CDT Discusses Key Policies Issues Surrounding User-Centric Identity Management

November 6, 2009

Supporting Documents

Policy Posts are in-depth analyses on current tech policy issues from CDT experts. Sign up to receive the latest Policy Posts here:

1) User-Centric Digital Identity

2) Government Pilots of Federated, User-Centric Identity

3) Key Policy Questions for User-Centric Identity Systems

---

1) User-Centric Digital Identity

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"). Traditionally, Web sites ask users to log in to the site in order to assert their identity – whether it is to enable participation or to provide services to the user. However, new models for digital identity have been evolving in order to streamline online interactions and make authentication easier for online service providers.

Many of the identity technologies developed to address problems with traditional identity solutions fall under the loosely defined term "user-centric identity." New models for identity management separate the service provider and the identity provider, allowing me to log in to thousands of websites using a single set of credentials. A trust framework often connects the user, the identity provider, and the service provider (often called the relying party), laying out a set of conditions that each party should adhere to in order to maintain a trusted system.

This term refers to identity systems where users, rather than service providers, control identity credentials and information flow. In user-centric identity systems, a user logs in to a Web site via a third party identity provider, who passes on information at the user's request. Such a system is literally "user centric" because the user is at the center of the interaction, rather than having a user authenticate directly to a site or having a third party authenticate the user without the user's direct involvement. Central to the success 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, allowing further flexibility and control.

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.

---

2) Government Pilots of Federated, User-Centric Identity

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. Outsourcing authentication this way allows users to use credentials they already have (rather than yet another set of user name and password) and allows agencies to free up development resources for other tools, instead of maintaining their own sign-on system. Being able to identify previous visitors will allow sites to provide a better user experience, such as personalized news feeds or libraries.

Of course, government Web sites are not going to trust just any identity provider to authenticate users, both to ensure that the .gov site is getting reliable information and to make sure that the federal government isn't working with providers who are not protecting user information. To this end, the ICAM has put together a set of conditions that must be met by trust frameworks. These trust frameworks will set a minimum standard for the operations of, policies of, and relationships between identity providers, users, and federal Web sites in order to ensure that identity providers are reliable and responsible. Once ICAM and the GSA evaluate a trust framework, the trust framework will 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 based on the level of assurance they can provide as to a user's identity.

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 important questions around the provision of identity and services online. While government pilots are driving trust framework creation, these systems will also be used extensively outside of government Web sites. Hence, the development of these frameworks raises questions around the best practices and minimum conditions that trust frameworks, identity providers, relying parties, and users should operate under.

---

3) Key Policy Questions for User-Centric Identity Systems

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). Without strong privacy and security protections, users are exposed to a host of harms - for example, identity theft, unauthorized account access, and embarrassment. One effective way to ensure that protections are adequate is to impose minimum terms of operation as a condition of participation in the trust framework, and create enforcement mechanisms to allow each part to the trust framework to enforce these terms.

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. Decisions made in creating trust frameworks and certifying identity providers 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.

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.

The practices that will protect a user's information must also be made clear as trust frameworks are designed. The scope of information collected, the acceptable uses of that information, and who has access to the information must be made clear in order to provide assurance to users and other members of the trust framework that information is protected and user's wishes are respected

around the use of their information.

Last but certainly not least, liabilities must be considered for all members involved with a trust framework, including dispute resolution procedures for these obligations. If it is unclear who bears the burden of mistakes, then users will be slow to adopt new identity management systems. In order for user-centric identity systems to protect privacy and enable trusted relationships online, trust frameworks 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.

For a more comprehensive list of questions that must be answered, please see our white paper.

Copyright © 2013 by Center for Democracy & Technology
The content on this website that originates with CDT can be freely copied and used as long as you make no substantive changes and clearly give us credit. Details.
Source URL:
https://www.cdt.org/policy/cdt-discusses-key-policies-issues-surrounding-user-centric-identity-management