Open Trust Frameworks for Open Government:
Enabling Citizen Involvement through Open Identity Technologies

Table of Contents

Executive Summary

Open government requires a way for citizens to easily and safely engage with government websites. *Open identity technologies*—specifically OpenID and Information Cards—fit this bill. They make it easier and safer for citizens to register, login, and when necessary share personally identifiable information across different websites and services. To bring open identity technologies and open government together, the OpenID Foundation and the Information Card Foundation are working with the U.S. General Services Administration to create *open trust frameworks* for their respective communities.

These frameworks, based on the model developed by the InCommon federation for higher education institutions, will enable government websites to accept identity credentials from academic, non-profit and commercial identity providers that meet government standards. These standards are critical as they represent the government's resolution of the challenging and often competing issues of identity, security, and privacy assurance. Open trust frameworks not only pave the way for greater citizen involvement in government, but enable even stronger security and privacy protections than those typically available offline.

A White Paper from the OpenID Foundation and Information Card Foundation

by Don Thibeau*, Executive Director*, OpenID Foundation and Drummond Reed, *Executive Director,* Information Card Foundation

10 August 2009

Introduction

Open Government

On his first full day in office, United States President Barack Obama issued a Memorandum on Transparency and Open Government.[1] Valerie Jarrett, Senior Advisor to the President, said, "This is an historic call to action – one that will help us achieve a new foundation for our government – a foundation built on the values of transparency, accountability and responsibility."[2]

The United States is not alone in moving towards this new political goal, which Wikipedia defines as:

> ***Open government*** *is the political doctrine which holds that the business of government and state administration should be opened at all levels to effective public scrutiny and oversight.*[3]

Open government is more than just publishing government proceedings and holding public meetings. The real goal is increased citizen participation, involvement, and direction of the governing process itself. This mirrors the evolution of "Web 2.0" on the Internet—the dramatic increase in user-generated content and interaction on websites. These same social networking, blogging, and messaging technologies have the potential to increase the flow of information between governments and citizenry—in both directions. However, this cannot come at the sacrifice of either security or privacy. Ensuring that citizen/government interactions are both easy and safe is the goal of a new branch of Internet technology that has grown very rapidly over the past few years.

Open Identity Technologies

Just as certain activities in the physical world—driving a car, flying in an airplane, applying for a mortgage—require identity credentials, so do certain activities in the digital world. Until recently, however, digital identity technologies were largely confined to *closed systems*, i.e., systems that only had to cater to a defined population of known users, such as corporate or university networks, or individual websites. These closed networks are in a position to dictate their own requirements for trusted transactions.

The rise of the Internet and the Web—interconnecting millions of different websites and systems—demands new digital identity solutions that "open up" closed systems to qualified users from anywhere on the Internet. The first open standard in this area was SAML (Security Assertion Markup Language), developed by the OASIS SSTC

[1] http://www.whitehouse.gov/the_press_office/Transparency_and_Open_Government/
[2] http://www.whitehouse.gov/blog/09/05/21/Opening/
[3] http://en.wikipedia.org/w/index.php?title=Open_government&oldid=293620033

(Security Services Technical Committee)[4] with key contributions from the Liberty Alliance Project.[5] SAML established a common XML (Extensible Markup Language) vocabulary for the exchange of authentication and authorization information across trust boundaries. It has gained significant adoption in vertical markets and communities such as universities and wireless carriers where the participants generally have pre-existing trust relationships of some kind.

However SAML was not optimized for "wide open" trust networks, such as the Internet, where the parties to a digital identity interaction may not have any pre-existing trust relationship. To fill this need, two new *open identity technologies* have been developed:

- **OpenID** is a Web registration and single sign-on protocol that lets users register and login to OpenID-enabled websites using their own choice of OpenID identifier. With OpenID, a user can operate their own OpenID service (such as on their blog), or they can use the services of a third-party OpenID provider (for example, most major Web portals, such as AOL, Google, and Yahoo, now offer OpenID service). One key advantage of OpenID is that it requires no client-side software—it works with any standard Internet browser. OpenID is a community-developed open standard hosted by the non-profit OpenID Foundation.[6]
- **Information Cards** are a new approach to Internet-scale digital identity in which all of a user's identities, whether self-created or from third party identity providers (e.g., employer, financial institution, school, government agency, etc.) are uniformly represented 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". Cards may be exchanged with websites using a variety of protocols and formats. All card selectors support at least the *IMI protocol* developed by the OASIS IMI TC,[7] however Information Cards are now being adapted to other protocols as well (including OpenID). Information Card technology is developed and promoted by the non-profit Information Card Foundation.[8]

OpenID and Information Cards are often called "user-centric" or "user-driven" identity technologies because they put the user in control of all identity-based interactions. Specifically, they put the user in the middle of connecting two parties to a digital identity transaction:

- The *relying party* (also called a *service provider*) is the website or service that requires a security credential from the user.
- The *identity provider* is the website or service providing a security credential (such as an authentication or authorization assertion) on behalf of the user. (Note that in the case of self-asserted identity credentials, the user is his/her own identity provider.) This security credential may contain a set of *attributes* (also called *claims*) that the identity provider asserts about the user, e.g., name, address, age, gender, etc.

[4] http://www.oasis-open.org/committees/security/
[5] http://www.projectliberty.org/
[6] http://www.openid.net/
[7] Identity Metasystem Interoperability Technical Committee, http://www.oasis-open.org/committees/imi/
[8] http://www.informationcard.net/

Despite their differences, OpenID and Information Cards both provide the same top-level benefits to users and websites:

- *Simplified login* reduces the many confusing username/password options users navigate today to a few secure methods standardized across all sites.
- *Identity portability* lets users "carry" the same identity credentials across different websites and services, just as people can now keep the same cell phone number across different wireless carriers.
- *Automatic data exchange* lets users register at a website or fill out a web form as easily as they swipe a credit card to make a payment today.

Bringing Them Together

Open identity technologies and open government fit together perfectly. The government gains efficient, market-driven digital identity solutions for open government initiatives, and the market gains a valuable new set of open-identity-enabled websites and applications. However bringing the two together requires more than just the government installing new software—that addresses only the technical part of the equation. It does not solve the problem of how government websites and applications can begin trusting credentials issued by academic, non-profit, and commercial identity providers with whom the government has no direct trust relationship, but with which citizens have established trust relationships that have been in place for years or even decades.

This is the same problem the credit card industry needed to overcome a half-century ago, when credit card readers had become standardized but merchants still needed to be able to verify that a particular credit card issued by a bank could be trusted. The solution was the introduction of credit card networks such as Visa, MasterCard, and American Express that could verify the relationship between a cardholder, a bank, and the trust network. A similar solution is needed now for open government.

Open Trust Frameworks

Trust Frameworks

In digital identity systems, certification programs that enable a relying party to trust the identity, security, and privacy assurances from an identity provider are called *identity assurance frameworks*, or more generally *trust frameworks*. Organizations that operate such programs are called *trust framework providers*.

This begs the question: why does a government need external identity providers at all? Why doesn't it just act as its own identity provider? After all, most governments already issue credentials for identifying citizens–for example the U.S. Social Security Administration began issuing Social Security Numbers (SSNs) starting in 1936.

It turns out there are a number of reasons why this is not desirable:

- *Data centralization and privacy.* As a rule, citizens would like to see fewer, not more, centralized government databases.
- *Duplication of private industry effort.* Even if the government did serve as an identity provider, it would not meet the needs of many segments of private industry, whose requirements are market-driven. Thus the government would only be duplicating functionality already deployed in the market.
- *Lack of market forces to drive efficiencies and innovation.* Digital identity tools, technologies and techniques are evolving rapidly to keep pace with Internet and Web 2.0 innovations. Private industry is able to incorporate these changes more efficiently than government.
- *Lack of choice.* Just as the government does not dictate which computer or operating system a citizen must use, the government should leave citizens free to choose the identity technology and identity provider with which they are most comfortable.
- *Cost savings.* Private industry can deliver these services at a lower cost than the government.

A Working Example: The InCommon Federation

What does a private trust framework look like? An excellent example is the InCommon federation.[9] InCommon was an outgrowth of the Shibboleth open source single sign-on project started at Internet2 in 2000.[10] The goal of Shibboleth was to lower barriers to learning and research by enabling students, faculty, and researchers from one higher educational institution to log in and access resources such as libraries and papers at other institutions.

Participants in Shibboleth realized that while SAML gave them the technical ability to share identity credentials, they still needed a way to verify these SAML messages were coming from a participating institution. They also needed to ensure participating institutions were maintaining minimum levels of security and privacy practices to keep all participants protected—every trust network is only as strong as its weakest link.

The solution was to create a SAML federation called InCommon. InCommon currently serves a community of over 3 million users, with 110 higher education participants, 6 government and non-profit agencies, and 41 sponsored service provider partners,[11] and is growing at the rate of 100 percent per year.

Given this success, it is no surprise that the InCommon federation is the first non-governmental trust framework to be considered for certification by the U.S. government. However, the higher education community only encompasses a fraction of the users who may need access to government resources. Are there other trust frameworks that can encompass the rest?

[9] http://www.incommonfederation.org/
[10] http://en.wikipedia.org/wiki/Shibboleth_(Internet2)
[11] http://www.incommonfederation.org/participants/

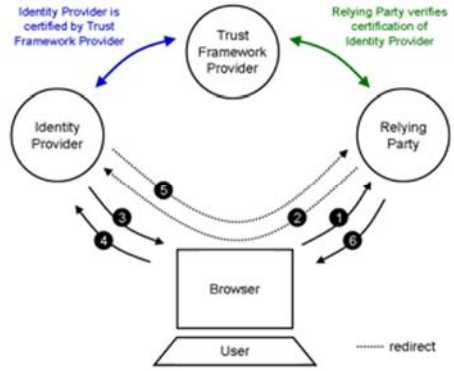

Fig 1: Where trust framework providers fit into the OpenID 2.0 protocol

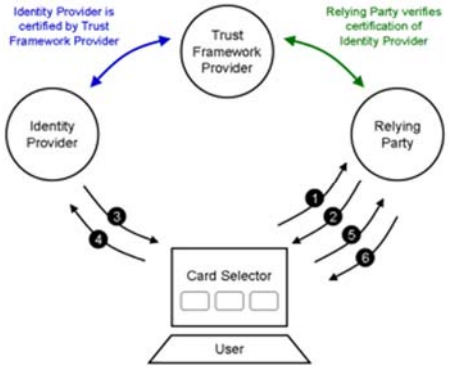

Fig 2: Where trust framework providers fit into the IMI 1.0 Information Card protocol

Trust Frameworks for Open Identity Technologies

OpenID and Information Cards are unique in that they provide solutions to Internet-scale digital identity that do not require pre-existing trust relationships between identity pro-viders and relying parties. But how can a trust framework operate at this scale?

The answer lies in the communities that have formed around each technology. The OpenID Foundation (OIDF) was formed in 2007 to support and promote the use of the OpenID protocol. It uses a "community governance" model, where the majority of directors are elected by the community, and a minority are representatives of companies who want to advance and promote the technology.

The Information Card Foundation (ICF) followed suit in 2008, adopting a similar community governance model. One difference is that the ICF does not sanction technical protocol work directly, but contributes to established Internet standards bodies, such as the previously-mentioned IMI Technical Committee at OASIS.

In both cases, the foundations exist to help their members collectively address the challenges necessary for OpenID and Information Cards to become Internet-wide digital identity standards. Their initial focus has been technical interoperability, user experience, and market education. However a natural next step is trust frameworks, for the simple reason that interoperability at the technical layer is a prerequisite to interoperability at the business layer. Technology-based trust frameworks are literally the "shortest path between two points"—point A being where two parties can interoperably exchange identity credentials, and point B being where a relying party can trust the credentials from a particular identity provider. Figure 1 illustrate this conceptually for the OpenID protocol and Fig. 2 for Information Cards using the IMI 1.0 protocol.

Besides neutrality, trust frameworks operated by industry non-profit associations have three other key advantages:

- *They give users a choice of technologies and providers.* This encourages participation and innovation by a variety of companies and non-profit organizations worldwide.
- *They can be operated as a cost center, not a profit center.* This helps prevent cost from being either a barrier to entry or a barrier to innovation, especially in the early stages of the development of this trust fabric.
- *They are the centers of industry-driven innovation.* Each foundation is a driver of a rapidly evolving social web technology that stands at the intersection of policy and practice for Internet scale digital identity, so they are well-positioned to tackle the social, business, and policy implications of open trust frameworks.

With the U.S. government's encouragement, and recognizing their mutual interests in developing open trust frameworks, the OIDF and the ICF began collaborating on this activity in the spring of 2009, with the goal of having their respective solutions operational as soon as practical. It is our hope that this leading edge collaboration may help similar efforts among other communities in the open identity ecosystem.

An Open Market Approach to Trust Frameworks

Whereas InCommon serves higher educational institutions, laboratories, and their associated service providers, the OIDF and ICF trust frameworks are intended to serve anyone using their respective open identity technologies. Just as these technologies were developed in an open market, the OIDF and ICF believe their trust frameworks should be driven by the open market. This means satisfying the following requirements:

1. *Open to all providers.* Any legal entity that can meet the technical and operational requirements of the trust framework should be able to apply and receive certification—OIDF or ICF membership should not be required.
2. *Open to provider self-certification.* For maximum flexibility and efficiency, the programs should permit an identity provider to self-certify if they prefer this approach. This self-certification is then audited by the provider's choice of any qualified auditor registered with each foundation.
3. *Open to auditor self-selection.* To ensure choice and competition, auditing should not be restricted or outsourced on an exclusive basis, but open to any organization that meets widely-accepted industry qualifications for information technology auditing and certification.
4. *Open to change and evolution.* In digital networking, the one certainty is change. The more lightweight and flexible the framework, the faster and more easily it can accommodate new requirements, be they technical, political, or economic.

Thankfully, most of these principles are already reflected in the design of the InCommon assurance rogram, which is why it is the starting point for the open trust frameworks under development by OIDF and ICF.[12]

[12] While we believe these principles can ensure openness, they cannot by themselves ensure fairness, i.e., the market will determine service fees and may favor organizations of a certain size or with in-house auditing resources at the ready. However the trust frameworks as envisioned herein will have no built-in bias.

Assembling this New Layer of Infrastructure

InCommon's experience gives the OIDF and ICF a model for implementing open trust frameworks that can proceed relatively quickly. Following are the key steps:

Certifying the Trust Frameworks

The first step is for the U.S. government to certify the InCommon, OIDF, and ICF trust frameworks for our respective communities. To do this, the General Services Administration (GSA) has created a Trust Framework Adoption Process (TFAP) that specifies the requirements for trust framework providers (TFPs).[13] GSA's requirements enable TFPs to certify identity providers at the four different assurance levels defined by the National Institute for Technology Standards (NIST) and the U.S. Office of Management and Budget (OMB).

This process is well underway.

Certifying Identity Providers

Once the trust frameworks are certified, each foundation can begin accepting certification applications from identity providers in its community. A number of potential applicants, both members and non-members, are currently preparing for this process.

Each provider may choose to perform its own self-certification or use external resources to perform this step. In either case, the provider then works with its selected registered auditor to perform the required self-certification audit. When both the self-certification and the auditor's report are submitted to the respective foundation, the foundation will verify the documents are authentic, complete, and properly executed.

Once these steps are performed, the identity provider is certified and the appropriate metadata reflecting this certification will be registered with the GSA and the foundation's own public (website) certification registry. These registries will be accessible to the online community at large and to any relying party for verification of identity provider certification status.

Monitoring Compliance

An operating trust framework is not a static entity. Certification requirements are updated as technology and policy evolve, and certifications must be renewed on a periodic basis (typically annually). The registry must also quickly reflect changes in certification status. Should an identity provider voluntarily submit for decertification, or if third party evidence demonstrates that the provider no longer meets the certification requirements, a provider may be decertified. The provider will be notified and the metadata registry updated. The operating policies of the registry and the cache refresh policies of the parties relying on this registry will determine how quickly the decertification is effective (normally within a few hours).

A decertified provider may reapply for certification once they can prove they have addressed the deficiencies and again meet all technical and administrative requirements. The foundations may choose to empanel a review committee of independent subject matter experts to help arbitrate protests or disputes should the need arise.

13 http://www.idmanagement.gov/documents/TrustFrameworkProviderAdoptionProcess.pdf

Realizing the Benefits

In the *Introduction*, we discussed the general benefits of OpenID and Information Cards as open identity technologies. In this section we enumerate the specific benefits of bringing them together with open government through open trust frameworks.

Security

Open trust frameworks based on OpenID and Information Cards should not merely meet the same level of security as standalone, non-federated identity systems; they should improve on it. Regardless of which technology is used, the security benefits of this infrastructure include:

- *Consistent, audited security policies.* By certifying providers against known requirements for different levels of assurance, open trust frameworks are an agile way of ensuring industry-standard security practices are being followed regardless of the underlying technology or protocol.
- *Dramatically reduced credential sharing.* Most people use the same usernames and passwords at different websites simply because it is easy to remember. Open identity technologies solve this problem by automatically generating identifiers so the user isn't forced to manually store separate credentials at separate sites.
- *Simplified user trust decisions.* Just as credit card networks like Visa, MasterCard, and American Express have made it much easier for consumers to know when a bank or a merchant is a member of a trust network, open trust frameworks will help Internet users recognize trusted identity providers and relying parties.
- *Leveraging strong authentication.* Today, every site or system that requires strong, multi-factor authentication has to deploy its own solution. Not only is this expensive, but it requires users to carry or learn an increasing number of second factor tokens.[14] OpenID and Information Cards enable any number of relying parties to leverage the multi-factor authentication options available from the user's chosen identity provider.

One area where OpenID and Information Cards using the IMI protocol differ is *anti-phishing protection*. Phishing is when a malicious site impersonates a real site to trick users into divulging security credentials such as their username and password. Because OpenID does not require any client-side software—it works with unmodified browsers—it can do little to protect against such attacks.[15] By contrast, Information Cards using the IMI protocol requires client-side software—the card selector. This can provide two types of anti-phishing protection: first, the selector can warn a user whenever he/she is asked to submit identity credentials to a relying party they have never visited before; and second, even if the user is tricked into submitting an Information Card to a malicious party, the resulting security credential does the attacker no good because it is customized for use only at that fake site. It cannot be replayed against the legitimate relying party.

Privacy

Stronger forms of identity authentication and security often come at the sacrifice of privacy. However deployment of OpenID and Information Card technology according to the GSA assurance profiles can achieve both. Specifically, both technologies can enhance privacy in the following ways:

- *Non-correlatable identifiers.* Although there is a misperception that OpenID means using the same identifier at every website, in fact OpenID 2.0 supports the automatic generation of pseudononymous identifiers when desired. This feature is designed into the GSA OpenID assurance profile to increase privacy. For its part, the IMI 1.0 protocol specifies automatic generation and maintenance of PPIDs (private personal identifiers) for all Information Card interactions. This avoids the use of any protocol-level correlatable identifiers regardless of the GSA assurance level.
- *Automatic minimum disclosure*. Most people, when asked for personal information, will supply everything requested, even when it is not required. Most automatic form-fill programs for the Web do the same thing. By contrast, intelligently designed identity providers (server-side) and card selectors (client-side) can do just the opposite: default to sending only the minimum personal information required, and require conscious manual action by the user to send additional optional information.
- *Personal privacy management and auditing.* OpenID and Information Cards, in the hands of privacy-conscious software designers and identity providers, can for the first time give users the ability to review when, where, why they have shared personal information, and potentially to correct and/or withdraw it. This is the same ability many companies have enjoyed for years with CRM (Customer Relationship Management) systems, only now this same corrective ability is available to the customers themselves.[16]

[14] Much like consumers are being asked to carry an ever-growing number of store loyalty cards on their key chains or wallets.

[15] Special browser plug-ins, such as Seatbelt from Verisign, have been developed to address this problem.

[16] This capability has been dubbed VRM (Vendor Relationship Management). See http://projectvrm.org.

OpenID and Information Card technologies also raise a new privacy concern: the ability for third-party identity providers to track and correlate user activities across any number of websites and services. Again, this is an area where the protections offered by OpenID and Information Cards using IMI 1.0 differ. With OpenID, one solution is to for a user to operate their own OpenID service, such as from their blog. Or, if a third-party OpenID provider is desired, anti-correlation can be enforced via contractual, behavioral, and/or regulatory controls.

Because it has an active client, Information Cards using the IMI 1.0 protocol offer a different anti-correlation solution: letting the user's own card selector track which relying parties receive which Information Card credentials so this information remains hidden from the identity provider. Note that this is currently only possible when the identity provider does not need any information about the relying party (such as its public key certificate); however this mode can be requested by the relying party and enforced by the user's card selector whenever possible.

Cost Savings

Sharing identity infrastructure saves costs for everyone. From the government's standpoint, it means not having to design, deploy, and maintain independent identity systems for different domains and applications. It also eliminates the need to become an identity provider except where the government is actually the authoritative source of the required identity information. While relying on non-governmental identity providers and trust frameworks still represents a cost to the government, particularly at higher assurance levels, it will be a fraction of what it would otherwise cost to implement.

This cost savings is not limited to the government, either: every relying party, regardless of industry or market segment, can enjoy this same benefit. Open trust frameworks, like the open Internet and open Web, produce the same economies of scale for identity and trust verification as the credit card networks produced for credit verification.

Reuse, Extension, and Adaptation

Though the initial problem these open trust frameworks solve is U.S. governmental trust in private sector identity providers, there is nothing to prevent them from being used by any other government—or for that matter by any private community or application that needs identity assurance across a diverse population of Internet users.

Furthermore, if a community needs different assurance profiles than those specified by the GSA, these can be added to the trust frameworks and interested identity providers can be certified against them. Again, reuse of the same basic infrastructure further increases the cost savings and network effects for everyone.

Conclusion

Open government, to which the Obama administration is publicly committed and other governments are also starting to embrace, requires a way for citizens to easily and safely engage and interact. OpenID and Information Cards offer an open standard means of achieving this via the Internet and other public networks, enabling online identity interactions to be both *easier* and *safer*.

However putting the two together requires trust frameworks that enable government websites and applications to accept identity credentials from academic and commercial identity providers.

InCommon provides a model for how this is already working today to serve the worldwide higher education and research community. The OpenID Foundation and Information Card Foundation are adapting this model to create open trust communities that can serve users and relying parties Internet-wide. In particular the OIDF and ICF are developing trust frameworks in which open market forces are used to ensure that the trust framework is as fair and efficient as possible.

These open trust frameworks give citizens two powerful benefits: a *choice* of open identity technologies and providers and *control* over where and how their personal information is used.

This will make it easier and safer for citizens to be directly involved in open government initiatives using any government website or application that supports OpenID and/or Information Cards. It will also enable all parties to realize substantial security, privacy, and cost-savings benefits. Lastly, these frameworks can be reused, extended, and adapted by any community to provide the shared level of assurances needed to make cross-domain trust decisions.

The result will be an open ecosystem for identity and trust on the Internet that can work across all applications, communities, and borders. In much the same way the Internet and Web have benefited society at large, the pursuit of open government and open trust frameworks will benefit citizens everywhere and democracy itself.

The OpenID Foundation (OIDF) is a non-profit organization that promotes, protects and enables the development of OpenID technologies.

For more information contact:

Don Thibeau
Executive Director, OpenID Foundation
don@oidf.org

The Information Card Foundation (ICF) is an non-profit community of individuals and companies working together to evolve the Information Card Ecosystem.

For more information contact:

Drummond Reed
Executive Director, Information Card Foundation
director@informationcard.net

Mary Ruddy
ICF Certification Committee Chair
mary@meristic.com