AN OPEN MARKET SOLUTION FOR ONLINE IDENTITY ASSURANCE

A New Solution for Internet-Scale Identity Assurance: the Open Identity Exchange

AUTHORS:

Don Thibeau - OpenID Foundation
Tony Nadalin - Microsoft
Mary Rundle - Microsoft
Drummond Reed - Information Cards
Eve Maler - PayPal

MARCH 2010

An Open Market Solution for Online Identity Assurance

Executive Summary

This white paper introduces a new solution for Internet-scale identity assurance: the Open Identity Exchange (OIX). It starts by summarizing the underlying *Open Identity Trust Framework* model on which OIX is based. It then covers the structure and operation of OIX itself, and how members qualify for certification listings for specific trust frameworks at specific levels of assurance and protection. It describes several OIX trust frameworks, both in operation and in development, and concludes by examining how OIX is designed produce a "race to the top" in online identity policy standards.

Table of Contents

March 2010

Introduction

"How many usernames and passwords do you have?" Ask any group of frequent Internet users that question and the answer will be a collective groan. Usually within seconds someone will fire back: "Why can't they solve that problem?"

Thankfully, someone has. Technologies now exist to let users bring their own registration and login credentials to a website instead of being forced to register YAUP (Yet Another Username/Password). The two best known are:

- **OpenID**, which lets users register and login to OpenID-enabled websites using their own choice of OpenID identifier and password (or other credential). Users can have their own OpenID service (such as their blog), or they can use a third-party OpenID provider like AOL, Google, or Yahoo. A key advantage of OpenID is that it requires no client-side software—it works with any standard Internet browser. The open standards for OpenID are maintained by the non-profit OpenID Foundation (OIDF).
- **Information Cards,** which represents all of a user's identities, whether self-created or from third parties (e.g., employer, financial institution, school, government, etc.) as visual "cards" in a software application called a *card selector.* The cards themselves may be stored on the same computer as the card selector, or on a mobile device, or "in the cloud". The open standards for Information Cards are developed at OASIS and promoted by the non-profit Information Card Foundation (ICF).

Collectively these solutions are referred to as *open identity technologies* because they take the closed identity systems currently deployed by most websites and "open them up" to accept identity credentials issued by other parties. In open identity systems, the sites producing identity credentials are called *identity service providers*, and the sites accepting them are called *relying parties*.

Figure 1 illustrates the basic "trust triangle" involved in all open identity solutions. By introducing a third party—the identity service provider—users are able to offload the work of maintaining identity management credentials for all the sites where they have accounts.

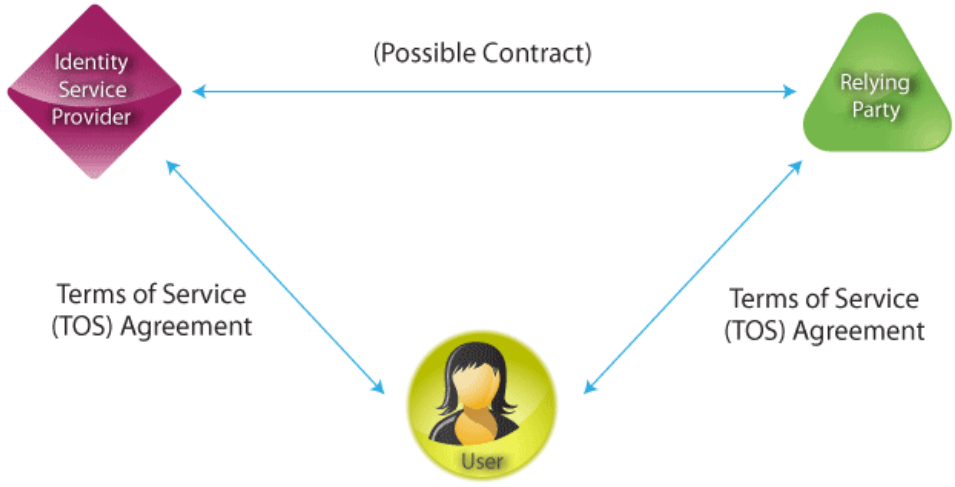

Fig. 1: The basic trust triangle involved in all open identity solutions

While the advantages of open identity technologies are obvious—they reduce the friction of using the Web, much like credit cards reduce the friction of paying for goods and services—they also introduce a new problem: *who trusts whom*? In other words, how does a relying party know it can trust credentials from an identity service provider without knowing whether that provider's security, privacy, and operational policies are strong enough to protect the relying party?

This is not a technology problem. It is a business, legal, and social problem—a *policy* problem—and thus must be solved with real-world legal agreements.

It is also a very real problem for—among others—the U.S. government. Shortly after coming into office, the Obama administration asked the U.S. General Services Administration (GSA) how to start using open identity technologies to let the American public more easily, efficiently, and safely interact with federal websites such as the National Institute of Health (NIH), the Social Security Administration (SSA), and the Internal Revenue Service (IRS).

But U.S. federal agencies can't just accept OpenID or Information Card credentials from anyone with a server. They must be able to verify that the identity provider's policies and practices meet a specific level of assurance (LOA) required by the government—a low LOA for simple tasks like reserving a campground at a national park, but a high LOA for accessing sensitive records such as tax returns.

So in meetings beginning at the 2009 RSA Conference, the GSA invited the OIDF and ICF to join it in a public/private partnership to create a solution—a solution that would do for the exchange of identity information what credit card networks like Visa® and MasterCard® did for the exchange of payment information.

This white paper, being released at the 2010 RSA Conference, describes this solution in four parts:

1. The model the industry developed to meet this need.
2. The new organization—OIX—the industry formed to implement this model.
3. The first examples of how OIX is being put to work.
4. The reasons this solution can work at Internet scale.

OITF – An Open Market Model for Online Identity Assurance

The key challenge to providing identity assurance at Internet scale is removing the need for the direct trust agreements shown in the basic trust triangle (Figure 1 above). When the credit card industry had to solve this same problem, their solution was to create credit card associations such as Visa® and MasterCard®. As shown in Figure 2, these associations replaced the direct "pairwise" agreements that were otherwise needed between banks and merchants.

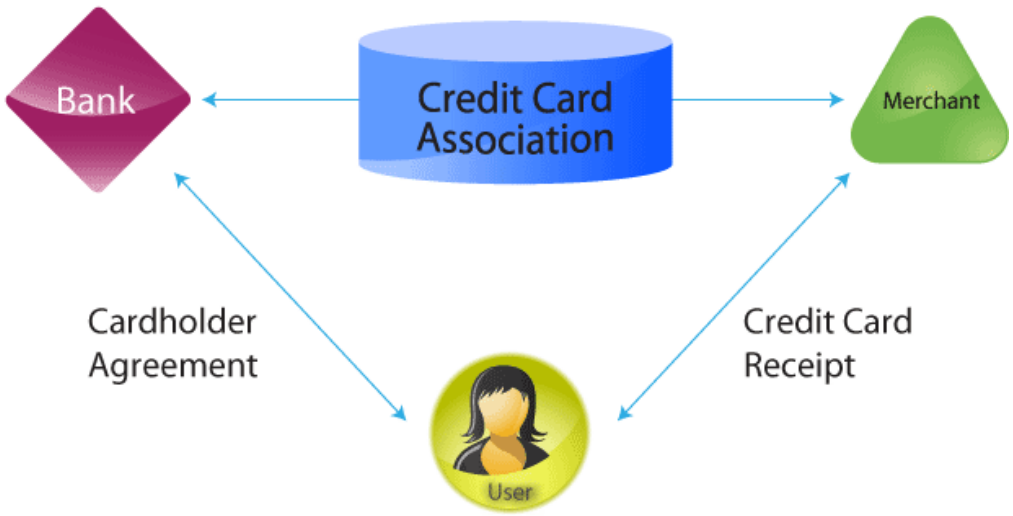

Fig. 2: Credit card associations replaced pairwise agreements between banks and merchants

Credit card associations set the policies banks and merchants need to follow in order for their transactions to be accepted on the network. They also vetted the qualifications of banks and merchants to become members of the network, and monitored them for ongoing compliance.

This approach has worked well for a network dedicated to the exchange of a relatively narrow set of information—payments—within a well-defined context—commerce—and within an industry that is already highly regulated. By contrast, the exchange of identity information is inherently broader, more contextual, and in many cases less regulated. So it calls for a more flexible model that can accommodate many different market requirements for identity assurance.

The OIDF, ICF, and their respective members collaborated to develop this Open Identity Trust Frameworks (OITF) model.[1] The fundamental schematic of this model is shown in Figure 3.

[1] See *The Open Identity Trust Framework Model* by Eve Maler, Tony Nadalin, Drummond Reed, Mary Rundle, and Don Thibeau, March 2010

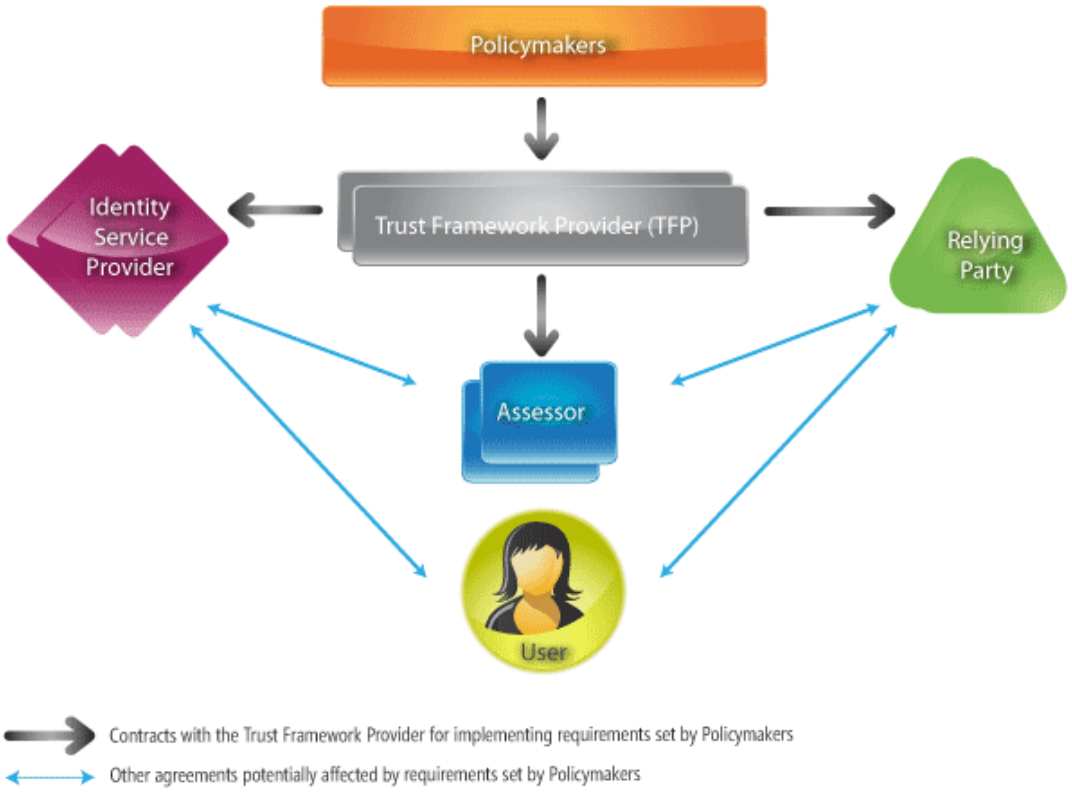

Fig. 3: the Open Identity Trust Frameworks model

The OITF model "breaks apart" the centralized credit card association model into separate pieces in order to create an open market for each of these functions, as described below.

Trust Frameworks

The single most important element of the OITF model is the concept of a *trust framework*: a written specification of the policies to which a participant must conform in order to be trusted at a particular LOA or LOP.[2] This specification is written (and maintained over time) by a group of *policymakers* representing a *trust community*. Any group with online identity assurance requirements can be a trust community: governments, NGOs, industry alliances, academic networks, social networks, etc. See specific examples in the following sections.

In addition to the identity, security, privacy, and data protection policies required for LOA/LOP, a trust framework also specifies (or references other specs for):

- *Technical profiles*—precise descriptions of the technical requirements participants must follow for interoperability "on the wire".
- *Assessor qualifications*—the professional credentials, experience, and other requirements assessors must fulfill perform certifications at each LOA/ LOP.

[2] The concept of LOA—level of assurance—is now being complemented by the new concept of LOP—level of protection. See *The Open Identity Trust Framework Model* for more about LOP.

Trust Framework Providers

Once a trust framework has been specified, the policymakers may contract with one or more *trust framework providers* (TFPs) to administer it. The job of the TFP is to:

1. Publish the trust framework so it is publicly accessible.
2. Accept applications from assessors who have the qualifications the trust framework requires to certify whether identity service providers (and in some cases relying parties) comply with the trust framework requirements.
3. Accept applications from identity service providers (and in some cases relying parties) who are successfully certified by a Listed Assessor.
4. Publish updates to the trust framework as it is revised, and periodically renew certifications of participants as required by the trust framework.

Assessors

In the OITF model, the TFP neither makes the trust framework rules, nor makes the judgment call about who complies with those rules. The former is the job of the policymakers who author the trust framework, and the latter is the job of *assessors*: professionals in the business of IT and legal/policy compliance auditing. The job of the TFP is to list assessors who meet the IT compliance auditing requirements of a particular trust framework at a particular LOA and/or LOP. Once listed, identity service providers and relying parties may choose—and negotiate pricing with—the assessor who best meets their needs.

Auditors

To maintain trust over time, trust frameworks require not just initial assessments but also ongoing audits of participants—either on a periodic basis, a random basis, or when a dispute occurs. Once again, under the OITF model, this is the job of third-party professionals; in this case specialists in the field of compliance auditing. A particular trust framework may specify the requirements for auditor qualifications as well as how frequently audits need to occur and how the results should be published.

Dispute Resolution Service Providers

Even with assessments and audits, disputes may still occur. Again, to scale to very large numbers of participants, a trust framework needs to enroll third-party *dispute resolution service providers* (DRSPs)—in particular DRSPs that specialize in online dispute resolution. A trust framework may specify qualifications for DRSPs as well as the requirements for participants to use them online and/or offline.

OIX – The First Open Identity Trust Framework Provider

Having developed the model, the next step for the open identity industry was to instantiate a trust framework provider using this model. Following meetings at the Internet Identity Workshop in November 2009, the OIDF and ICF formed a Joint Steering Committee to study the best implementation options. In January 2010 both boards approved grants to fund the creation of a new non-profit organization called the Open Identity Exchange (OIX). It was formed as Washington State non-profit corporation, and in the United States will apply for 501(c)(6) tax-exempt status, however OIX is intended from the start to be an international organization, and it will assume the appropriate form in all relevant jurisdictions.

In addition, members of OIDF and ICF including Booz Allen Hamilton, CA, Equifax, Google, PayPal, Verisign, and Verizon agreed to become founding members of OIX.

OIX Membership

To keep the trust framework participant process as simple and lightweight as possible, OIX has just two classes of membership:

- *General Members* include all types and sizes of organizations that wish to participate in any role relative to any OIX-listed trust framework.
- *Executive Members* are General Members whose organization appoints an individual to serve on the OIX board.

The fees for becoming a General or Executive Member vary with the size and type of a participating organization. See the membership page of the OIX website.

OIX Listing Categories

Once an organization is either a General or Executive Member of OIX, it can apply for as many Membership Listings as it needs in any of the following OIX categories:

- Trust Framework
- Identity Service Provider
- Relying Party
- Special Assessor
- Assessor
- Auditor
- Dispute Resolution Service Provider

For a Trust Framework, the member's proposed listing must meet the OIX Trust Framework Requirements,[3] including the OITF Principles of Openness.[4] In all other

[3] These are currently under development by OIX.
[4] See section V of *The Open Identity Trust Framework Model*.

listing categories, the member must meet the requirements specified by the applicable trust framework at the applicable LOA and/or LOP.

Assessor Qualification

Before Identity Service Providers or Relying Parties may be certified against a Listed Trust Framework, Assessors must first be qualified for it. In OIX, that job is performed by a *Special Assessor*: a party who both OIX and the Trust Framework publisher agree has the qualifications and experience to evaluate other Assessors for that trust framework. Note that, to avoid conflicts, a Special Assessor may not also serve as a Listed Assessor for the same trust framework.

Identity Service Provider and Relying Party Certification

Once Listed Assessors have been established for a particular trust framework, OIX members may apply to become Listed Identity Service Providers (and, if LOP are specified, Listed Relying Parties) using the following process:

1. First, the member must prepare the evidence that it meets the trust framework's requirements at the desired LOA or LOP.
2. Second, the member must undergo assessment by a Listed Assessor.
3. Once assessment is successful, the member may submit a Membership Listing Application Form to OIX.
4. Once OIX has verified the Listing Application Form information, the listing will be published in the OIX Listing Service.

The OIX Listing Service

The ultimate value OIX delivers is a publicly-accessible online registry of all of its listed trust frameworks and the OIX members listed for each trust framework in each role it defines, at each LOA and/or LOP it defines, and for each technical profile it defines.

The OIX Listing Service is designed to be both human-readable and machine-readable. This means that for people, it represents a real-time picture of the online trust ecosystem and the open market for identity assurance and protection services. And for machines, it represents an authoritative source of the metadata necessary to verify the certification status of an identity service provider or relying party with regard to any particular trust framework, any particular LOA or LOP, and any particular technical profile.

Example OIX Trust Frameworks

US ICAM

The first example OIX trust framework was developed in conjunction with the U.S. GSA on behalf of the Identity, Credential, and Access Management (ICAM) subcommittee of the U.S. CIO Council. Designed to meet the first of the four LOAs defined by the ICAM *Trust Framework Provider Adoption Process* (TFPAP),[5] the OIX US ICAM LOA 1 trust framework[6] was approved by ICAM on 15 February 2010 and went operational on 3 March 2010.

As the introduction to the TFPAP explains:

> *To support E-Government activities, Identity, Credential, and Access Management (ICAM) aims to leverage industry-based credentials that citizens already have for other purposes. In order to ensure these credentials are trustworthy, the government requires a mechanism to assess these credentialing processes against federal requirements as codified by Office of Management and Budget (OMB), National Institute of Standards and Technology (NIST), and General Services Administration (GSA)… This approach enables a scalable model for extending identity assurance across a broad range of citizen and business needs.*

In short, the US ICAM LOA 1 trust framework enables U.S. federal agency websites, such as the National Institute of Health (NIH), the National Library of Medicine (NLM), and the Library of Congress (LOC), to begin accepting OpenID and Information Card credentials from private-industry providers such as Google, PayPal, Equifax, Verisign, and Verizon. This is illustrated in Figure 4.

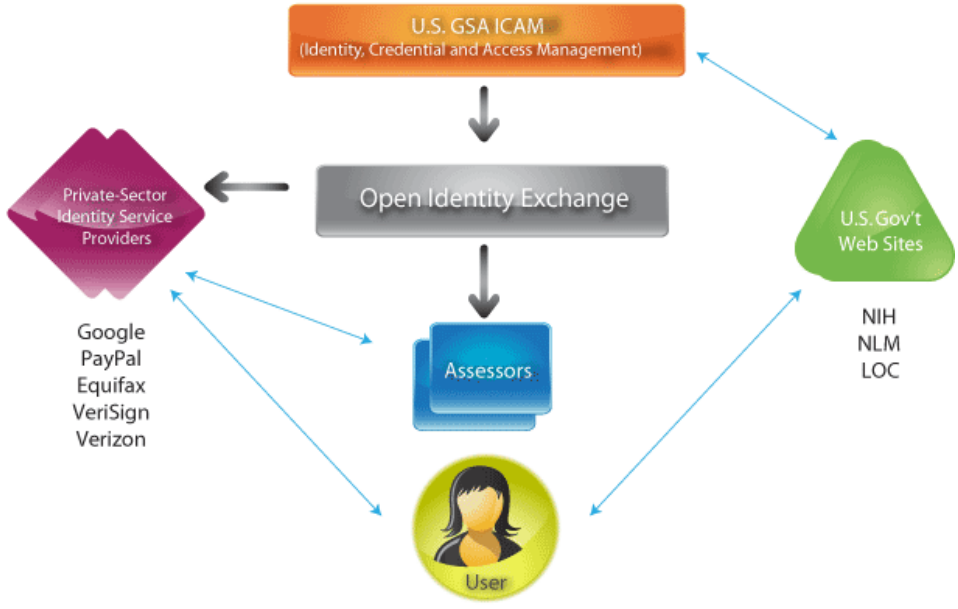

Fig. 4: Participants in the OIX US ICAM LOA 1 trust framework

[5] http://www.idmanagement.gov/documents/TrustFrameworkProviderAdoptionProcess.pdf

[6] http://www.openidentityexchange.org/sites/default/files/oix-us-icam-loa1-tfp-assessment-package-2010-02-12.pdf

Note that under this particular trust framework, federal agencies acting as relying parties already have a direct legal relationship with the U.S. government. So even though the TFPAP requires relying parties to protect identity data, it is not necessary for them to undergo OIX certification as relying parties.

PBS Public Media

While the U.S. ICAM example illustrates that governments are natural trust communities, there are also many other public organizations that can serve in this role. A prototypical example is the U.S. Public Broadcasting System (PBS) affiliate network. In addition to increasing audience involvement and integrating television and online content, PBS would like to build subscriber relationships, streamline donations, and offer special "members only" online features by having people log in securely when they visit PBS-related websites. PBS can do this with the public media trust framework illustrated in Figure 5.

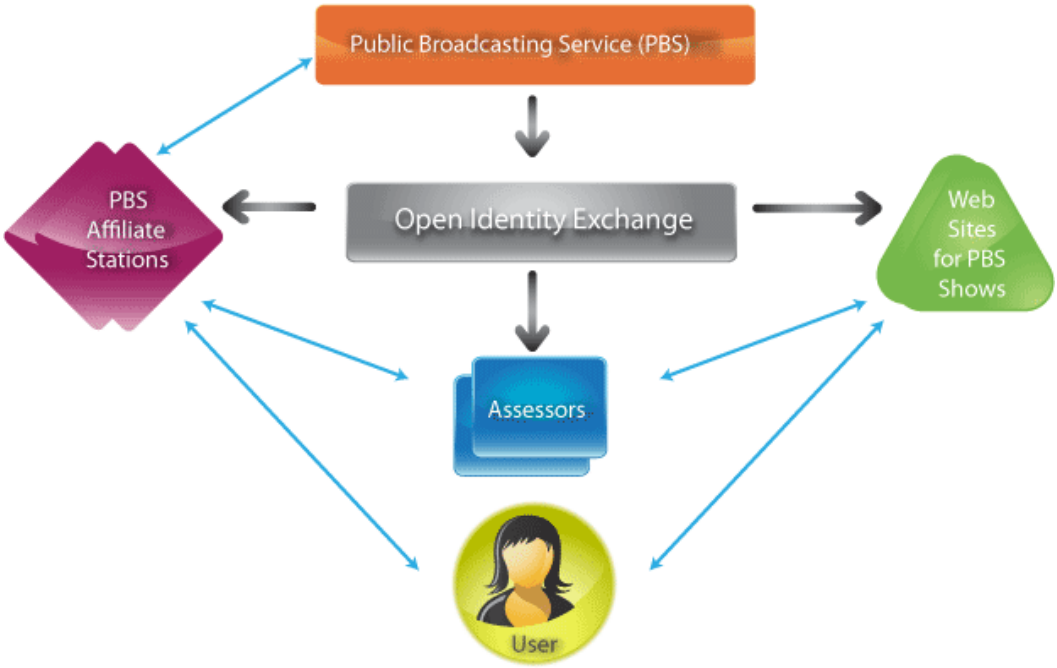

Fig. 5: Participants in the PBS public media trust framework

This trust framework will enable public television viewers to register with their local PBS affiliate station, such as WGBH in New York, WTTW in Chicago, or KCTS in Seattle, and sign up for a PBS OpenID or Information Card. This credential will then make it easy to login to any PBS-affiliated sites, prove you are a paid-up member, personalize the site, access special features, and make donations. It can even make it easier for children to prove they are PBS kids for safe access to popular PBS children's show sites such as Sesame Street®, Arthur®, and Curious George®.

More details about this trust framework will be published soon—see the PBS Public Media Trust Framework page of the OIX website.

National LIDB Forum

Other trust frameworks may come entirely from the private sector. An example is the Line Information Database (LIDB)[7] Forum, a national association of telecommunications companies with decades of experience in phone system interchange and billing applications. Recent government regulations allow new applications to use subscriber data for fraud prevention and other identity-centric applications. However the lack of open standards and industry-certified best practices has led data aggregators to create an estimated half-billion dollar grey market in cached subscriber data without adhering to fair information practices.

To address this problem, AT&T, Telecom Network Specialists, and other LIDB members are now considering an OIX trust framework for subscriber identity information as illustrated in Figure 6.

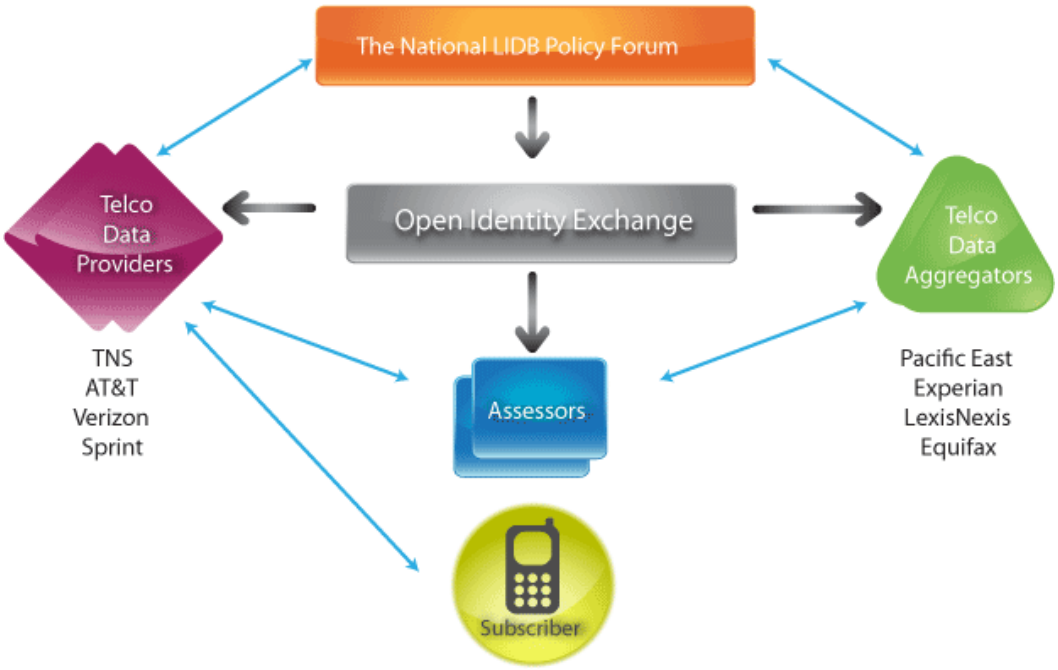

Fig. 6: Participants in the LIDB trust framework

Using this trust framework, LIDB members would act as the identity service providers holding private subscriber data "in trust". Relying parties would include merchants, credit bureaus, governments, and others that are willing to comply with the data protections specified in the LIBD trust framework, for example prohibitions against reselling or aggregating data. Note that under this trust framework relying parties will be explicitly certified by OIX-qualified assessors.

[7] Line Information Database is used by traditional telephone companies to store and retrieve Caller ID records. Local phone switches, also known as Class 5 switches, use SS7 signaling protocol to query these centralized databases and pass this information during call set up.

A Race to the Top: Benefits of the OIX Open Market Model

When designing policy mechanisms, regulators often speak of trying to create a "race to the top"—incentives that reward good market behavior in a virtuous cycle. This is a very conscious goal of OIX, as explained in this section.

Survival of the Fittest Trust Frameworks

Today, most identity, security, and privacy policies are either: a) site-specific (apply at the level of a single site), or b) jurisdiction-specific (apply within one regulatory jurisdiction). What trust frameworks do is introduce a new option: *portable* identity policies. In other words, the same way technologies like OpenID and Information Cards make identity information portable across different sites, trust frameworks make identity policies portable across different trust communities.

The result is an *open market for policies*: trust frameworks competing with each other in order to give websites and users greater choice and control over the policies that will apply to their interactions. In this dynamic, there are no losers, only winners: trust frameworks that produce superior balances between the levels of assurance sought by relying parties and the levels of protection sought by users and identity service providers.

Market Pricing

The second way OIX creates a race-to-the-top is treating each the roles in the OITF trust framework model as its own market. This begins with TFPs, who compete with each other to attract trust framework business. Next come assessors, who compete with each other for the business of certifying identity service providers or relying parties for different trust frameworks at different LOA and LOP. Then come the identity service providers and relying parties, who compete with each other across different trust frameworks to offer the best identity management services and most attractive data protection terms. And final auditors and DRSPs compete for auditing and dispute resolution business from participants across many different trust frameworks.

All of this competition means more choices, better prices, and higher quality services throughout the ecosystem.

Economies of Scale

As other Internet infrastructure has shown (routing, hosting, domain names), standardization of network services leads to powerful economies of scale. This may be even more pronounced with an OITF trust framework ecosystem because the economies are not just of *volume*, but also of *harmonization*. In other words, a successful trust framework will first produce economies of scale simply by standardizing what all participants must do to comply, driving down implementation, assessment, auditing, and ultimately even dispute resolution costs.

But this is only the first order effect. The second order effect is that the more successful a trust framework is, the more its policies will influence (or be directly referenced by) those of other trust frameworks to follow. In this respect each successful trust framework becomes a "carrier" of best practices throughout the market, encouraging their adoption much more quickly than conventional techniques.

Serving the Long Tail

Harmonization does not mean commoditization. One of the most distinguishing features of identity interactions is their very high sensitivity to context. This means no matter how popular certain trust frameworks become, there will never be "one size fits all". Rather the distribution is likely to follow a power law where a small number of trust frameworks are widely adopted and a much higher number have more limited distribution.

The high number of trust frameworks and trust framework participants in the "long tail" are particularly important because they represent the great diversity of contexts and policies that are necessary for a healthy online ecosystem. For this reasons the founders and members of OIX are committed to ensuring that its pricing and policies are designed to support all segments of the open identity market from the head to the tip of the tail.

For More Information

OIX was formally announced at the 2010 RSA Conference and is growing quickly. We invite your input and participation as we continue to lay the foundation for this next layer of online identity infrastructure. For more information please visit the OIX website at www.openidentityexchange.org or contact:

Don Thibeau **OIX Board Chair** don@openidentityexchange.org *202.841.8222*	**Drummond Reed** **OIX Acting Executive Director** director@openidentityexchange.org *206.618.8530*
Scott David **OIX Counsel** scott.david@klgates.com *206.715.0859*	**John Ehrig** **OIX Program Manager** jehrig@inventures.com *925.216.1552*

