The Open Identity Trust Framework (OITF) Model

Managing Editor:
Mary Rundle

Co-Authors:
Eve Maler
Anthony Nadalin
Drummond Reed
Mary Rundle
Don Thibeau

March 2010

Acknowledgements

The authors would like to express thanks to the many people who provided guidance during the writing process. They would specifically like to note contributions by Bob Blakley, John Bradley, Scott David, and Mary Ruddy.

I. Introduction

Today many online interactions require the sharing of identity information[1] even though this sharing poses substantial trust challenges, both for the party disclosing the information and the party receiving the information. These trust issues to date have been addressed by a fairly simplistic model in which a third party, referred to as an "identity service provider"[2], discloses identity information on behalf of a user[3] to a recipient, called the "relying party"[4]. The identity service provider reduces risk and promotes efficiency by issuing credentials and confirming aspects of the exchange, for example that the user is who he or she claims to be, is in a certain role, and has certain attributes. Figure 1 illustrates this traditional triangle of parties involved in an exchange of identity information.

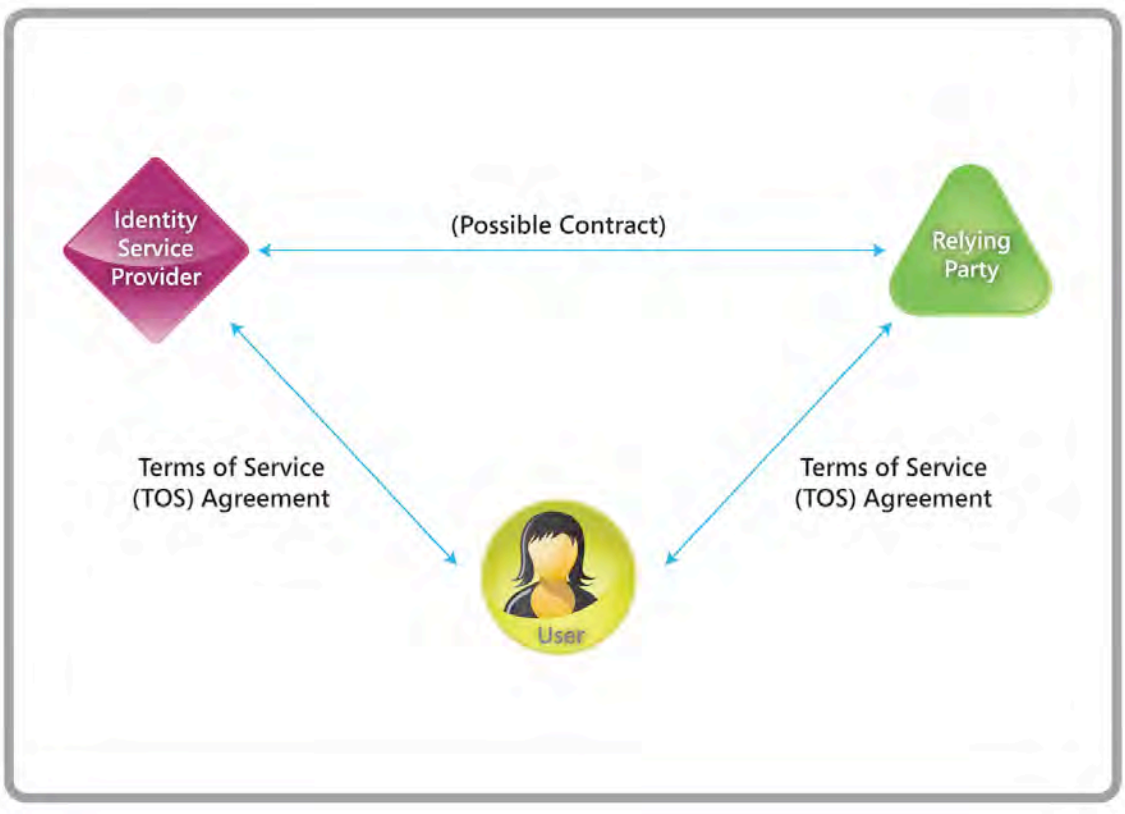

Figure 1: The traditional triangle of parties involved in an exchange of identity information

With this basic model, strangers from all over the world can interact easily, especially as technologies like OpenID and Information Cards facilitate the flow of identity information.

[1] The term "identity information" here includes both authentication information for establishing that a legal person or an entity is who he, she, or it claims to be (which may or may not include an identifier), as well as attribute information (details about that person or entity). Such identity information is sometimes referred to as "claims".

[2] This role is sometimes referred to as "identity provider", "IdP", "IP", "OpenID provider", or "OP".

[3] In this paper the term "user" refers to a natural person (i.e. a human being) or a juridical person (e.g., a corporation); the user is represented by a partial digital identity (on the theory that a person is never entirely represented in digital form). To the extent non-legal entities (e.g., devices) act in the exchange of identity information, the legal persons responsible for their operation may be held accountable.

[4] This role is sometimes referred to as "service provider".

Still, these flows of identity information carry significant risks. How can parties wishing to interact know that reasonable technical, operational, and legal safeguards are in place to govern their practices? For example, the relying party wants to know whether the user has been authenticated to some degree of assurance, whether the attributes imputed to the user by the identity service provider are accurate, and whether the identity service provider is authoritative for those attributes. For its part, the identity service provider wants to know if it has accurate information about the user and whether, if it shares information, the relying party will use it in accordance with contractual terms and conditions and the law. And the user wants to know if the identity service provider and relying party can be entrusted with sensitive information and if they will abide by the user's preferences and respect the user's privacy. Most importantly, all the parties want to know if the practices described by the other parties are actually those implemented by the parties, and how reliable those parties are.

So the question becomes: can these aspects of exchanges involving identity information be worked out in a way that reduces barriers and promotes trust, so that people can get on with what they want to do?

This paper proposes the Open Identity Trust Framework (OITF) model as a way to achieve this confidence. Section II introduces the basic roles and relationships in the model. Section III describes implementation mechanisms. Section IV provides examples to illustrate the types of exchange relationships that the OITF model can facilitate. Section V defines a set of "Principles of Openness" that are built into the OITF model to establish a base level of transparency, accountability, and open competition. Lastly, because some key questions remain unresolved, Section VI highlights tough issues and calls for the involvement of a broad representation of stakeholders to grapple with these challenges and craft appropriate approaches forward.

II. OITF Roles and Relationships

Figure 1 (above) illustrated the notion that one way to promote confidence among identity service providers, relying parties, and users is with direct legal agreements. These agreements are common when two players, such as an airline and a car rental company, frequently do business with each other's customers. The primary challenge with these simple, triangular relationships is that they do not scale to large numbers of identity service providers, relying parties, and users who have no way to gauge each other's technical, operational, and legal practices. Even if parties could, the transaction costs for working out matters among themselves would be prohibitive as such interactions would require "pair-wise" (bilateral) contracts. Quite simply, the overhead of establishing contractual agreements bilaterally would not be justified by the value and frequency of the transactions.

To enable large-scale networks of trust, the solution proffered is an *Open Identity Trust Framework (OITF)* – that is, a set of technical, operational, and legal requirements and enforcement mechanisms for parties exchanging identity information. In an OITF additional actors look after these requirements and mechanisms to support the flow of information among users, identity service providers, and relying parties. The roles and relationships of these additional actors are as follows:

- **Policymakers** decide the technical, operational, and legal requirements for exchanges involving identity information among a group they govern. (Technical requirements might include, for example, product version levels, system configuration, settings, and protocols; operational requirements may address, for example, asset management, access control, and disaster

management; and legal requirements might be geared toward fair information practices, for instance.) Although governments are likely to play this role, a private body could establish requirements and in effect serve as the policymakers for a given group (e.g., a professional association).

- **OITF Providers** (OITF Providers) translate the requirements of policymakers into their own blueprint for a trust framework that they then proceed to build. As OITF Providers do so, they need to attract parties by explaining how their requirements support the interests of all. They then arrange a way for the practices of identity service providers and relying parties to be assessed to see if they are comparable to the policymakers' requirements and meet any additional conditions that the OITF Provider may set out; if they pass and are certified, an OITF Provider contracts with these parties to apply these methods in exchanges involving identity information. The OITF Provider typically operates a certification listing service that indicates which identity service providers and relying parties have been certified by which assessors, for which criteria, and for which trust frameworks.
- **Assessors** evaluate identity service providers and relying parties and certify that they are capable of following the OITF Provider's blueprint.
- **Auditors** may be called on to check that parties' practices have been in line with what was agreed for the OITF.
- **Dispute resolvers** may provide dispute resolution services for disagreements of a legal nature.

These entities support interactions among the parties to the traditional triangle, with the whole lot being the "participants" in the OITF.

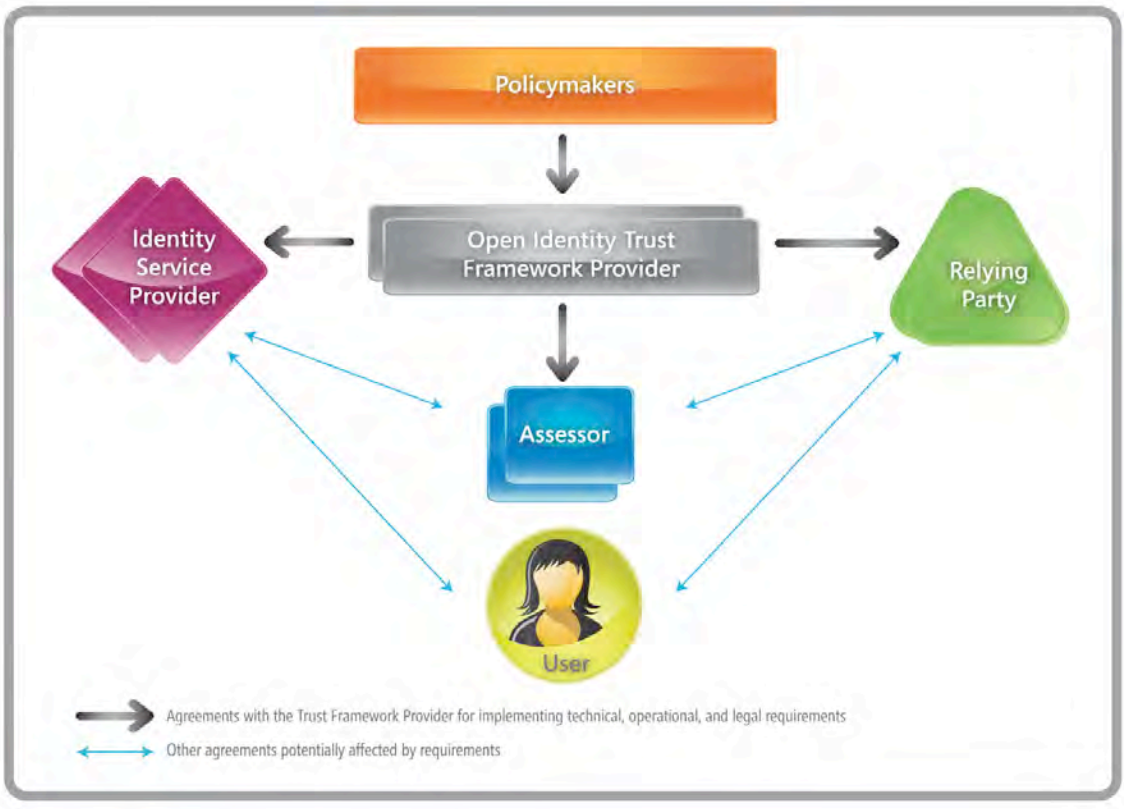

Figure 2: The participants in an OITF for identity information

Figure 2 shows these roles and relationships in terms of agreements that link the participants. Policymakers start by deciding the technical, operational, and legal requirements for exchanges of identity information that fall under their authority. They then select OITF Providers to implement these requirements. These OITF Providers translate the requirements into a blueprint for a trust framework that may include additional conditions of the OITF Provider. The OITF Provider vets identity service providers and relying parties and contracts with them to follow its trust framework requirements when conducting exchanges of identity information. The contracts carry provisions relating to dispute resolvers and auditors for contract interpretation and enforcement. Requirements flow down through agreements, as shown in the directional arrows in Figure 2.

III. Implementation Mechanisms

Implementation mechanisms include the following:

A. ***Criteria for measuring*** a party's ability to meet technical, operational, and legal requirements for the OITF.
B. ***A set of certification processes*** for evaluating and publishing whether parties are capable of meeting the OITF's requirements.
C. ***A set of legally binding agreements*** that together constitute the legal structure of the OITF.

A. Criteria for measuring capabilities

As noted above, policymakers set out the technical, operational, and legal requirements for exchanges of identity information over which they have authority. OITF Providers translate these requirements into actionable form and possibly add their own requirements as they create a trust framework. As they establish and implement requirements, policymakers and OITF Providers will need to include criteria by which potential OITF participants may be measured.

Rather than developing the criteria themselves, policymakers and OITF Providers may wish to draw on standard criteria that experts have already elaborated. The more they use standard criteria across different trust frameworks, the easier it is for participants to understand and apply the criteria consistently. Moreover, named sets of criteria can serve as shorthand to indicate different degrees or types of rigor in requirements or capabilities.

Because the need for OITFs is shared worldwide, it is logical that standard indicators will serve best if they attain international support.

Example: Level of Assurance and Level of Protection

Policymakers may set out requirements for what "level of assurance" (LOA) an identity service provider must meet in terms of its ability to provide reliable identity information. Similarly, policymakers may establish requirements for what "level of protection" (LOP) a relying party must be capable of applying to identity information that it receives – in other words, the degree to which a party's treatment of data reflects internationally accepted data protection principles. These requirements will need to be accompanied by criteria for measuring participants if they are to be meaningful. Because different trust frameworks will vary in their concern for LOA and LOP, it will be helpful for the sake of common understanding to have not just criteria, but also a standard way to signal degrees of rigor.

Policymakers may look to experts to develop these standard indicators. Continuing with the LOA example, the U.S. Government issued a "specification profile" setting out technical, operational, and legal requirements for identity service providers from the private sector to authenticate citizens for interactions on web sites of the U.S. Government.[5] Rather than starting from scratch in developing LOA criteria, the Federal agencies involved in this Identity, Credential, and Access Management (ICAM) process looked to a four-level standard for LOA that the U.S. National Institute of Standards and Technology (NIST) had already developed for entity authentication. (In this context, the term "assurance" concerns proofing processes at registration and the technologies used when that person subsequently logs in to perform an identity-based transaction – as well as the policies and practices that implement both.)

In terms of international support, a joint committee of the International Telecommunication Union (ITU) and the International Organization for Standardization (ISO) is considering adopting LOA standards similar to those of NIST. This new work will further flesh out standards for entity authentication assurance; the bodies could also decide to extend these standards to attribute assurance. Because the LOP concept nicely complements the LOA notion, a reasonable step would be for policymakers at the international level (e.g., the International Conference of Data Protection and Privacy Commissioners) to develop standards for LOP.

[5] See http://www.idmanagement.gov/drilldown.cfm?action=openID_openGOV. It is worth noting that policymakers may call for multiple OITFs, any of which may have its own specification profiles. A specification profile may be reused in different trust frameworks.

B. A set of certification processes

The general impetus for an OITF may come from policymakers' setting out overall technical, operational, and legal requirements for exchanges of identity information over which they have authority. OITF Providers may then meet this demand by assembling all the necessary components to build a trust framework. In doing so, the OITF Provider bears responsibility for ensuring that potential identity service providers and relying parties are able to fulfill the trust framework's requirements, whether those requirements are identical to what the policymakers call for or whether the OITF Provider has a comparable set of requirements that are at least as rigorous. The OITF Provider does its vetting and vouching of capabilities through a set of certification processes.

This vetting and vouching may begin with the OITF Provider establishing a clearly defined set of requirements and sharing them publicly to enable understanding of the methods used in certification. While certification methods may vary between different OITF Providers according to the requirements of different trust frameworks, typically they will include five basic processes:

- A process by which an assessor may apply and be approved to provide evaluations for a particular trust framework, including conditions like competence, independence, absence of a conflict of interest, etc.
- A process by which an identity service provider or relying party may apply for certification from among the options available from a particular OITF (for example, self-certification, audited self-certification, and third-party certification).
- A process for conducting the assessment required for certification.
- A process for accepting the assessment results and publishing the final output of the process through certification metadata in a certification listing service typically operated by the OITF Provider.
- A process for renewing these certifications at regular intervals (with possible auditing of compliance) and on occasions when trust frameworks are revised, participants update their practices, market conditions change, etc.

C. A set of legally binding agreements

Five basic types of agreements work together as a set to constitute the legal structure of a trust framework:

1. *Policymaker-OITF Provider Service Agreement (sometimes referred to as a Memorandum of Agreement, or MoA)*. This agreement is between the policymakers (or a related entity that has the capacity to enter into agreements) and an OITF Provider. The agreement spells out technical, operational, and legal requirements set by policymakers.
2. *Identity Service Provider Certification Agreements.* These are contracts between the OITF Provider and identity service providers who have been certified to meet the technical, operational, and legal requirements of a trust framework. (It is foreseeable that not all trust frameworks will call for these agreements as part of their basic legal structure. For example, if policymakers already have a relationship with identity service providers, those parties may be deemed acceptable without certification.)
3. *Relying Party Certification Agreements.* These are contracts between the OITF Provider and relying parties who have been certified to meet the technical, operational, and legal requirements of a

trust framework. (Here again, it is possible that not all trust frameworks will call for these agreements as part of their basic legal structure. For example, if policymakers already have a relationship with relying parties, those parties may be deemed acceptable without certification.)

4. *Assessor Agreements.* In their contracts with OITF Providers, assessors agree to serve the OITF by evaluating whether identity service providers and/or relying parties that wish to participate in the OITF meet requirements. These agreements need to bind assessors to use a set of recognized and enumerated processes when they conduct assessments. Assessors then sign contracts with these would-be participants to conduct their evaluations and certify them if they are capable of meeting the requirements. (Not all trust frameworks involve these agreements; for example, those that allow self-certification might not.)
5. *Terms of Service (TOS) Agreements*. If an OITF is designed to establish rights and responsibilities for users that they do not already have in TOS agreements with identity service providers and relying parties, the relevant requirements may need to flow down to the TOS agreements that directly involve users as parties. The OITF Provider might promulgate a set of model terms to be included by identity service providers and relying parties in their TOS agreements with users. For example, model terms might address opportunities for redress and the right of parties to require audits of each other's practices.

Note that there may be no single "trust framework agreement" to constitute the legal structure of an OITF; rather, the five types of agreements work together to do so.

The set is shown in Figure 3, where numbered arrows correspond to the five types of agreements.

Because the OITF Provider sits "between" various parties, a single agreement that each has with the OITF Provider takes the place of an exploding number of pair-wise (bilateral) direct agreements that might otherwise be required among them.

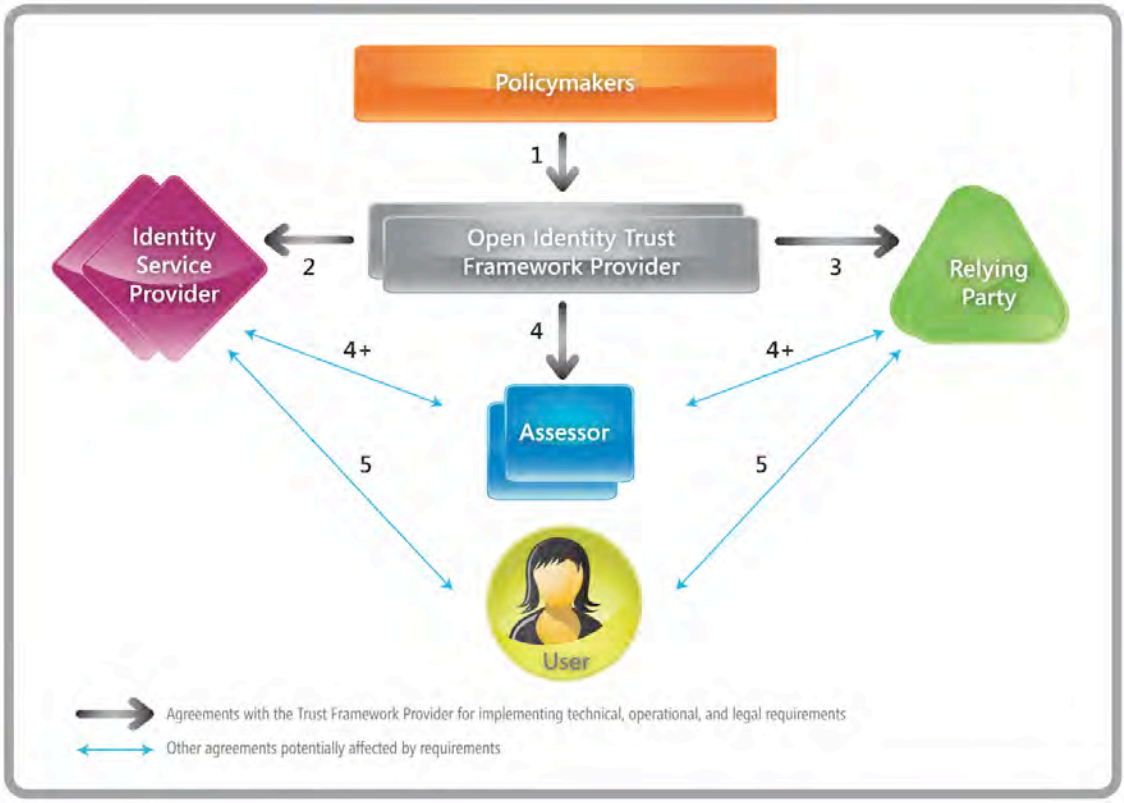

Figure 3: Agreements among OITF participants

To administer their requirements, the policymakers may form agreements with multiple OITF Providers, which in turn may contract with multiple identity service providers and relying parties, and possibly assessors (as shown in Figure 3). Not shown are the multiple sources of policy (such as government agencies) that may inform the official technical, operational, and legal requirements established by the policymakers. OITF Providers meet these demands as they actualize the OITF for the policymakers; if policymakers approve them, OITF Providers may have their own approaches that are comparable to what the policymakers spell out, and the OITF Providers may even raise the bar by imposing requirements that are more rigorous.

It is worth noting that policymakers, OITF Providers, assessors, identity service providers, relying parties, and (by extension) users might all participate in multiple trust frameworks. Because these relationships could result in quite a tangle, one challenge is to promote clarity regarding which OITF is governing any given transaction.

Again, provisions for audits and dispute settlement can reinforce confidence across all these agreements. The larger the number of participants served by a trust framework, the more important it is to have an efficient and equitable means of determining what has actually occurred in exchanges and of resolving disputes. For example, an OITF that spans the globe and serves not just multinational enterprises but also small organizations and individuals will need to provide a way for parties at all income levels to determine if something has gone wrong in a transaction and to obtain speedy redress for a breach of contract. An OITF may arrange for standing auditors and dispute resolvers – typically professional organizations that

specialize in these functions and are always available to conduct audits and mediate disputes involving various parties. Agreements would need to oblige parties to collect, preserve, and share information about their operations for fact-finding pursuant to dispute resolution.

IV. Examples of Trust Frameworks for Identity Information

Following are three examples of possible trust frameworks for the exchange of identity information.

The first is a governmental plan whereby an agency serving in the policymaker role approves private OITF Providers to run trust frameworks that involve private-sector identity service providers and public-sector relying parties. Figure 4 illustrates how, because the relying party web sites would be governmental, the OITF Providers might not need to vet and vouch for them in order to satisfy the policymaker agency.

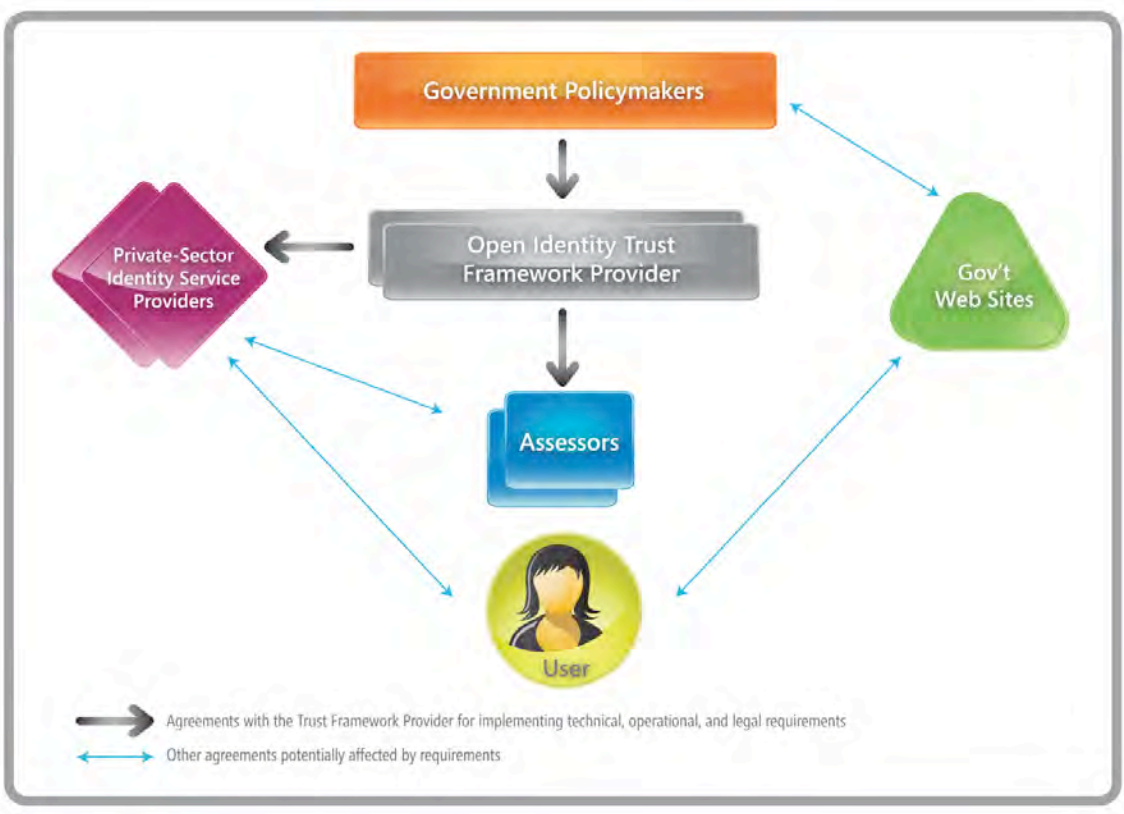

Figure 4: The flow of requirements in a government-commissioned OITF

The example suggests that governments at all levels – national, sub-national, and local – could serve as policymakers setting out requirements for exchanges involving identity information. The U.S. GSA Identity, Credential, and Access Management (ICAM) pilot project announced on 10 September 2009 follows this structure.

Figure 5 shows how non-profit associations could also create demand for trust frameworks.

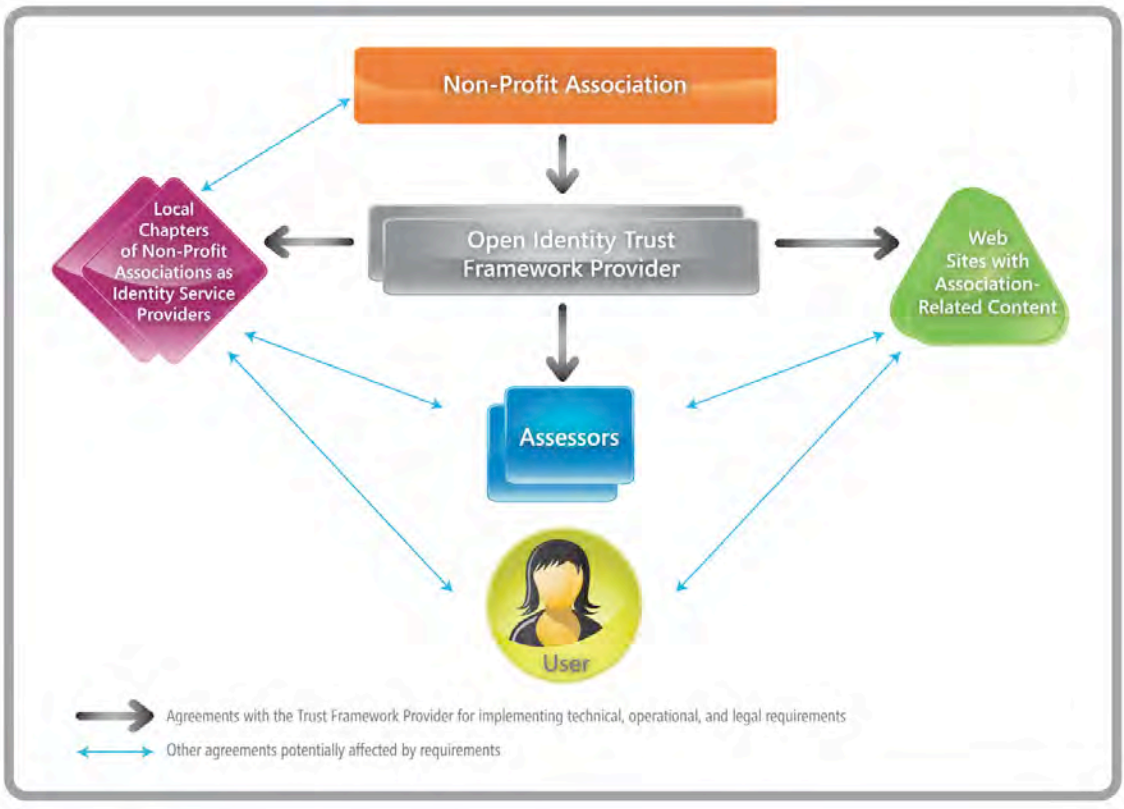

Figure 5: Non-Profit Associations Spurring Demand for OITFs

For example, if an association had chapters, an OITF could enable members to register with their local chapter and to sign up for credentials with them as identity service providers. Members could then use these credentials to log in to web sites relating to the association so as to prove they were members in good standing and entitled to access special features (e.g., discounts).

Another type of organization that may wish to use an OITF is an industry association that has some member entities serving as identity service providers and others serving as relying parties (or possibly some serving in both capacities). If those entities were in the business of adding value to identity information, they might have relationships structured according to the diagram shown in Figure 6, where the identity service provider has the connection to the user.

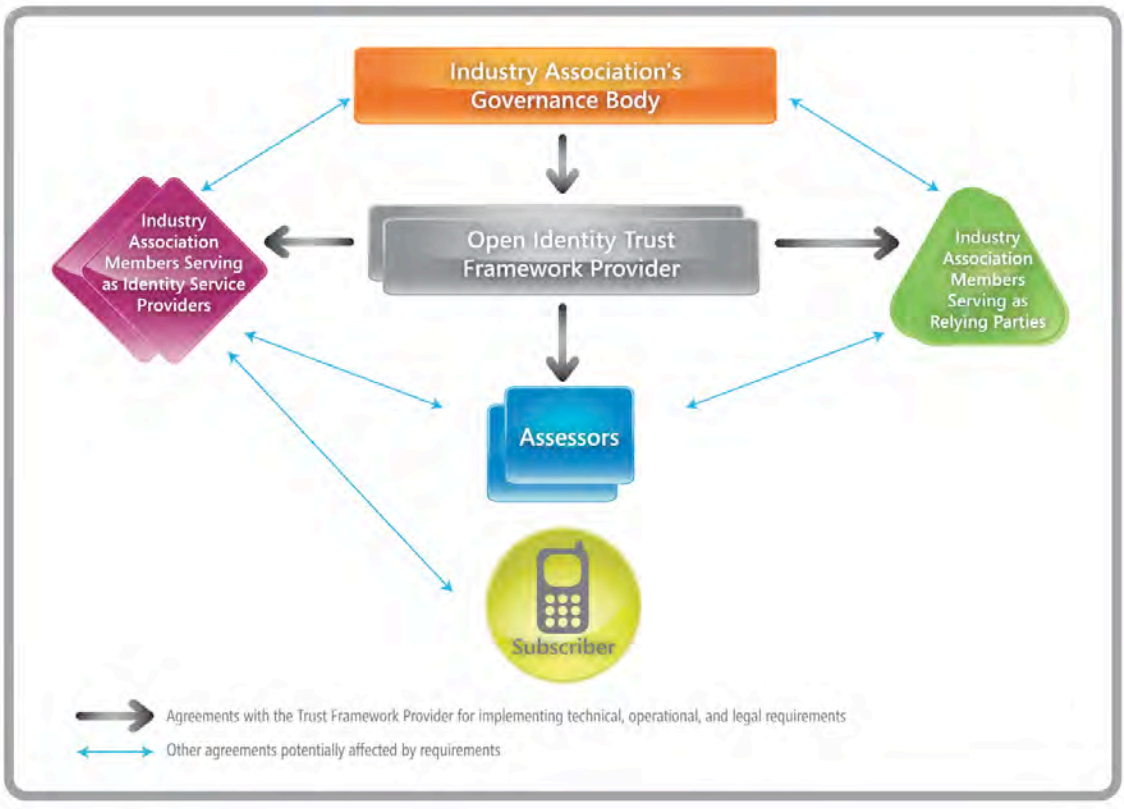

Figure 6: An industry association whose members add value to identity information

Note that this figure shows a device that the user might use when interacting electronically; the device could be the source of data that the identity service provider gleans, with a subscription contract containing terms whereby the user at some stage consented to allow the provider to use his or her identity information. The members of the industry association might add value to this data by analyzing that user's patterns and making this information available to other service providers (e.g., firms that tailor advertising to user interests or security outfits that analyze intelligence information).

V. Principles of Openness

As explained above, an OITF needs to combine objective criteria for measuring parties' capabilities, processes for conducting assessments, and a set of agreements tying participants together. But these components alone are not sufficient to address the deep misgivings many people have today about online exchanges involving identity information. How can participants protect themselves from the risk that an OITF could be corrupt or otherwise flawed? What will give them confidence is if an OITF also offers transparency, accountability, and open competition.

The OITF model helps accomplish this by incorporating a set of Principles of Openness, contained in the box below. When combined with the OITF participant roles and relationships and implementation mechanisms described in previous sections, these Principles define the heart of the OITF model.

Principles of Openness

All participants in an Open Identity Trust Framework must commit to abide by the Principles of Openness and to incorporate them into their agreements relating to the trust framework. These Principles are:

Lawfulness. OITF Providers are responsible for ensuring that the technical, operational, and legal requirements of the OITF are consistent with the laws of the jurisdiction(s) where parties use it to conduct exchanges involving identity information.

Open reporting and publication. OITF Providers must produce periodic reports on the operation and governance of the trust framework. They must ensure that a web site devoted to the OITF provides easy and timely access to (a) the periodic reports, (b) all agreements that constitute the legal structure of the trust framework, (c) all policies and procedures by which the OITF operates (including criteria and processes for certification), (d) a plain-language explanation of the trust framework's trust characteristics (for example, data protection strengths and weaknesses), and (e) records of dispute resolution activities and their results. However, publication is not required for assessment reports. OITF Providers must ensure that all parties to agreements under the OITF have visibility into who is participating in it and in what capacity.

Ombudsmen. OITF Providers must ask governments where they do business to designate independent ombudsmen whose role is to look after the interests of individual users under their respective jurisdictions, and they must ensure that the OITF is designed to allow these ombudsmen to do their job. If law requires the sharing of identity information (including biometric data, behavioral data, and social graphs) without the informed consent of the person in question, parties to the OITF who are ordered to share this information must involve the ombudsmen.

Anti-circumvention and open disclosure. OITF participants must not be party to any side agreements that compromise the integrity of commitments under the trust framework. If a participant is party to any agreements that might otherwise conflict with obligations under the trust framework, that party must disclose the existence and nature of these agreements to the affected party or parties at the earliest opportunity. OITF Providers and assessors must disclose all their agreements and the terms of those agreements.

Non-discrimination. Participants in the OITF must avoid discrimination. Participants must not engage in exclusive dealing arrangements relating to the trust framework.

Interoperability. Software and hardware specified in the technical requirements of an OITF must conform to defined standards that promote interoperability.

Open versioning. OITF Providers must spell out how new versions of the OITF will be decided, when they will be published, how participants will be transitioned to these new versions, and how the interests of participants in the OITF will be protected.

Participant involvement. OITF Providers must enable participants to share contact details so that they may convene virtually to discuss matters related to the trust framework.

Data Protection. Participants in OITFs will adhere to data protection practices at least as strong as those of the OECD's Privacy Guidelines (Part Two in its entirety, concerning collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability).

Accountability. OITF Providers must state on a publicly accessible web site how the OITF provides accountability to all participants, including the users whose identity information will be exchanged under it.

Auditability. OITF Providers must ensure that all parties to agreements under the trust framework, including themselves, agree to be subject to audit for conformance with these Principles of Openness.

Redress. OITF Providers must ensure that all agreements under the OITF afford the parties an effective right and mechanism to seek redress.

Of course, for the Principles of Openness to instill true confidence, they must apply in fact and not just on paper.

Participants in OITFs have an interest in preserving the brand value of the OITF model since it is an indicator of quality service. The shared interest in preserving the brand value of the OITF model may suggest the need for a governance body, though this notion is debatable. At any rate, the details of how best to set up such a governance body and ensure its proper functioning would require considerable attention.

VI. Conclusion

This paper has asserted that, for exchanges involving identity information, the OITF model is a solution that provides parties with assurance that practices are effective, accurately described, and faithfully executed – and that there is recourse for failures. The Principles of Openness are touted as the strength of the OITF model as they afford transparency, accountability, and open competition. Is this promise as good as it sounds?

In terms of *transparency*, a key question is whether people will even be able to know if the Principles of Openness are being followed. For example, there could be a deal among policymakers, OITF Providers, identity service providers, and relying parties to treat identity information in a way that is not consistent with the Principles of Openness (including data protection), and users might be left in the dark. Hurdles abound since without transparency it will be well nigh impossible for participants to be aware when conditions of an OITF are violated, or to prove that a violation occurred, or to determine what harm resulted. Is it sufficient to rely on the good will of others to shed light on what is taking place? Moreover, since policymakers, OITF Providers, assessors, identity service providers, relying parties, and (by extension) users might all participate in multiple trust frameworks, it will likely be hard for users to understand which trust framework is governing any given transaction and to be able to assess its trust characteristics. Lastly, it is particularly important that the design and operation of the certification listing service be transparent and open to expert scrutiny, because this vital technical function of an OITF Provider is the operational component upon which the market depends for accurate metadata on certification status.

Regarding *accountability*, will participants be able to hold each other responsible if they fail to follow the Principles of Openness? OITF participants are all obliged to incorporate the Principles into their agreements with each other, but if those agreements do not explicitly provide third-party beneficiaries the right to enforce those commitments, only the direct parties to the agreements may hold each other to account. In other words, if those parties decide not to require each other to follow the Principles, other participants in the OITF cannot bring a claim against them pursuant to that contract. Aside from the right of enforcement, there is the fundamental challenge that conflict resolution can be tenuous and prohibitively expensive, especially when disputes involve parties on opposite sides of the globe; the OITF model needs to address this problem if opportunities for redress are to be meaningful.

When it comes to *open competition*, an important question for an emergent system of trust frameworks is what kind of market structure is likely to result. Will there be concentration, such that only a few players occupy the choicest positions in the marketplace? Will the market structure spur product differentiation, or will it result in a narrowing of offerings? Will it be easy for new entrants to compete? If the effects on the market structure are negative, the system could damage not just the economy but also the political landscape as a few powerful players would be able to exercise enormous influence over digital services.

For these reasons it is clearly important to safeguard against ways in which a system with the potential to enable trusted transactions at Internet scale could be abused. For example, imagine that the OITF model takes off and identity aspects of all digital communications become reliant on this new layer of the Internet. Society could become dependent on this type of infrastructure for collective action. The authors want to make it clear that trust frameworks for identity information portend to be so important for the future information society that they warrant extensive scrutiny, participation, and feedback from a wide representation of stakeholders.