could inform a future version. **Disposition: Future**
FOG_20Sept_#07	Should there be an independent 3rd party "FO tester" agency that acts like a 'white hat hacker' to test and verify the robustness of a FO's ability to enforce proper identity management?	Maybe someday but how many levels of oversight do we need at the present state of this model? Perhaps this would apply more readily to higher LOA's where PKI or equivalent is required. **Disposition: Future**
FOG_20Sept_#08	The FO should have some sort of line in the sand concerning how rapidly it can a) detect and b) disable violations of proper identity management.	Real time "detection" would be very difficult in general. FO action would depend on being notified of such violations, and/or negative results during periodic audits. **Disposition: Not addressed**
FOG_20Sept_#09	P. 8, line 159 Is it the identity federation or the FO or both that should have membership process procedures in place? This is an example of the ambiguity between identity federation and FO that seems to run through the entire document.	The federation governing body establishes the rules; the FO implements them. Modified text: [See item #01 above.] **Disposition: Addressed**
FOG_20Sept_#10	10. P. 9, line 161 How does a Federated Network of Trust (FNT) relate to an FO? How does it relate to an identity federation? Why is FNT material contained in a document describing FOs? There should be an introductory section explaining this relationship and how this section relates to the FO topic.	Modified text: *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 federation governing body 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 CSPs 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. **Disposition: Addressed**
FOG_20Sept_#11	P. 9, line 163 "… role of the federation …" Another ambiguity, please clarify. Is this a role of the FO or of the identity federation or both? It might be extremely helpful if the document contained a diagram showing how FO(s), CSP(s) and identity federation(s), CSPs, IdPs, etc. relate.	The "federation" is a collective, not necessarily an organizational entity. A diagram would be very sparse today. Perhaps a future version will have more complexity. **Disposition: Future**
FOG_20Sept_#12	P. 9, line 165 "credential strength" is not defined. I have an intuitive sense of what is meant here but I think this document needs to provide a precise definition.	Modified text: [the term "credential strength" now is followed by a reference to the definition in NIST 800-63. See section 4.1 in the current document. Also: ...] *Credential strength is a function of credential technology and parameters and should be commensurate with the level of assurance that the CSP asserts* **Disposition: Addressed**
FOG_20Sept_#13	P. 9, line 180 I believe that the FO must agree to undergo active penetration and integrity testing by a 3rd party. How else can a skeptic actually trust the FO's claims?	This would seem to apply more to high LOA CSPs Modified text: *consider whether "performance guarantees" for the operation and maintenance of FO functions are important and, if so, document what the intended target values are.* *Federations that certify high*

		assurance CSPs should consider active penetration and integrity testing by a third party as well. **Disposition: Addressed**
FOG_20Sept_#14	P. 9, line 184 I would change 'annual' to periodic. I think it is likely that an FO will need to publish quarterly or even monthly compliance assessments.	Modified text: *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.* **Disposition: Addressed**
FOG_20Sept_#15	P. 19, line 194 Spell out RP. Is this relying party, resource provider, or some other entity?	Modified text: *Relying Party (RP)* **Disposition: Addressed**
FOG_20Sept_#16	P. 11, line 199 Again, 'federation' is used ambiguously. Please clarify.	Reference not found. **Disposition: Not addressed**
FOG_20Sept_#17	P. 12, the term 'registration authority' in the definition for a CSP is not defined.	Added (also clarified some definitions) Modified text: *Registration Authority —A functional entity that accepts requests for registration with the CSP, does identity proofing as required, and creates a record for the Subject in the CSP's identity management system.* **Disposition: Addressed**
FOG_20Sept_#18	18. P. 12 & 13 Any synonyms for a term being defined should be listed in that definition and given their own definition in the table.	The entire glossary needs review and refinement. See also item #26. **Disposition: Future**
FOG_20Sept_#19	Please add an acronym key at the end of the document.	Modified text: *CSP—Credential Service Provider* *eID—electronic Identity* *FBCA—Federal Bridge Certification Authority* *FIPS—Federal Information Processing Standard* *FO—Federation Operator* *etc.* **Disposition: Addressed**
FOG_20Sept_#20	The guidelines read to us that we have to be assessed for Liberty Alliance Identity Assurance by a Liberty Alliance Identity Assurance	The intent is to provide a generic set of guidelines. The Kantara

	Expert Group approved assessor, so that we can then be assessed by the Kantara Management Board for Kantara Compliance. It's unlikely this federation will participate with so many hoops to jump through before we can even begin to be mapped to your assurance levels. Particularly when our members would only be willing to meet level 1 (bilateral arrangements would be used for higher levels).	IAF is an example of requirements that a federation might adopt for identity service providers. Modified text: *The Kantara Initiative formed the Identity Assurance Working Group (IAWG) to foster adoption of consistently managed identity services. ... This document is one product of the IAWG but its principles should apply equally well to identity federations other than that operated by Kantara*. **Disposition: Addressed**
FOG_20Sept_#21	General comment: I think the paper uses 'federation participant' and 'federation member' interchangeably. This may need looking at.	Modified text: [federation member now is used throughout Also: ...] *Federation Member— An otherwise independent entity that enters into a contract or 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.* **Disposition: Addressed**
FOG_20Sept_#22	Line 85: would suggest this be downgraded to 'may'. Not all federation operators are in the business of providing credentials - this is often specifically the role of its members / participants.	This reference is for identifying credentials for the member IdP itself or it's administrative contacts. Modified text: *supporting a mechanism whereby Federation member IdPs and RPs can be certain they are interacting with another Federation member;* **Disposition: Addressed**
FOG_20Sept_#23	Line 132: not all federations will guarantee verification of 'identity', but will assure verification of assertion. See section 6 of the UK federation Rules Of Membership for more detail.	Fair enough, although we think many readers will be confused by the difference... Modified text: *the processes used to verify the*

		identity information that will be asserted on behalf of Subscribers [In other words, whatever is asserted to a RP must be trustworty somehow.] **Disposition: Addressed**
FOG_20Sept_#24	Line 185: again, not all federations require this type of audit as a 'must' but as a reserve the right to audit. Clarity needed here as to whether self-audit is included in the meaning of this sentence.	Modified text: *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.* *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 CSPs should consider active penetration and integrity testing by a third party as well.* **Disposition: Addressed**
FOG_20Sept_#25	My main point is that the FO should be positioned more as kind of a notary, and the obligations for certification, policy mapping should be moved to accredited auditors and members.	The Federation serves as a virtual trust anchor and therefore must perform whatever obligation that entails. It may assign certain functions to the FO or it could adopt other means. Note that section 2 defines the FO roles as "may include..." **Disposition: Not addressed**
FOG_20Sept_#26	In general I would like to see that the document refers to the central KI glossary instead of a local one.	We will need to align the Kantara Glossary with this one. Then we can do as suggested. **Disposition: Future**
FOG_20Sept_#27	Line 83: Ignorant of the status of MDX standardization, and assuming that severl options might exist: This is only one of several options. E.g. in consideration of the EU TSL (trust service status list), the list of accredited root CAs is already given. The FO needs only to list the federation members and their roles using x.509 subject names. That list needs to be signed of course. An other alternative would be to provide signed meta data containing all member's certificates This sentence could be changed like: "providing the trust anchor that allows reliable authentication and authorization of federation" members"	I believe the comments above apply mostly to PKI-based federations.

FOG_20Sept_#28	Line 84: The FO should only specify the standards for certification, and how auditors and test facilities are accredited. The pattern should follow ISO 9000/27000.	A role of the FO is to ensure that certification happens, not necessarily to perform certification. Modified text: *supporting a mechanism whereby Federation member IdPs and RPs can be certain they are interacting with another Federation member* **Disposition: Addressed**
FOG_20Sept_#29	Line 85: In my view the FO only vouches and publishes for the member, but the collection and maintenance of meta data (except the member's subject names and roles) is up to each CSP or RP.	There are several different ways to accomplish this, including dynamic discovery and bilateral exchange. Clearly the member must create its own metadata (which might be checked by the FO for sanity). However, the FO itself also creates some metadata WRT the member so that must be integrated somehow. Modified text: *as necessary, collecting and making available metadata describing members' infrastructure entities* **Disposition: Addressed**
FOG_20Sept_#30	Line 87: The term trust anchor should only be used on one level, either technical (like a list of certificates) or social/legal. I would rather prefer a usage on the technical level. There is no definition in this document or in the glossary.	The intention was to offer a parallel to the PKI TA as a way to help readers understand the role of the FO. Modified text: *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 functional role of a "trust anchor" similar to that described in the ISO x.509 PKI framework.* **Disposition: Addressed**
FOG_20Sept_#31	Line 115: "Members .. are eligible for membership" – the category member is too general and should be deleted.	What entities are eligible for membership is an issue, e.g.

		must be a legal entity perhaps. Modified text: *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* **Disposition: Addressed**
FOG_20Sept_#32	Line 116: Only CSP is defined in the KI glossary, and IdP is synonymous.	IdP is also in the glossary. Some federations use one term and others use the other term. They may or may not be fully synonymous. **Disposition: Not addressed**
FOG_20Sept_#33	Line 166: (syntax) information of and respect for	Modified text: *it should ensure proper handling of sensitive or confidential information and respect for the privacy of identity Subject information* **Disposition: Addressed**
FOG_20Sept_#34	Line 170: In my view the FO role is more like to that of a notary. The participant would be responsible to do the mapping and have the compliance certified by an auditor accredited for the Federation. The FO may aid the process as a service, but is only responsible to publish the results.	Like many duties, this could be delegated. The FO must ensure it happens and is in accord with federation standards. Modified text: *The FO would be responsible for ensuring that this mapping occurs in a reliable and trustworthy process in cooperation with the potential Member.* **Disposition: Addressed**
FOG_20Sept_#35	Line 200: The Document should use the Kanrata Glossary instead of this one. Definitions are different. IdP and CSP have different definitions, although seem to have a similar concept.	Agreed, but that is not yet available. See comment #26 above. **Disposition: Future**
FOG_20Sept_#36	Definition Table - “Cross Certify”: Terms that are not used in the document should not be defined here	Agreed, the Glossary needs a lot of work. See comment #26 above. **Disposition: Future**
FOG_20Sept_#37	Line 201: These references are not being referenced in the document. They should be renamed to “Further reading” or inserted at the proper places in the document or removed if not required.	Modified text: *9. IDENTITY STANDARDS FOR FURTHER REFERENCE* **Disposition: Addressed**
FOG_20Sept_#38	IdP vs. CSP: Line #74 prefers IdP, but CSP is still being used in some parts of the	IdP is used throughout now except where CSP is

	document.	appropriate. Modified text: *CSP: 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.* *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.* [These will be refined in the process of aligning glossaries.] **Disposition: Addressed**
FOG_20Sept_#39	Scope of the federation (and FO duties): Line #78 says: "An identity federation is a set of identity service providers and relying parties [..] that agree to operate under compatible policies, standards, and in order that end-user identity information provided by IdPs can be understood and trusted by RPs." Was it a conscious decision to limit the function if the federation to entity authentication assurance? An identity federation is subset of a trust federation, although the major one. Other objectives in a trust federation might be: 1. Confidentiality requirements by the RP to the user 2. User requirements to RP: 2a. Privacy beyond idm-specifc PII (like OIX's Levels of Protection) 2b. Information security (like protection against malware on server and correct processing of IdP assertions and meta data) 3. Service level (Availability, liability) of the IdP from the RP's perspective 4. According the the definition of IdP, attribute providers are not included 5. Service level of the RP to the user	For many reasons we need to limit the scope of this initial document. We may wish to expand it in the future. See comment #43 below. Modified text: *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.* **Disposition: Addressed**
FOG_20Sept_#40	The role definition of the FO is not quite clear: Line #111 says: "In this document, the term Federation refers to the [entities] that together define, create and support the trust framework upon which federation members rely." Although a trust framework is mentioned, only identity federation activities are mentioned. I would see some arguments for making the complete set of requirements of a trust federation a concern of the FO: a) If the scope of the federation is too limited, additional bilateral contracts would be needed, reducing the effectiveness of the contractual framework.	See Item #43 below. **Disposition: Addressed**

	b) To make inter-federation contracts manageable, a single trust framework would be needed. c) Given that the other areas must be managed somehow, it seems incomplete to me, if a FO would not be charged with the management the these areas, at least number 1 to 5.	
FOG_20Sept_#41	line #276: "and assurance level are critical to proper" - levels should be plural.	Modified text: *Where protocols that are used to convey identity information and assurance levels are critical to proper operation of the federation* **Disposition: Addressed**
FOG_20Sept_#42	page 8: some acronym definitions are not used, or will not be used if the glossary is moved to a the glossary document: FBCA, HSPD, IDABC, NIH, PEGS, and my be others.	This will be corrected when the Kantara Glossary is referenced instead of this one. See item #26 above. **Disposition: Future**
FOG_20Sept_#43	General comment: The FOG scope reflects pretty much the scope of the IAF which is limited to the assurance of the subject's identity. The scope of the document is too narrow. It should include all the elements that will interact in a trusted fashion. There is a list of other requirements to establish a complete trust federation. It includes: - RP requirements - Identity subject requirements - PII privacy requirements - Richer identity - SOA of attributes - etc.	The FOG, as originally envisioned, was based on a set of identity service providers and relying parties agreeing to abide by a set of rules. The federation operator would have a direct contractual relationship with those entities. It would not, in general, have a direct relationship with subjects; subject requirements would have to be reflected in IdP rules. While a SOA for richer attributes might be a federation member, that function has yet to be defined in a stand-alone sense. For now, the IdP is assumed to gather authoritative attributes (although that is missing from the current IAF). Modified text: *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.* **Disposition: Addressed**
FOG_20Sept_#44	I suggest that the scope for initial release of the FOG be FO, IdP, and RP issues and/or requirements. Additional elements could be added at a later date.	See comment #43 above. **Disposition: Addressed**
FOG_20Sept_#45	I would suggest that section 3 be reworded to identify the documentation that needs to exist rather than the actions that need to take place to develop the documentation. As such, "Develop an Operating Policy which should" would become "Federation Operating	At this point we are providing guidance as opposed to specific requirements. Perhaps a future revision can be more specific.

	Policy which includes:". The lead in paragraph identifies that the Federation governing body should develop (or adopt existing) these items.	**Disposition: Future**
FOG_20Sept_#46	I would suggest that the topics addressed in sections 3.1, 4.1, 4.3, 4.3, 4.4, and 5 be reworked into either a role the FO needs to play or business practice documentation that should exist. This reworking would leave the FOG identifying the role of the FO and the business practice documentation it should consider having in place. The important points in each of these sections which justify the role or documentation item could, if really required, become part of the Background and Context section.	Agreed that the structure of this document is somewhat rough. The hope is that the next revision will address that and make the flow more directly accessible. **Disposition: Future**
FOG_20Sept_#47	Define "Federation governing body" (FGB)	Modified text: [Several references have been modified in the document body and added the following to the Glossary] *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.* **Disposition: Addressed**