



PRIVACY & SECURITY LAW



REPORT

Authentication

Identity Management

The need to authenticate a person's identity plays a key role in establishing the trust necessary to fight identity fraud and facilitate electronic transactions of all types, and has become a legal obligation in its own right. This article by attorneys from Wildman Harrold identifies some of the legal issues raised by the authentication model receiving the most attention—federated identity management—and focuses on the need to develop an appropriate legal infrastructure necessary to make it work.

Addressing The Legal Challenges of Federated Identity Management

By THOMAS J. SMEDINGHOFF AND
DAVID A. WHEELER

“Who are you?” is a fundamental question for all online business activities. Whether a company wants to allow employees, customers, or business partners to remotely access its networks or engage in online commercial transactions, the need to authenticate the identity of the remote party is critical. It plays a key role in establishing the trust necessary to fight identity fraud and to facilitate electronic transactions of all types,¹ and has become a legal obligation in its own right.

¹ See, e.g., OECD Recommendation on Electronic Authentication and OECD Guidance for Electronic Authentication,

Thomas J. Smedinghoff is a partner and David A. Wheeler is a senior associate in the Privacy, Data Security, and Information Law Practice at the law firm of Wildman Harrold, Chicago. They can be reached at smedinghoff@wildman.com and wheeler@wildman.com.

A company's duty to provide appropriate information security clearly includes an obligation to properly authenticate persons seeking to access its networks or services.² For example, banking regulations impose requirements for authentication in online banking activities,³ and common law negligence was applied in a recent case to hold a credit card issuer liable for failing to properly authenticate the identity of the applicant/imposter.⁴

Depending on the process selected, complying with the obligation to authenticate can itself raise a myriad of legal issues. And these issues are becoming as complex as the technical requirements of the authentication solutions themselves. This article identifies some of the

June 2007, at p. 7; available at <http://www.oecd.org/dataoecd/32/45/38921342.pdf>.

² See, generally, Thomas J. Smedinghoff, “It's All About Trust: The Expanding Scope of Security Obligations in Global Privacy and E-Transaction Law” 16 Michigan State Journal of International Law 1, 29-41 (2007).

³ Federal Financial Institutions Examination Council, Authentication in an Internet Banking Environment, October 12, 2005, available at http://www.ffeec.gov/pdf/authentication_guidance.pdf.

⁴ *Wolfe v. MBNA America Bank*, 485 F. Supp.2d 874, 882 (W.D. Tenn. 2007).

key legal issues raised by the authentication model receiving the most attention—federated identity management—and focuses on the need to develop an appropriate legal infrastructure necessary to make it work.

Identity Management

Understanding federated identity, its critical role in online commerce, and the legal issues it raises, begins with understanding the underlying subject of identity management. It has two basic components, which center around the concepts of identification and authentication.

First, before a company allows someone to access its systems, or enters into a transaction with someone over the Internet, that person must be properly identified (e.g., this is John Smith, an employee of ABC company who works in accounting). *Identification* is concerned with determining who a specific person is. This is done by associating attributes with a person, such as name, address, Social Security number, gender, date of birth, background, criminal history, credit history, employment status, membership status, etc. The level of identification that is necessary will, of course, vary with the circumstances. Some remote transactions may require minimal identification (such as determining only that the person is over a minimum age or is a member of certain group), whereas others may require detailed identification.

Second, once the identification process has determined enough about a person that a company is willing to do business with him (e.g., grant him access to its network/computer system, allow him to open an account, etc.), an *authentication* process is used when someone purporting to be that person seeks remote access. This involves verifying that the person trying to access the system is who he claims to be—i.e., that he really is the person that was previously identified and determined to be trustworthy.⁵

In the past, each business has handled its own identity management. For example, a company would identify each of its employees and customers, and then set up a mechanism, such as usernames and shared secrets or passwords, by which those persons could be authenticated for remote network access. Today, however, businesses and government agencies increasingly want to use third parties to handle these difficult and often expensive tasks. In addition, users, overloaded with passwords, are looking for a one-stop option. This is where federated identity management offers a promising solution for dealing with the cost and complexity of addressing these identity management problems.

Federated Identity Management

Federated identity management has been defined as “the use of agreements, standards, and technologies to make identity and entitlements portable across auto-

⁵ In this context, the U.S. Homeland Security Act of 2002 defines authentication as “utilizing digital credentials to assure the identity of users and validate their access.” Homeland Security Act of 2002 § 1001(b), amending 44 U.S.C. § 3532(b)(1)(D).

nous identity domains.”⁶ Its goal is to facilitate the secure exchange of identity credentials between organizations—i.e., to enable users of one domain to securely access data or systems of another domain seamlessly, and without the need for redundant user administration. In other words, a federated identity model enables the portability of identity information across different systems and entities.

For example, a federated identity arrangement would allow one organization (e.g., the Social Security Administration) to authenticate the identity of a person seeking access by relying on an identity assertion made by a separate organization (e.g., that person’s bank) which has previously identified that person as part of its customer screening process. So long as a protocol exists for sharing the identity data between the bank and SSA, that person can do business with SSA using the user ID and password (or other identity token) issued by his bank.

That assumes, of course, that SSA trusts the identification process used by the bank, that the bank can limit its liability risk should it make a mistake, and that the individual involved trusts both the bank and the SSA to properly use and protect the personal information he initially provided to the bank. These issues, among many others, are some of the key legal problems that the parties involved in the process of federated identity management must address before it will scale.

Much work is being done by groups such as the World Wide Web Consortium (W3C), the Organization for the Advancement of Structured Information Standards (OASIS), the Liberty Alliance, WS-Federation, and others to develop technical specifications that allow a business to verify the identity of a person seeking to access its systems by referencing a digital credential issued by a third party. Yet the concept of federated identity management raises critical legal issues that often get overlooked in the development of appropriate specifications. Failure to recognize and address these legal issues will likely slow the widespread implementation of federated identity options. Thus, a legal framework is required as well.

While the technical details and specifications of a federated identity system can become quite complex, the key legal issues are readily apparent by looking at an oversimplified summary of what actually happens:

- A business (the **relying party**) wants to authenticate the identity of a particular person (the **subject**). The subject may, for example, be an individual seeking access to the relying party’s network, a person seeking to enter into an online contract with the relying party, or someone seeking to access an account with the relying party.
- To provide the required identity information, and facilitate the authentication process, a third party that has previously identified the subject (the **identity provider**) issues a digital credential or token to make an assertion about the identity of the subject to the relying party. The token could be as simple as an electronic record, or as complex as a cryptographically signed digital certificate.
- The token is communicated to the relying party (by either the subject or the identity provider, depend-

⁶ Archie Reed, *THE DEFINITIVE GUIDE TO IDENTITY MANAGEMENT*, Chapter 2, p. 43, available at <http://nexus.realtimepublishers.com/content/DGIMFinal.pdf>.

ing on the system involved), the relying party validates the token to ensure that it is still good, and then relies on the associated identity assertion from the identity provider to authenticate the subject in order to grant access or proceed with the proposed transaction.

There are many ways to implement these processes, ranging from relatively simple user ID and password systems to very complex public key infrastructures. But in all cases, there are key legal issues that need to be addressed in order to make it work, and a need to implement a basic legal framework to provide the answers.

Key Legal Issues

Transferring identity information and assertions across organizational boundaries creates risk for all participants in the process. In order to effectively and predictably allocate that risk and make it work from a legal perspective, federation participants need an enforceable legal framework that addresses the relevant issues and compliance obligations. Examples of key issues that need to be addressed by a federation's legal framework include the following:

Identification Process. First and foremost, both subjects and relying parties need to understand the process that the identity provider uses to establish the identity of the subject, and need some reasonable assurance that this process is always followed. For example, does the identity provider do an in-person interview of the subject and examine multiple government-issued photo identification documents, or does it simply rely on the subject's self-asserted claims made over the Internet? What mechanisms are in place to ensure that the identity provider has actually complied with that process? For example, is there a requirement for an external audit?

Privacy. By its nature, federated identity management involves the collection (by an identity provider) and disclosure (to a relying party) of personal information about the subjects. What information is collected by the identity provider? How securely it is handled? How much information is disclosed to relying parties? The answers to these questions will vary with the federation, but need to be clearly understood by everyone. Thus, establishing the rules that govern the privacy and security of that personal information is a critical concern for all participants. Issues will include notice regarding the purpose of collection, rights to use the information, consent of the subject and representations as to accuracy, obligations to ensure that the data is accurate, complete and up-to-date when used, restrictions on retention and proper destruction, requirements for the use of reasonable security measures to minimize the risk of unauthorized use, modification, or disclosure, and rights of the subject to control the use of his personal data, or to have it revised, corrected, or erased.

In addition, the collection and sharing of information between organizations may also be governed by a variety of domestic and international laws and regulations. In the European Union, for example, the Electronic Signatures Directive regulates the collection of personal data about subjects by certain identity providers

(certification-service-providers).⁷ And transfer of that data across country borders, whether for identification or identity assertion purposes, will also raise issues under EU country privacy laws. In the United States, state security laws governing personal information will also be a key factor.

Scope of Assertion. The scope of the identity assertion must be defined. The identity provider needs to know the legal standard to which it will be held, and the relying party needs to know the scope of the identity representation on which it is relying. For example, does an identity assertion that someone is "Bill Gates" mean that such person is the *founder* of Microsoft Corp., or just anyone who happens to have that name? Or does it mean that such person has a bank account in the name of Bill Gates? Or does it simply mean the person "claims" to be Bill Gates? The answer to this type of question will have a significant impact on the willingness of the relying party to proceed with different types of transactions on the basis of the identity assertion. It will also affect the liability of the identity provider in the event the assertion is incorrect.

Use of Assertion. What type of transaction is appropriate for use of the identity assertion? The level of identification required to make an identity assertion for purposes of accessing the control processes of a nuclear reactor is presumably much greater than the level of identification necessary to justify access to the local garden club Web site. The identity provider may also want to limit the use of an identity assertion in order to control its potential liability for errors.

Liability. A primary concern with any identity federation model is who will bear the risks associated with faulty authentication, and consequential unauthorized access or circumvention of access controls through identity fraud or mistake. Specifically, what is the liability of the subject for providing false identity information, or for failing to protect the password or key necessary to initiate an identity assertion? What is the liability of the identity provider for failing to follow proper identification procedures that result in an incorrect identity assertion? What is the liability of the relying party for relying on a fraudulent assertion (e.g., in the case of identity theft), especially in a case where it could have determined that the assertion was false? A study of this issue in the context of one type of identity provider (certification authorities) reveals many potential concerns.⁸

Models for a Legal Infrastructure

There are a variety of possible approaches to developing a legal infrastructure to address questions like these. They include the following:

Legislative and Regulatory Models. Numerous laws and regulations have been enacted in an attempt to define a legal framework for at least some aspects of federated identity management. While they have been the subject of criticism, particularly where they assume that the technical model will be based on public-key cryptography, they must be addressed in the jurisdictions

⁷ Directive 1999/93/EC of 13 December 1999 on a Community Framework for Electronic Signatures, Article 8, available at <http://op.bna.com/pl.nsf/r?Open=dapn-7carb7>

⁸ See Thomas J. Smedinghoff, Certification Authority Liability Analysis, available at <http://www.wildman.com/resources/articles-pdf/ca-liability-analysis.pdf>.

where they exist, particularly where they are mandatory. Examples include provisions found in the EU Electronic Signatures Directive,⁹ the Malaysia Digital Signature Regulations,¹⁰ the recently-repealed Utah Digital Signature Law, and the UNCITRAL Model Law on Electronic Signatures (which has been incorporated into the law of several countries).¹¹

Contractual Models. Most common are contractual models that seek to bind the participants to a pre-defined set of rules and legal obligations. The Liberty Alliance, for example, recommends that the participants establish a contractual legal infrastructure that it refers to as a “circle of trust.”¹² Such contractual frameworks can take a variety of forms, including:

- A “governing entity” model where a single entity is created (often by a group of initial participants) to establish and enforce a standard set of rules, and all of the participants in the identity federation agree in a contract with the governing entity to be bound by those rules for the benefit of all of the other participants. Examples of such an approach (although not necessarily for purposes of identity authentication) include the credit card contractual frameworks set up by Visa and MasterCard, the ACH [Automated Clearinghouse] electronic payments system set up by the National Automated Clearinghouse Association, and the PKI [public key infrastructure] system set up by Identrus.
- A “founding entity” model, where a single entity sets up the rules, and all of the participants in the identity federation agree in a contract with the founding entity to be bound by those rules for the benefit of the founding entity. An example of this approach is the series of one-on-one contractual relationships that the federal government has been

entering into with selected identity providers in its E-Authentication program.¹³

Public Standards Models. A related approach is for a standards body to establish and maintain a set of standards that govern the rights of participants in the identity federation, and require an independent audit for verification. Identity providers then opt-in to those standards, such as by publicly declaring their willingness to be bound by them, and submitting to an independent audit to verify their compliance as a condition of participating. The theory is that other parties that rely on identity assertions are on notice as to the rules, and by their reliance on the identity assertions are bound thereby. An example of this approach is the EV SSL [Extended Validation SSL] Certificate Guidelines and the WebTrust audit requirements specified by the CA/Browser Forum for the issuance and use of Extended Validation SSL [secure socket layer] certificates to identify Web site operators.¹⁴

Self-Defined Standards Models. In some cases, identity providers simply establish their own standards, by publicly declaring the manner in which they operate, the rules to which they will be subject, and the liability (if any) that they will accept. Like the public standards model, it they hope that subjects and relying parties will be bound by the limitations of the self-declared standard. An example of this approach can be seen in the Certification Practices Statement issued by VeriSign with respect to the digital certificates that it issues.¹⁵

Each of these approaches has positive and negative attributes, but all are essentially untested by any court. Regardless of the approach, participants need to recognize that there are numerous other laws which, while not specifically focused on identity management, will have a significant impact. These include the various laws regulating the privacy and security of personal information.

Without some type of a legal framework to address all of the issues noted above, however, a federated identity model will likely not scale. At least in the case of economically significant transactions, the risks to each of the parties of such unresolved issues are often too great to justify reliance on the federated process. Providing a legal mechanism to address these questions, and others like them, is key to establishing a viable federated identity management infrastructure.

⁹ See, e.g., EU Electronic Signatures Directive (1999/93/EC), Articles 6 – 8 and Annexes I and II, available at http://europa.eu/eur-lex/pri/en/oj/dat/2000/l_013/l_01320000119en00120020.pdf.

¹⁰ See Malaysia Digital Signature Regulations, 1998, available at http://www.mcmc.gov.my/the_law/NewAct/Act%20562/Rules%20&%20Regulations/pua%20359y1998/pua359y1998bi/pua0359y1998.htm.

¹¹ See United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Signatures 2001, Articles 8 – 12, available at http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2001Model_signatures.html.

¹² See, e.g., the Liberty Alliance Contractual Framework Outline for Circles of Trust, available at http://www.projectliberty.org/liberty/files/whitepapers/liberty_alliance_contractual_framework_outline_for_circles_of_trust.

¹³ See U.S. E-Authentication Identity Federation Web site at http://www.cio.gov/eauthentication/membership_documents.cfm.

¹⁴ See CA/Browser Forum Web site at <http://www.cabforum.org>.

¹⁵ See VeriSign Certification Practice Statement (CPS), available at <http://www.verisign.com/repository/CPS>.