KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

ISSUES FOR RESPONSIBLE USER-CENTRIC IDENTITY

November 2009 – Version 1.0

In light of the announcement of a series of federal pilots for federated identity providers, we have analyzed the governance and policy issues around creating a user-centric identity management system. Key questions must be answered in the process of creating an effective framework that can foster trusted relationships online. CDT believes that user-centric federated identity has great promise to make online interactions easier, more secure, and more easily controlled by the user if these questions are addressed properly.

One of the central challenges of the digital age is creating, managing, and sharing digital identities online. As online interactions become richer and more complex, individuals are asked to identify themselves increasingly often - using their name, their address, or simply an identification number to correlate their visits. In addition, services online are increasingly being offered subject to user authentication; for example, users can use a credit card to make a purchase or file their taxes online, as long as they can prove their identity. As the use of authentication increases, so does innovation around online identity. However, these innovations must be considered thoughtfully in order to ensure that they are protective of the user, building trusted online relationships.

The U.S. government is launching a series of pilot programs that will use third party user credentials to authenticate users to federal Web sites in order to provide a better user experience. Using third parties to authenticate users makes sense in many ways, allowing users to use credentials they already have (rather than yet another set of user name and password) and allowing agencies to free up development resources for other tools, instead of maintaining their own sign-on system. In order to work with the government, these third party identity providers must adhere to a trust framework that sets a minimum level of best practices for the identity provider. However, creation of robust trust frameworks for government use, as well as for general use, requires that identity providers and trust framework providers work together to answer a set of questions around the provision of identity and services online.

Background

In the digital context, identity is simply a claim or set of claims about the user, similar to the physical claim of a driver's license ("this person is allowed to drive according to this state") or a library card ("this person is allowed to borrow books"). This identification is often subject to authentication - that is, the process to verify that the identification is, in fact, true. The process of claiming identity, authenticating identity, and authorizing that identity to use certain services is known as Identity Management.

Traditionally, identity exchange has been a direct interaction between a user and the service provider. This model is evolving as Web services and Internet applications now frequently require new forms of identity information. Some of these new models for identity management place the user in the middle of an interaction between an identity provider and an online service. This method, called Federated Identity, allows service providers to rely on trusted third parties to authenticate users of their service. Often, this eases use for users by reducing the number of sign-in credentials they must remember.

Many of the federated identity technologies developed to address problems with traditional identity solutions fall under the loosely defined term "user-centric identity." This term refers to systems where users, rather than service providers, control their identity credentials. This is a closer metaphor to the offline world, where we carry a variety of identity documents issued by different authorities, and choose which identity credential or authenticator to present in each transaction. These new online systems must be designed with privacy and security as foremost concerns due to the often-sensitive nature of the information held by the identity provider.

User-centric federated identity systems have the potential to improve the security and privacy of authentication and services for users; however, if improperly designed, these systems can negatively impact users and prove a burden instead. CDT believes that user-centric federated identity has great promise to make online interactions easier, more secure, and more easily controlled by the user. There is skepticism from privacy and security advocates that user-centric federated identity will be implemented in ways that maximize the potential of these technologies for consumers, industry, and government. We hope to serve as advisors on policy matters in order to ensure that the promise of user centric federated identity is maximized as we move towards implementation of these federal government pilot programs.

User-Centric Identity

Whereas in traditional systems users directly exchange identity information with service providers, the relationships within a user-centric federated identity system is becomes more complicated:

1. The *trust framework provider* creates a trust framework with a set of minimum practices that must be upheld in order to be considered trusted within the framework, and evaluates identity provider practices against this framework.
2. The *identity provider* manages the user's identity information and provides authentication of the user to service providers.
3. The service provider, also referred to as the *relying party*, provides a service to the user, based on identity information provided by an identity provider.
4. The *user* registers his or her identity information with one or more identity providers and controls how that information is shared with service providers.

Central to the vision of these technologies is that there is no single central identity provider. There can be a variety of competing identity providers offering services tailored to particular needs of both users and relying parties. Robust competition in

this market will potentially give users greater choice and control over how they manage their personal information in online transactions. In some cases users themselves may act as the identity provider.

Figure 1: Traditional Identity Authentication

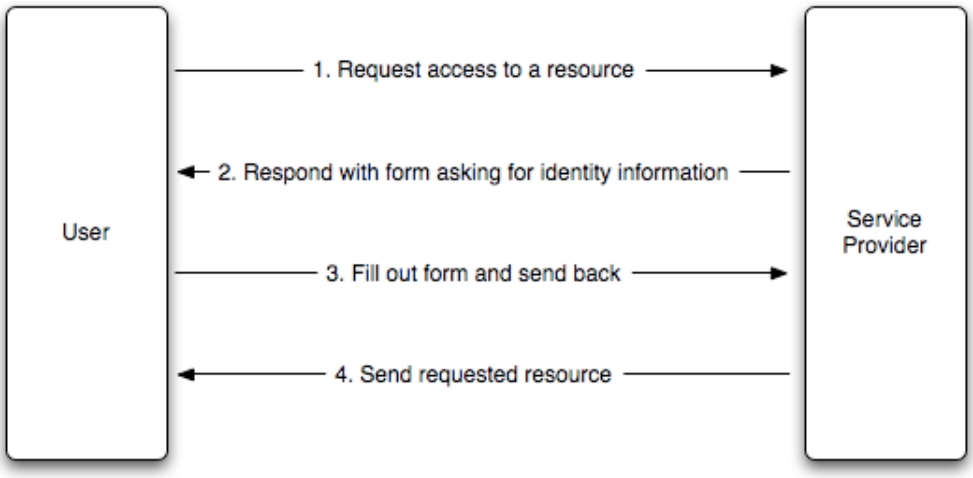
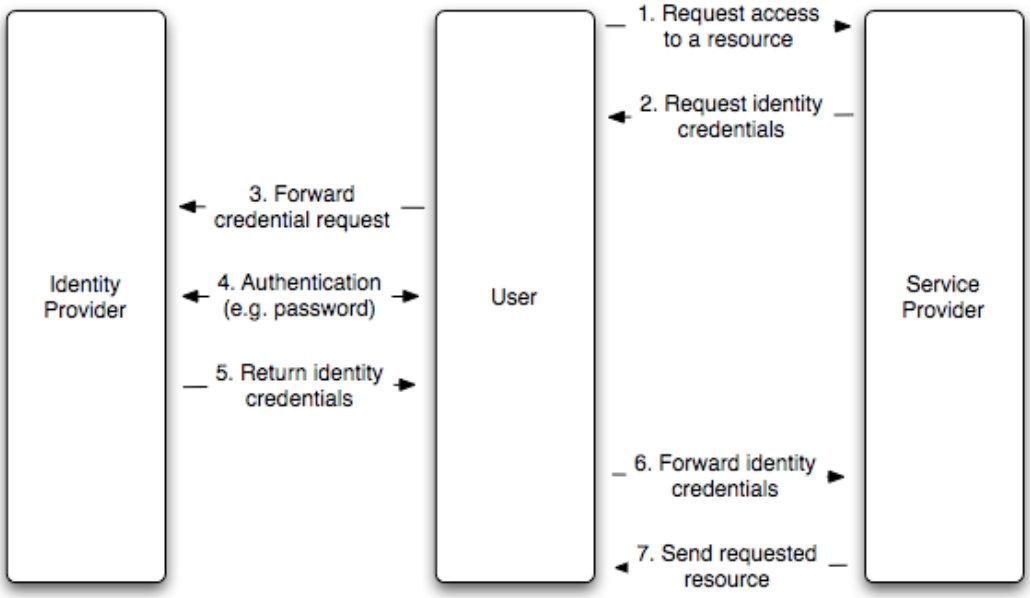


Figure 2: User-Centric Identity Authentication



In a user-centric federated identity transaction, a credential is passed between the identity provider, the user, and the service provider. This credential is a secure message stating “Identity Provider X certifies that the holder of the credential satisfies Y,” where Y might be “user name is ‘JohnDoe’,” or even “the user works for Widgets Inc.” This credential is useful to the service provider only to the extent that it trusts the identity provider. Low-sensitivity services might trust any identity provider that correctly follows the protocol outlined in a trust framework or identity schema. High-

sensitivity uses might require well-known identity providers that do offline verification of the data they provide.

Benefits and Liabilities in Federated Identity Management

Using a third-party identity provider has benefits for both the user and the service provider. The service provider is freed from the significant effort required to manage user accounts, verify identity claims, and reset forgotten passwords. Users benefit from not having to register with each new service provider, and not having to remember separate user names and passwords.

However, introducing a third party that uses personal information to interact with so many online services on behalf of the user introduces new privacy and security concerns. In order to benefit from user-centric identity systems, users must disclose personal information to identity providers and relying parties. The benefits of user-centric identity to both users and relying parties will be lost if users do not have sufficient confidence that their information will be protected against unauthorized use or disclosure (and confidence in avenues for redress to deal with subsequent harms that may flow). These risks apply not only to information provided by users to identity providers and relying parties, but also information collected from third parties about the user and transaction data about users generated as a result of their online activities. Without strong privacy and security protections, users are exposed to a host of harms---for example, identity theft, unauthorized account access, and embarrassment.

Third party management of personal information also raises key questions around how to best allocate legal obligations and liability among the parties to both encourage robust competition in this market and protect the privacy and security of user data. One category of potential liability centers on the misuse or unauthorized disclosure of user information. By using a third party to manage user information, relying parties may be freed from some legal requirements and liability. However, the identity provider may assume more liability and risk. Potential liability may arise where there is a faulty identification, faulty authentication, or failure to follow trust framework procedures. Users and relying parties can suffer harm and potential liability where a relying party acts on a faulty identity credential it thought was valid, or fails to act on a credential it believes is faulty. Users can also suffer harm when they are denied access or authorization to a service they are actually entitled to because of improper action by either the identity provider or relying party.

In addition, the relying party may still aggregate information about a user, in which case liability and legal requirements are not removed. In fact, additional burdens may be placed on the relying party as part of a trust framework or as part of a transaction with the trust provider, in order to ensure that the relying party does not require unnecessary information to be passed.

U.S. Government Pilots

The newest entrant into the user-centric identity field is the U.S. Government, having recently announced three pilot programs using user-centric federated identity

management to improve access to government information while leveraging existing credentials for users. These pilots will be held through the Center for Information Technology (CIT), the National Institutes of Health (NIH), and the U.S. Department of Health and Human Services (HHS).

The Identity, Credential and Access Management group (ICAM) has developed a set of schemas for the adoption of trust frameworks for use in government[1]. These trust frameworks will govern the operations of, policies of, and relationships between identity providers, users, and federal Web sites. Once ICAM and the GSA approve a trust framework, the trust framework may certify identity providers as compliant with their trust framework, and in turn federal sites involved with the pilot will be able to accept credentials from these identity providers.

Trust frameworks establish the conditions under which individual identity providers (and perhaps their relying parties) will qualify for participation in a federated system for collection, exchange, and authentication of user information. In addition, the trust framework determines how trustworthy a given credential is, determining what kinds of services it can authorize on federal Web sites. In order to be trusted by the government pilot, an identity provider must be operating as part of a trust framework approved by the ICAM Trust Framework Adoption Process. Currently, OpenID Foundation, Information Card Foundation, Kantara Initiative, and the InCommon Federation are active in this process. The trust framework provider must ensure that each identity provider that they certify is behaving within the bounds of the trust framework.

These trust frameworks are adopted based on the level of certainty that they can provide. The adoption process compares the trust framework to the applicable federal requirements, policies, and laws. As part of this adoption process, a Scheme Profile that determines how the federal government will use the identity profile created by each trust framework, how secure it is, and what level of authentication it can provide. Each Scheme Profile is then matched against the levels of assurance defined in OMB Memorandum 04-04[2], which sets out levels of assurance that are necessary for government transactions:

- Level 1: Little or no confidence in the asserted identity's validity (for example, used to personalize federal Web sites for users or allow participation in government discussions online; pseudonymous)
- Level 2: Some confidence in the asserted identity's validity (for example, changing an address of record)
- Level 3: High confidence in the asserted identity's validity (for example, submission of proprietary patent information, or disaster management information for first responders)
- Level 4: Very high confidence in the asserted identity's validity (for example, law enforcement criminal records databases or health records from the VA)

[1] Materials released by ICAM can be found at idmanagement.gov, including relevant memorandum.
[2] M-04-04 "E-Authentication Guidance for Federal Agencies" <
http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf>

Each of these levels is determined based on the information needed by the particular Web site or application, the importance and sensitivity of the services, and the potential harms.

While these government pilots are driving trust framework creation in user-centric identity, it is expected that User Centric Identity Systems will be used extensively for purposes unrelated to government sites. Accordingly, the development of these trust frameworks raises questions that go far beyond what minimum requirements the government might impose as a condition to treating a particular identity provider or trust framework provider as acceptable for access to government sites at any particular level of assurance.

Key Initial Policy Questions for User-Centric Trust Framework Providers

The direction that is taken on key policy questions in these trust frameworks for federal use may well shape the direction for the operations of user-centric identity for the near future. Key in the development of a trust framework is the creation of a set of minimum conditions that must be met by each participating identity provider, and how the trust framework will certify (and decertify) each provider. In addition, the responsibilities, obligations and liabilities of the trust framework provider, the identity provider, the relying party, and the user must be made clear. Establishing an appropriate set of rules around these minimum obligations can create trust for users, increase user adoption of these services, and make it significantly easier to establish relationships online.

There are several options for shaping an appropriate set of rules between the framework, the identity provider, the relying party, and the user. Traditionally, terms of service and privacy policies created and posted by Web sites define various rights and responsibilities of the Web site in regards to user data. Often, user responsibilities are also included. However, these terms and policies are rarely understood and do not address the obligations of or relationships to third parties.

Current privacy policies and terms of service are simply not effective for this kind of practice. Identity management across many Web sites carries new privacy risks and more data and information than other kinds of services, and users must be given greater control over their information.

Legislation or regulation might be used to establish mandatory practices among the members of a federated identity management. However, this approach would not deal well with the evolution of services online. Legislation and regulation should likely be the last resort if key players do not move promptly and responsibly to address privacy protections and key aspects of user-centric governance.

The provision of identity services via trust frameworks raises many policy questions. A promising way to resolve these issues would be for the Trust Framework to impose, as a condition of participation, some minimum terms that would govern the interactions among all three parties – the Identity Provider, the Relying Party and the User. Such mandatory contract terms might be made enforceable by each of the parties against the other, thereby reducing burdens on the trust framework provider.

One way or another, these will be addressed in the context of implementation decisions. These decisions will determine the level of risk to privacy and security for users and the types of liability and redress for potential harm that may exist for each member of the federated identity system.

Trust framework providers

1. *Admitting identity providers*: On what basis will the trust framework will certify identity providers as meeting a minimum standard? Will the assertions made by the identity provider be trusted, or will an audit of identity provider practices be performed? On what basis could a trust framework decline to admit a new member?
2. *Auditing identity providers*: If identity providers must be audited, who will do the audit, what independence criteria might apply, and to whom will the auditor owe an obligation?
3. *Showing compliance*: Will the framework give identity providers a way to show compliance with the framework, such as a mark or seal? With what resources and how will compliance be policed?
4. *Setting framework policy*: How will the trust framework policy be set, and by whom? How will user interested be taken into account, and how will policies be communicated to users? How will policies evolve?
5. *Breach of service*: If an identity provider were to breach its obligations within a trust framework, what would be the consequences?

Minimum rules for identity providers

1. *Trust framework requirements*: Will the trust framework require some minimum contract with the identity provider in order to constrain the terms that the identity provider can provide the user?
2. *Relationship to trust framework*: What will the relationship between the identity provider and the trust framework provider be? Will it be contractual, and will it also involve the user and relying party?
3. *Relationship to relying party*: Will identity providers exercise any discretion regarding with which Relying Parties they will deal? Will the provision of authenticated information to Relying Parties carry with it any obligation or potential liability for relying parties or identity providers (other than an obligation to provide information believed in good faith to be accurate)?
4. *Relationship to user*: Will identity providers be subject to some minimum requirements regarding the privacy and security of information regarding users? Will there be data retention or use limitation policies?
5. *Obligations with information passage*: Will relying parties be subject to some obligations as a condition of getting access to information about the user?

Recourse and Liability

1. *Liability of and obligations to the user*: If an identity provider fails to provide the expected services or fails to meet their obligations under the trust framework, and users are harmed, will there be any user recourse? If user information is misused or disclosed without authorization, what rights does the user have? Does the user bear liability for providing false identity information?
2. *Liability of the identity provider*: What is the liability of the identity provider of a faulty identification or faulty authentication? For failing to adequately protect user information against unauthorized use or disclosure?

3. *Liability of the relying party*: What is the liability of the relying party for relying on a faulty authentication (for example, in the case of identity theft) or rejects a valid credential it mistakenly believes is compromised? For failing to adequately protect user information against unauthorized use or disclosure?
4. *Obligations to trust framework*: If the trust framework imposes minimum contractual obligations, who will be entitled to enforce the contract? Will there be any obligation to enforce the contract?
5. *Dispute resolution procedures*: What dispute resolution procedures would be available for disputes between identity providers and trust framework provider? Between identity provider and trust framework? For the user, with respect to any of the parties?
6. *Accuracy*: Is there a method in place to allow the accuracy of information to be determined? Is there a way for a user to correct the record?

Privacy and Security

1. *Data minimization*: Is there a limit on the scope of information that may be collected (by any party) about the user? Is there a limit on the length of time that data is retained, and how is it destroyed?
2. *Purpose specification and use limitation*: Are there limitations on how information collected can be used by any party?
3. *Transaction authorization*: Will identity services provide the User with the option to approve or decline submission of authenticated information to a relying party in every instance? Can uses prohibit particular users of certain information?
4. *Security*: Will identity providers or relying parties be subject to minimum requirements on the security of data? What governance mechanisms will be imposed to prevent against unauthorized use or disclosure?
5. *Courts*: What standards apply to law enforcement access or disclosure associated with civil litigation?

Each set of questions must be resolved while establishing the obligations within a user-centric identity regime. Any such regime must impose and enforce a set of rules that increase trust for identity providers within the regime.

Conclusion

If trust framework providers can establish an appropriate set of rules regarding the minimum obligations of identity providers, relying parties and users, there is a large potential to increase the ease with which trust relationships can be formed online. Particularly for single transactions between parties who do not otherwise know each other, UCI systems have the potential to reduce transaction cost and risk. And, indeed, they may even be useful in enabling the formation of more online communities.

However, this model can only be successful if privacy and security are adequately protected and risks and liability are allocated in such a way as to enable enforcement and encourage user adoption.

The development of trust frameworks for user centric identity provides a unique opportunity to design truly user-centric and privacy protective identity management

regimes. These design decisions will determine the ease of use, liabilities, and obligations between each player in the federated identity.

Determining the obligations of each party interacting within the auspices of a trust framework will be the key aspect of creating a trust framework. Creating strong relationships between each of the parties in a user-centric federated identity system will in turn create stronger, more trusted relationships online.

Any set of answers to questions about identity must:

- impose and enforce some set of rules that increase trust in associated identification services, thereby enabling productive transactions between strangers.
- allow flexible evolution of the relevant services and support an adequate business model for participants.
- be robust against fraud or manipulation, protect the privacy and security of User data, and provide appropriate avenues for dispute resolution, redress, and/or liability in the event of performance failure.
- be adequately open to new participants without eliminating minimum qualifications and rules.