Developing federated identity management to build trust

Thomas J. Smedinghoff, Of Counsel at Locke Lord LLP, and Chair of the American Bar Association Identity Management Legal Task Force, provides detailed analysis of the development of identity management to build trust in online commerce, which includes comparisons between the approaches being adopted by the EU and the US.

In this age of phishing, hacking, identity fraud, and other forms of cybercrime, answering two simple questions - 'Who are you?' and 'How can you prove it?' - is fast becoming a critical requirement for online business activities. Yet building trustworthy interoperable identity systems to address this need has proved difficult.

In any significant online transaction each party has a need to know, and to be able to verify, relevant information about the identity of the other party. A bank, for example, must be able to verify that the person seeking to transfer funds from an account is, in fact, the authorised account holder. Likewise, a government agency providing online citizen services must be able to verify an applicant's identity before disbursing benefits to such person.

Traditionally, businesses have dealt with this issue by verifying the identity of every party they transact with, and then using a username and password scheme to authenticate that identity in each online transaction. As a result, users go through some type of identification process with every organisation they deal with online, and must manage an increasing number of usernames and passwords. This has become quite expensive for businesses, and quite cumbersome for users. Moreover, as passwords are increasingly compromised, the reliability of this approach is doubtful at best.

To promote online commerce, facilitate increased security, and deter identity fraud, both the EU and the US have now made it a priority to establish federated identity systems for online transactions. In a federated system, transacting parties can avoid the cost and expense of setting up their own identity management system, relying instead on identification and authentication services provided by third parties. And users can avoid the need to obtain separate credentials for every business they deal with.

As might be expected, the EU and US are pursuing somewhat different approaches to reach this goal. The EU has initiated a legislative process, beginning with the adoption of the eIDAS Regulation in July 2014[1], to address public sector federated identity transactions. The US, by contrast, developed a National Strategy for Trusted Identities in Cyberspace ('NSTIC')[2], and has created a public-private partnership known as the Identity Ecosystem Steering Group ('IDESG')[3] in an attempt to implement that strategy on a voluntary basis.

Identity management

Understanding the EU and US approaches, and the challenges, begins with an overview of the key identity management processes involved. Although the term 'identity management' is relatively new, the concept is not. Traditional passports, driver's licences, and employee ID cards are all components of what might be referred to as identity management systems - i.e., they are credentials issued by an entity for the purpose of identifying individuals, and they are used by such individuals to validate their identity. There are many different approaches to identity management, whether online or offline. But it essentially involves three basic processes: (1) identification, (2) credential issuance, and (3) authentication.

The identification process is designed to answer the question 'who are you?' Performed by someone filling the role of an identity provider, it involves associating one or more identifying attributes (e.g., name, address, birth date, email address etc.) with a particular person in order to identify and define that individual to the extent sufficient for the contemplated purpose. Sometimes called 'identity proofing,' this process is usually a one time event. It involves the collection and verification by an identity provider of personal information about the person to be identified (referred to as the 'subject' or 'user'). As might be imagined, the collection and verification of this identifying information raises numerous privacy and data security issues.

Following completion of the identification process, the subject's identity is typically represented by data in a paper or electronic document issued by the identity provider and referred to as an identity credential[4]. In the physical world paper-based identity credentials include driver's licences, passports, and employee identification cards. In the online world, an electronic identity credential can be as simple as a username the user must remember, or as complex as a cryptographically-based digital certificate that might be stored on a computer, cell phone, smart card, flash drive, or similar device.

When a person presents an identity credential, claims to be the individual identified by the credential, and seeks to exercise a right or privilege granted to such

individual, an authentication process is used by the relying party to determine whether that person is, in fact, who they claim to be. In other words, once someone makes a declaration of who they are, authentication is designed to answer the question 'how can you prove it?'

Authentication is a transaction-specific event that involves associating a remote person with an identity credential to verify that the person trying to engage in the transaction or access a resource is in fact the person that was previously identified and authorised for the transaction. If the credential is a paper-based passport, this association is typically done by comparing the picture on the passport to the person presenting it. With an online username, the association is established by use of a secret PIN or password which (in theory) is known only to the person to whom the username was issued.

Once a person is successfully authenticated, the relying party then engages in its own authorisation process to determine the rights and privileges accorded to such person. This process addresses the question 'What can you do?' In other words, authentication of identity is not just an end in itself, but rather a process used to authorise some type of grant of rights or privileges, to facilitate a transaction or decision, or to satisfy an evidentiary obligation.

The ultimate vision of federated identity is that businesses, government agencies, and others will be able to rely on a process performed, and identity information provided, by any one of several third party identity providers. This will, for example, allow individuals to use an identity credential of their choosing to conduct online transactions with numerous enterprises and government agencies, just as an individual might use a driver's licence for a variety of different offline transactions.

EU vs. US approaches

The EU eIDAS Regulation focuses on identity systems[5] that issue credentials for use in online transactions with public sector bodies. Its key goal is mutual recognition of such credentials in cross-border public sector transactions - i.e., to enable individuals who have such an identity credential issued in one EU Member State to use that same credential to access online public services in another Member State.

To achieve that goal, each Member State can notify the EU Commission of those identity systems whose credentials are accepted for its own online public services, and which should be granted mutual recognition by government agencies in other Member States. Once such notification is made, other EU Member States are obligated to accept credentials from those systems for online public services.

The eIDAS Regulation does not require that such notified identity systems be government operated. Accordingly, credentials issued by the Member State, under a mandate from the Member State, or independently of the Member State (e.g., by the private sector) but recognised by the Member State, are all acceptable. However, they must also comply with the applicable technical specifications, standards and procedures regarding assurance levels set out in the implementing act currently being developed.

The US, by contrast, seeks to address the problem of online identity management for both the commercial and public sector. It contemplates that the private sector will both lead the development and implementation of an identity ecosystem in accordance with a set of four basic guiding principles, and own and operate the vast majority of the identity services.

The US National Strategy does not contemplate legislation, taking the view that government should not over-define or over-regulate the market for identity and authentication services. Instead, it seeks to establish a voluntary interoperable identity ecosystem where individuals have the choice of obtaining and using different credentials from a variety of different identity providers.

The need for rules

Both the EU and US approaches require building trustworthy identity systems. That is, the identity proofing must yield the correct identification, the identity credentials and the authentication processes must be secure, the identity credentials must be interoperable, and the overall process must protect the privacy of the subjects. The hardware, software, and other tools necessary to build such trustworthy systems already exist. The real challenge is developing the rules specifying the use of specific tools and processes that will achieve a reliable online verification of identity.

Much like the Visa or MasterCard rules that govern credit card systems, identity system rules provide a structure to govern the operation of the identity system. They include technical specifications and operational rules and requirements necessary to make the system functional and trustworthy, and legal rules that define the rights and legal obligations of the parties and facilitate enforcement where necessary.

The source and content of those

rules, and the method of assuring each participant that all of the other participants are following those rules, have provided some of the key challenges for developing economically viable identity systems. Both the EU eIDAS Regulation and the US NSTIC program seek to address those challenges via different approaches.

Source of rules

Identity system rules can be defined by either (1) statutes or regulations imposed on the parties by the government, or (2) the set of rules that govern a given identity system which are agreed to by the parties through a voluntary contract. The contract-law identity system rules are often referred to as a 'trust framework' or 'scheme rules.' In most cases, identity systems will be governed by some combination of the two approaches.

The EU relies primarily on public law, as set forth in the eIDAS Regulation, and on minimum technical specifications, standards, and procedures set forth in an implementing act currently being developed. At the same time, however, the EU Regulation also recognises that Member States will be responsible for some aspects of the rules for their own identity systems, although such rules must be consistent with the Regulation.

The US, by contrast, does not contemplate enacting identity management legislation or regulation. Instead, it is looking to the private sector to develop the rules governing each identity system. The NSTIC project seeks voluntary compliance of identity systems with the set of rules to be developed by the IDESG that reflect the NSTIC guiding principles.

Allocation of liability

The risk of liability, and uncertainty as to the scope of that risk, are major barriers to participation in identity systems. The rules regarding liability can come either from existing public law, or from the private rules governing an identity system. In many cases, they may come from a combination of both sources.

The US, by contrast, does not contemplate enacting identity management legislation or regulation. Instead, it is looking to the private sector to develop the rules governing each identity system

The EU addresses the liability issue directly in the eIDAS Regulation. It holds Member States liable for damage caused intentionally or negligently due to a failure to comply with its obligations set forth in the implementing act currently under development, or to ensure the availability of online authentication. It provides similar allocations of liability for parties issuing identity credentials and operating authentication procedures.

The US, by contrast, does not contemplate legislation specifically addressing liability in the context of online identity transactions. The current US approach is to leave the allocation of liability to existing common law rules, or alternatively, to the rules agreed upon by the parties in the trust framework governing the identity system.

Source of assurances

Rules themselves aren't enough. Building a trustworthy identity system also requires that each participant has confidence that each of the other participants with whom they interact in an identity transaction will follow those rules. To a certain extent, assurances can be provided by making the rules legally enforceable - either by statute or contract. But legal enforcement occurs only after a loss has been incurred.

Another approach is to require certification based on a successful audit of the processes, procedures, software, and hardware implemented by a participant to verify that it follows the rules. In both the EU and US, certification takes on an important role.

The problem with certification, however, is that engaging a third party to audit someone's system and verify compliance can be expensive and time consuming. The alternative, which is implemented in the eIDAS Regulation, and also being discussed in the US, is the concept of self-certification.

Conclusion

Both the EU and the US are taking different paths to motivate businesses and users to build and participate in federated identity systems. While trust is important, in all cases the value received by each role must be sufficient to justify the cost or hassle involved in participating. Both the EU and US approaches deserve close monitoring to see if either or both provide the necessary incentives for the development of a viable federated identity ecosystem.

Thomas J. Smedinghoff Chair of the American Bar Association Identity Management Legal Task Force, and Of Counsel
Locke Lord LLP, Chicago
tom.smedinghoff@lockelord.com

1. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, (referred to as the 'eIDAS Regulation' - electronic identification and signature), available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG
2. National Strategy for Trusted Identities in Cyberspace, 15 April 2011; available at http://www.nist.gov/nstic/ ('National Strategy').
3. https://www.idecosystem.org/
4. The eIDAS Regulation refers to identity credentials as 'electronic identification means.'
5. The eIDAS Regulation refers to identity systems as 'electronic identification schemes.'