Introduction to Online Identity Management

By Thomas J. Smedinghoff[1]

---

[1] Thomas J. Smedinghoff is a partner in the Privacy, Data Security and Information Law Practice at the law firm of Wildman Harrold in Chicago. He is Co-Chair of the Identity Management Legal Task Force of the American Bar Association (ABA) Section of Business Law, and Chair of the International Policy Committee of the ABA Section of Science & Technology Law. Mr. Smedinghoff is also a member of the U.S. Delegation to the United Nations Commission on International Trade Law ("UNCITRAL"), where he participated in the negotiation of the United Nations Convention on the Use of Electronic Communications in International Contracts. He is also the author of INFORMATION SECURITY LAW: THE EMERGING STANDARD FOR CORPORATE COMPLIANCE (IT Governance Publishing, 2008). He can be reached at smedinghoff@wildman.com.

Introduction to Online Identity Management

In this age of phishing, hacking, social engineering, and identity theft, the answer to the question "Who are you?" has taken on a new dimension. In an online environment, without the benefit of face-to-face personal contact, authenticating the identity of the remote party is more important than ever. It plays a key role in fighting identity fraud, is essential to establishing the trust necessary to facilitate electronic transactions of all types, and in many cases has become a legal obligation. Yet at the same time, it raises significant privacy and identity theft concerns, among others.

Verifying the identity of a person or entity[2] that seeks remote access to a corporate system, that authors an electronic communication, or that signs an electronic document, is the domain of what has also come to be called "identity management." It is increasingly playing a critical role in online commerce. As the European Commission has noted:

> Electronic Identity Management is a key element for the delivery of any e-services. On the one hand, e-identification gives individuals using electronic procedures the assurance that no unauthorised use is made of their identity and personal data. On the other hand, administrations are able to make sure that the individuals are the persons they claim to be and have the rights that they claim to have (e.g. to receive the requested service).[3]

The OECD, in its Recommendation on Electronic Authentication, has expressed a similar view, noting that:

> Electronic authentication provides a level of assurance as to whether someone or something is who or what it claims to be in a digital environment. Thus, electronic authentication plays a key role in the establishment of trust relationships for electronic commerce, electronic government and many other social interactions. It is also an essential component of any strategy to protect information systems and networks, financial data, personal information and other assets from unauthorized access or identity theft. Electronic authentication is therefore essential for establishing accountability on line.[4]

---

[2] For an example of an identity system focused on corporate identity see the Guidelines for Extended Validation SSL Certificates established by the CA/Browser Forum at http://www.cabforum.org. For a recent example of corporate identity theft, see "WVa scam is rare type of ID theft," Chicago Tribune, May 9, 2009; available at http://www.chicagotribune.com/news/chi-ap-wv-auditorscam,0,4039207.story. Identity management issues also arise in the context of verifying the identity of a device on a system or network. However, this paper will focus only on the identity of persons and entities.

[3] European Commission, "Action Plan on e-signatures and e-identification to facilitate the provision of crossborder public services in the Single Market," COM(2008) 798 final (28 November 2008); available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0798:FIN:EN:PDF

[4] Organisation for Economic Co-operation and Development (OECD) Recommendation on Electronic Authentication and OECD Guidance for Electronic Authentication, June 2007, at p. 7; available at http://www.oecd.org/dataoecd/32/45/38921342.pdf.

Identity management is also a critical building block of information security. It forms the basis for most types of access control and for establishing accountability online. Thus, it contributes to the protection of privacy by reducing the risks of unauthorized access to personal information, data breaches, and identity theft.

The critical importance of online identity management in facilitating trustworthy e-commerce and ensuring national security is now well-recognized. Several other governments and inter-governmental forums are already actively working to address the applicable technical and legal issues. These include Australia,[5] Canada,[6] the EU,[7] India, the OECD,[8] Scotland,[9] and the United States.[10]

Without adequate identity management, the need to identify persons seeking online access is complicating life for individual users (who must remember or track numerous User IDs and passwords), and is becoming increasingly costly for businesses who must identify and authenticate the ever-growing number of persons and entities with whom they deal electronically. In addition, it increases privacy risks to the individuals being identified, especially as more and more entities collect and exchange an ever-increasing amount of personal data from and about such individuals, all in the name of identity management.

One approach to address the challenges of identity management that is gaining widespread attention is the concept of federated identity management. It allows businesses to, in effect, outsource the identification and authentication processes to a third party, and eases the burden on users and consumers by allowing them to use a single sign-on.

This paper will outline the basic concepts behind identity management and the developing concept of federated identity management, and then identify and examine some of the key legal risks that must be addressed to make it work. The focus will be on identity

---

[5] See, e.g., Australian National Audit Office, Attorney–General's Department Arrangements for the National Identity Security Strategy, ANAO Audit Report No.29 2009–10, April 21, 2010; available at www.anao.gov.au/uploads/documents/2009-2010_Audit_Report_29.pdf.

[6] Treasury Board of Canada Secretariat, Directive on Identity Management, July 1, 2009; available at www.tbs-sct.gc.ca/pol/doc-eng.aspx?section=text&id=16577.

[7] See, e.g., Commission of the European Communities, Action Plan on e-signatures and e-identification to facilitate the provision of crossborder public services in the Single Market, COM(2008) 798 final, November 28, 2008; available at http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=en&DosId=197692; and Secure Identity Across Borders Linked (STORK-eID Consortium), Report on Legal Interoperability, February 24, 2009; available at www.eid-stork.eu/index.php?option=com_processes&Itemid=60&act=streamDocument&did=578.

[8] OECD, "The Role of Digital Identity Management in the Internet Economy: A Primer for Policy Makers", OECD Digital Economy Papers, No. 160, June 11, 2009; available at www.oecd.org/dataoecd/55/48/43091476.pdf

[9] Scottish Government, Privacy and Public Confidence in Scottish Public Services: Draft Identity Management and Privacy Principles, August 31, 2009; available at www.scotland.gov.uk/Publications/2009/08/PrinciplesConsultation.

[10] "National Strategy for Trusted Identities in Cyberspace," (Draft, June 25, 2010), at p. 1 (hereinafter "**NSTIC**"); available at http://www.dhs.gov/xlibrary/assets/ns_tic.pdf.

management of persons rather than devices, conducted in a business context rather than social networking setting.

To understand federated identity management, and the legal issues it raises, we begin with an overview of the basic processes involved in identity management.

1. Identity Management Basics

Although the term "identity management" is relatively new, the concept is not. In fact, the underlying processes have been in use for many generations in an offline environment. Passports, driver's licenses, 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 in order to enter into a transaction with a third party.

While there are many different approaches to identity management,[11] it essentially involves two fundamental processes: (1) the process of identifying a person and issuing an identity credential to reflect that identity ("identification"), and (2) the process of later verifying that a particular person presenting that credential and claiming to be that previously identified person is, in fact, such person ("authentication"). Once an individual's identity is successfully authenticated, a third process, referred to as "authorization," is used by the business relying on the authenticated identity to determine what rights and privileges are accorded to such person – e.g., whether such person should be granted access to a website, a database, a bar, an airport boarding area, etc.

A simple and familiar example of these processes can be seen in the case of an employee who logs into his or her employer's network using a user ID and password. Before a company allows a person to access its internal network, that person must be properly identified in a manner appropriate for the transaction (e.g., as an employee with certain authority), and then that identity must be authenticated at the time of each transaction. Employees are identified by their employer, and issued an identity credential consisting of a unique identifier (typically a User ID) which is linked to other relevant information attributes stored on the company's computer system. A secret (in this case, a password), is then used to link the employee to the identity credential. Thereafter, when the employee wants to remotely access the company's network, he or she can be authenticated by using the password in an authentication protocol. The authentication protocol allows the employee to demonstrate to the employer that he or she has or knows the secret, and thus, is the person previously identified.

---

[11] The OECD defines identity management (IdM) as: "the set of rules, procedures and technical components that implement an organisation's policy related to the establishment, use and exchange of digital identity information for the purpose of accessing services or resources. Effective IdM policies safeguard digital identity information throughout its life cycle – from enrolment to revocation – while maximising the potential benefits of its use, including across domains to deliver joined-up services over the Internet." OECD Working Party on Information Security and Privacy, The Role of Digital Identity Management in the Internet Economy: A Primer for Policy Makers**,** DSTI/ICCP/REG(2008)10/FINAL, (June 11, 2009), at p. 4; available at http://www.oecd.org/dataoecd/55/48/43091476.pdf (hereinafter "**OECD Report**").

A key characteristic of some existing offline identity documents (such as a passport or drivers license) is that their use is not limited to transactions with the entities that issued them. Rather, they are often accepted by third parties (such as airport security, a bank, or a bartender) when proof of certain aspects of one's identity is required. This characteristic is critical for the identity credentials needed for e-commerce.

Such an approach, whereby a business or government agency relies on an identification process performed, and identity information provided, by one of several possible unrelated third parties is sometimes referred to as a federated identity model. Under such a model, a single identity credential can be used with numerous organizations that had no involvement with the original issuance of the credential.

The challenge is to import a similar approach to the digital online environment. That is, to create secure, reliable and trustworthy digital identity credentials that can be used across different ecosystems and entities. This allows individuals to use the same identity credential to sign on to the networks of more than one business in order to conduct transactions.

Thus, lets us begin by looking more closely at the nature of the identification and authentication processes that form the foundation of identity management, as a clear understanding of those processes is important to the legal analysis.

(a) Identification

The ***identification*** process is designed to answer the question "who are you?" It involves associating one or more ***attributes***[12] (*e.g.*, name, height, birth date, SSN, employer, home address, passport number) with a person in order to identify and define that individual to the level sufficient for the contemplated purpose. Sometimes called "identity proofing," "identity vetting," or "enrolment," this process is usually a one-time event. It typically involves the collection of personal information about the person to be identified, and often relies on a patchwork of government-issued documents from birth certificates and Social Security cards to driver's licenses and passports.[13] The personal information may be collected directly from the person being identified, as well as from third party sources (e.g., government agencies, credit agencies, public record databases, etc.). Note that the attributes may be permanent (e.g., date of birth) or temporary (e.g., current employer), inherited (e.g., DNA), acquired (e.g., educational degrees), or assigned (e.g., employee number).

Identification is the act through which data subject presents itself. Such presentation can take many forms, and is generally more formalized and intensive (and more potentially "intrusive") as the purposes for which the identification is being made become riskier and

---

[12] Identity attributes are personal information concerning a specific category or characteristic of a given identity, such as name, address, age, gender, title, salary, health, net worth, driver's license number, Social Security number, etc.

[13] Industry Advisory Council Transition Study Group, "Identity and Access Management," (December 9, 2008) at p. 4; available at www.actgov.org/knowledgebank/studies/Documents/Transition%20Study%20Group%20Papers/Identity%20and%20Access%20Management,%20IAC,%2012-9-2008.pdf (hereinafter "**Transition Study Group Report**").

involves higher value transactions. All data and information system depends on identification to separate authorized and unauthorized parties. Different "rituals" and requirements are imposed for identification of individuals, entities and things, since each has different characteristics (called "attributes" in identity-speak).

The identification (or enrolment) process can in theory be conducted in person, by mail, fax, phone, or online. "More stringent enrolment processes may require the presentation in person of physical credentials issued to the person by other entities. These may include government-issued credentials (e.g., passports, identity cards and drivers licenses) and/or credentials issued by private sector entities (e.g., employee badges, mobile wireless SIM cards, and credit cards). Government institutions such as motor vehicle departments and post offices sometimes accomplish identity verification through this type of 'in-person' proofing. In addition, in-person proofing is common among banks, schools, and employers in their enrolment processes."[14]

(1) Scope and Accuracy

The process of identifying a person can vary widely across two different dimensions. The first dimension relates to the scope of the personal information attributes collected about and associated with an individual to establish his or her "identity" – i.e., which and how much information is collected and verified. A second dimension of the identification process relates to the degree of certainty with which the identifying attributes are ascertained – i.e., how accurate is the information likely to be.

The amount and type of personal information that is required will, of course, depend on the purpose of the identification. In some cases, only minimal information is required, and the process can be limited to verifying only a very few attributes, such as "this person is over 21 years old" or "this person is a member of the group entitled to admission." This might be the case, for example, for some activities (such as purchasing wine) where a single attribute (e.g., age) might be sufficient. Generally, the fewer the attributes collected, the lower the privacy risk.

At the other end of the spectrum, it may be necessary to collect a large number of very detailed identifying attributes, such as name and address, physical characteristics, gender, race, Social Security number, employment details, criminal background, credit and financial history, medical history, and information about prior activities and transactions. This might be necessary in certain cases to ensure uniqueness, or in cases where a person is being considered for employment in a very sensitive position or for access to a very sensitive database, and a much more detailed form of identification is required to determine whether authorization should be granted. Of course, this also tends to increase the privacy risk to all parties.

The second dimension of the identification process focuses on the accuracy of the identifying attributes. This is largely a function of the reliability of the source of the data and the trustworthiness of the person or system verifying the information. For example, identifying attributes (such as name, address, date of birth, or SSN) might be "verified" simply by asking the

[14] OECD Report at p. 7.

person being identified to provide the information. Alternatively, they might be verified by reference to an authoritative source of information, such as a driver's license, passport, or other government issued identity card, or even double-verified by checking with third-party sources. Obtaining the information from an individual "in person" is also generally considered more reliable than cases where it is done remotely. But in all cases the issue is, in essence, a question of trust – i.e., how much do I trust the veracity of the information provided? It is measured by reference to an "assurance level" (discussed below).

(2) Issuance of Credential

At the end of the identification process, a person's identity is typically represented by data in a paper or electronic document referred to as an identity ***credential***. A credential is data that is used to authenticate the claimed digital identity or attributes of a person.[15] In the physical world, examples of an identity credential include a driver's license, a passport, a library card, or an employee identification card. In the online world the identity credential may be as simple as a User ID, or as complex as a cryptographically-based digital certificate.

Electronic identity credentials typically contain a unique ***identifier*** (such as name, user ID, account number, Social Security number, etc.) along with the relevant identity attributes that describe or define the person to the level necessary for the purpose at hand (e.g., address, title, gender, membership status, date of birth, credit score, medical information, etc.). In addition, identity credentials are often associated with an ***authenticator*** (also called a ***token***) possessed and controlled by the person identified in the credential. The authenticator assures that the credential can be reliably associated with the specific person about whom it relates. The authenticator can be digital information, such as a secret known only to the individual (e.g., a password), or a physical object such as a smartcard or ATM card. A photo on a drivers license or a passport also serves as an authenticator. The authenticator and credential may then be used in subsequent authentication events.

With respect to both of the dimensions of identification, the nature of the process is critical. Before someone relies on an identity that is based on the results of an identification process, they need to be able to trust that the process is both appropriate for the task and that it was accurately conducted. Likewise, following completion of the identification process, the continuing security of the data and the authenticator (or token) is also a critical concern. If a new photo can be pasted into a driver's license, or if a password is lost or stolen, an identity thief can successfully claim to be the person identified by the credential created during the identification process.

(b) Authentication

When a person presents an identity credential (such as by inputting a User ID on a corporate network, or presenting a driver's license at an airport), claims to be the individual identified in the credential, and seeks to exercise a right or privilege granted to the individual named in the credential (e.g., to access the network or a sensitive database, to board a plane,

[15] OECD Guidance for Electronic Authentication (2007), at page. 12, available at: http://www.oecd.org/dataoecd/32/45/38921342.pdf.

etc.), an ***authentication*** process is used to determine whether that person is, in fact, who they claim to be.[16] In other words, once someone makes a declaration of who they are, authentication is designed to answer the question "OK, how can you prove it?" In essence, it is the process of establishing confidence in a person's claimed identity.

Typical legal definitions of authentication include: "the corroboration that a person is the one claimed,"[17] "utilizing digital credentials to assure the identity of users and validate their access,"[18] and a "procedure for checking a user's identity."[19] It is a transaction-specific event that involves verifying that the person trying to engage in the transaction really is the person that was previously identified and authorized for the transaction.

There are a variety of technologies and methodologies to authenticate individuals. These methods include the use of passwords, personal identification numbers (PINs), digital certificates using a public key infrastructure (PKI), physical devices such as smart cards, one-time passwords, USB plug-ins or other types of "tokens," transaction profile scripts, biometric identification, and others.[20]

In all cases, however, authentication is essentially performed by cross-checking a claimed identity against one or more authenticators, often referred to as "tokens," that are associated with or linked to that identity. An authenticator (or token) typically consists of one of the following *factors*:

- Something the person *knows* (e.g., a secret such as a PIN, password or other secret code);[21]
- Something the person *possesses* (e.g., a cryptographic key, an ATM card, a smart card, drivers license, or other physical token); or
- Something the person *is* (e.g., a biometric characteristic,[22] such as a fingerprint or retinal pattern).

---

[16] *See* U.S. Federal Rules of Evidence 901(a). *See also*, Federal Trade Commission Report, "Security in Numbers: SSNs and ID Theft" (FTC, December 2008), at p. 6; available at http://www.ftc.gov/opa/2008/12/ssnreport.shtm.

[17] HIPAA Security Regulations, 45 C.F.R. Section 164.304.

[18] Homeland Security Act of 2002 § 1001(b), amending 44 U.S.C. § 3532(b)(1)(D).

[19] Spain, Royal Decree 1720/2007 of 21 December, Which Approves The Regulation Implementing Organic Law 15/1999, of 13 December, on the Protection of Personal Data, Article 5(2)(b).

[20] Federal Financial Institutions Examination Council ("FFIEC"), "Authentication in an Internet Banking Environment," October 12, 2005, at p. 2; available at http://www.ffiec.gov/pdf/authentication_guidance.pdf (hereinafter "**FFIEC Guidance**").

[21] The use of a user name or user ID, coupled with a secret string of characters such as a password or PIN, is one of the most common authentication methods. The security provided by user IDs and passwords is, of course, dependent upon the password being kept a secret.

[22] A biometric identifier measures an individual's unique physical characteristic or behavior and compares it to a stored digital template to authenticate the individual. Thus, it represents "something the user is." Commonly used biometrics include a person's voice, fingerprint, hand or face geometry, the iris or retina in an eye, or the way the person signs a document or enters key board strokes. The security of a biometric identifier rests on the ability of the digitally stored characteristic to relate to only one individual in a defined population.

For example, when someone presents a driver's license, the biometric characteristic that comprises his face (something he "is") can be compared to the picture embedded in the license, and if they match, the person's claimed identity (e.g., name, age, etc. as stated on the license) is authenticated. Likewise, in the online environment, when an employee logs into the company network, his password (something he "knows") is checked against the password associated with his identity credentials stored on the company's server, and if they match, the employee's claimed identity (represented by the identifier known as a userID) is authenticated.

Authentication processes may require one or more of these factors. The online use of a password is *single factor authentication* (i.e., something the user knows), whereas an ATM transaction requires *two factor authentication* – i.e., something the user possesses (the ATM card) combined with something the user knows (the PIN number).[23] Properly designed and implemented multi-factor authentication methods typically are more difficult to compromise than single factor systems. As a result, they are more reliable indicators of authentication and stronger fraud deterrents.

(c) Authorization

Once a user is successfully authenticated, an *authorization* process determines what the user is allowed to access and use. It addresses the question "What can I do?" In other words, authentication of identity is not just an end in itself, but rather a process used to authorize some type of grant of rights or privileges (e.g., to access and use certain ecosystem resources), to facilitate a transaction or decision, or to satisfy an evidentiary obligation. For example:

- With respect to *computer ecosystems and networks*, authentication is often used for access control – e.g., to determine who is seeking access in order to ensure that only authorized persons are given the right to access a database of sensitive personal information or the right to transfer funds out of a bank account.

- With respect to *electronic communications*, authentication of identity can be used to assure the recipient of a message that the sender is who he or she (or it) claims to be so that the recipient can determine whether to proceed with the transaction. For example, when a bank receives an electronic payment order from a customer directing that money be paid to a third party, the bank must be able to verify the source of the request and ensure that it is not dealing with an impostor. This is a critical defense against identity theft.

- With respect to signed *electronically signed records*, authentication might be used to verify the identity of the signer. Someone seeking to enforce an electronic promissory note, for example, must be able to authenticate the identity of the signer. In this case, it serves an important evidentiary function.

[23] FFIEC Guidance, at p. 3.

In all cases, note that there is a clear difference between identification and authentication. *Identification* is the process of verifying a person's identity to a level sufficient for the intended purpose (such as during the hiring process or an account origination process) and usually occurs once. *Authentication* is the process of confirming that a person presenting him or herself as a previously identified person entitled to certain rights and privileges is, in fact, that person (such as when a person attempts to gain access to an online ecosystem), and typically occurs at the time of each transaction.

(d) Assurance Levels

Both identification and authentication are critical to access control and to otherwise stopping identity theft. Without reliable identification, one person can pose as another, and obtain an identity credential in another's name. And even with proper identification, if the authentication process fails – e.g., when an imposter successfully presents himself as someone else by using a stolen password – identity theft can occur. In other words, there are two basic ways an identity thief can succeed: (1) by compromising the identification process, or (2) by compromising the authentication process. Thus:

- With respect to the identification process, there is always the risk someone can misrepresent his or her identity, and if successful, obtain an identity credential in the name of someone else.

- With respect to the authentication process, there is the risk that, although a person was correctly identified based on legitimate documentation, the password or other authenticator (i.e., token) used to link that person to the resulting accurate identity credential might be compromised, thereby allowing an imposter to successfully complete the authentication process and steal such person's identity.

In light of these risks, a person relying on an authenticated identity must also consider the degree of confidence or trust that it has in both the identification and authentication processes. One approach to addressing these issues is to define various "assurance levels." Assurance levels are numerical assignments to objectively defined levels of reliability and "trust" associated with a given credential. The levels are each correlated with specific requirements regarding the technology, processes, policies and other elements that are applied to support the issuance and use of credentials online.

The "assurance level" describes the ***strength*** of the identification and authentication processes – i.e., it provides a basis for determining the degree to which a party to an electronic business transaction can be confident: (1) that the identity information being presented actually represents the person named in it (e.g., that the person who was identified as Bill Gates really was Bill Gates, and not an imposter), and (2) that the person identified in the credential is the person who is actually engaging in the electronic transaction (e.g., that it is really Bill Gates on the remote device who is seeking access to a company's system, and not someone who stole his password).[24]

[24] See, e.g., Liberty Alliance Project, Liberty Identity Assurance Framework, Version 1.1 (2008), at page 7; available at

The U.S. Federal government has defined four levels of assurance to describe the degree of certainty associated with identification and authentication processes. The four assurance levels range from little or no confidence in the asserted identity's validity (level 1), to some confidence (level 2), to high confidence (level 3), to very high confidence in the asserted identity's validity (level 4).[25] Since the assurance level is a function of the strength of the processes and the technology used in connection with the identification and authentication, the primary factors that affect the assertion level include:[26]

- The nature of the identity proofing processes: What was done do to vet the person's identity? – e.g., What kind of identity credentials were relied upon (e.g., passport or library card)? Was the process done in-person or remotely via the Internet?
- The authenticator (i.e., token) used: What kind of tokens were used for proving identity and how strong or reliable are they? – e.g., weak passwords, strong passwords, one-time password device tokens, cryptographic keys stored in hardware devices, etc.?
- The remote authentication mechanisms used: What is the combination of credential, authenticator (i.e., token) and authentication protocol[27] used to establish that a claimant is in fact the person he or she claims to be? – e.g., how resistant are they to eavesdroppers, imposters, and hijackers?

Obviously, different types of transactions will require different assertion levels, and not all transactions will require the highest assertion level. However, the confidence level that a business has in a particular identity, and its willingness to proceed with the transaction (e.g., to transfer the funds) or grant the requested privilege (e.g., access to a sensitive database) is clearly tied to assurance levels in some form. And the greater the risk of the transaction the greater the assurance level must be. Thus, in many developing identity management systems there is a focus on the strength of the identification and the authentication processes, even if not evaluated formally in terms of assurance levels.[28]

---

http://www.projectliberty.org/resource_center/specifications/liberty_alliance_identity_assurance_framework_iaf_1_1_specification_and_associated_read_me_first_1_0_white_paper (hereinafter "**Liberty Identity Assurance Framework**"); Office of Management and Budget, **"**E-Authentication Guidance for Federal Agencies," OMB Memo M-04-04, (December 16, 2003), at Section 2.1; available at http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf (hereinafter "**OMB Memo M-04-04**"). OMB Memo M-04-04 provides that: "assurance is defined as 1) the degree of confidence in the vetting process used to establish the identity of the individual to whom the credential was issued, and 2) the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued."

[25] OMB Memo M-04-04, Section 2.1.

[26] See, e.g., National Institute of Standards and Technology, "Electronic Authentication Guideline," Special Publication No. 800-63, Version 1.0.2, (April, 2006) at p. 2; available at http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf (hereinafter "**NIST Special Publication 800-63**").

[27] "An authentication protocol is a defined sequence of messages between a claimant and a verifier that enables the verifier to verify that the claimant has control of a valid token to establish his/her identity. An exchange of messages between a claimant and a verifier that results in the authentication (or authentication failure) of the claimant is a protocol run." NIST Special Publication 800-63, at p. 26.

[28] See, e.g., NIST Special Publication 800-63; Liberty Identity Assurance Framework.

A practical problem, however, is that achieving a higher assurance level often requires obtaining more personal information, thereby increasing the privacy risk. For while the strength of the identity credential and the authentication mechanism can be addressed technically (e.g., a hardware-based digital certificate is stronger than a mere password), the strength of the identification (or the identity proofing) is often a function of the amount of personal data collected about an individual. As one commentator has noted:

> Reliability of identity can be built up from a series of credentials and records . . . . This is an example of the principle that many bits of somewhat reliable data may aggregate into a bit of quite reliable information. If an individual presents a driver's license, automobile registration and insurance card for the same vehicle, all of which have the same name and address, that is, if they are mutually referential, a much stronger case can be made that the series of credentials reliably defines an identity. Add a mortgage account, a checking account, voter registration records, medical insurance account, and the overall confidence one has in the individual's identity grows even greater. Add to this list access to medical records (undesirable for reasons other than identity proofing, but then we are speaking here in the abstract) and credit history and the confidence in the individual's identity rapidly rises towards certainty, that is, the electronic credential issuer is just about 100% sure the individual presenting all these credentials – onerous as that surely would be – is who he or she claims to be.[29]

It should be noted, however, that the strength of the identity is also dependent on proper performance of the identity proofing and authentication processes. Because the assurance level determination focuses on the nature of the process and technology, and not on the risk that a participant will fail to perform its obligations, it does not necessarily address the performance risk discussed below (e.g., although an identification process may require an in-person review of two government-issued picture IDs, a willingness to circumvent that process and issue an identity credential based only on a telephone claim of identity will defeat the strength of that identity-proofing process).

2. Portable Identity Credentials – Federated Identity Management

Traditionally, each business entity and government agency has handled its own identity management. For example, a company would identify each of its employees and customers, and then issue them an identity credential (typically a user ID) and associate an authenticator or token (typically a password) to that User ID, so that those persons could be authenticated for remote network access. Only two parties are involved in this type of identity management process – the business and the individual to be granted access. And the credential and authenticator (User ID and password) could only be used with the business that issued it.

Today, however, businesses and government agencies increasingly want to: (1) use third parties to handle the difficult and often expensive tasks involved in identity management,

[29] Peter Alterman, "On the Reliability of Authentication of Identity," at pp. 4-5, 7; available at http://www.cio.gov/fpkipa/documents/ReliabilityAuthenticationIdentity.pdf

particularly in situations involving high volume or one-off transactions, or (2) leverage the identification and authentication previously done by a related business (e.g., a hotel and car rental company might want to rely on an airline's identification of a traveler). In addition, users, overloaded with user IDs and passwords are looking for a one-stop option. This is where a three-party identity management model, known as *federated identity management*, offers a promising solution for dealing with the cost and complexity of addressing these identity management problems.

Under a federated identity model, a business relies on an identification process performed, and identity information provided, by a third party. The goal is to facilitate the secure exchange of identity credentials between organizations – i.e., to enable the portability of identity information across different systems and entities. Thus it allows an individual to use the same identity credential and authenticator in order to conduct transactions with more than one enterprise.

Federated identity management (FIM) has been generally summarized by Ann Cavoukian, the Information and Privacy Commissioner of Ontario, as follows:

> Within the FIM model, identity credentials issued to a user by a particular service or institution are recognized by a broad range of other services. Though complex to implement online, this is similar in concept to, and can provide improvements over, traditional identification schemes in the "physical world." A typical example would be government-issued ID credentials (birth certificate, driver's license, passport, citizenship card, etc.), issued by an institution (a government agency), that is broadly recognized by others (as proof of name, address, age, etc.). The user of the service does not need to prove his/her identity with each transaction; rather, it is enough to show that he/she has, at some prior point, been authenticated by a trusted authority. The service's burden then lays, not in identification of the presenter but in the verification of presented credentials – a much less onerous task.[30]

Much work is being done by groups such as the Kantara Initiative,[31] the Open ID Foundation,[32] the Information Card Foundation,[33] the Organization for the Advancement of Structured Information Standards (OASIS),[34] the World Wide Web Consortium (W3C),[35] and others to develop technical specifications and online protocols that allow a business to authenticate the identity of a person seeking to access its systems by obtaining and validating

---

[30] Information and Privacy Commissioner of Ontario, "The New Federated Privacy Impact Assessment (F-PIA): Building Privacy and Trust-enabled Federation" (January, 2009), at p. 4; available at http://www.ipc.on.ca/images/Resources/F-PIA_2.pdf (hereinafter "**Privacy Commissioner of Ontario Paper**").

[31] http://kantarainitiative.org/, formerly known as the Liberty Alliance, http://www.projectliberty.org

[32] http://openid.net/foundation/

[33] http://informationcard.net/foundation

[34] http://www.oasis-open.org

[35] http://www.w3.org

online identity information provided by a third party. Most of that work, however, focuses on the practical and technical issues of communicating identity-related information in an inter-operable manner. The legal issues associated with federated identity management are often overlooked and have not been the subject of much discussion to date.

(a) The General Process

At its essence, identity management essentially involves two fundamental groups of processes: (1) the processes of identifying a person and issuing a credential to evidence that identity ("identification"), and (2) the processes of using that credential to later verify that a particular person claiming to be that previously identified person is, in fact, such person ("authentication"). Once an individual's identity is successfully authenticated, a third set of processes, referred to as "authorization," is used by the business relying on the authentication to determine what rights and privileges are accorded to such person – e.g., whether such person should be granted access to a database, an online bank account, a bar, an airport boarding area, a country, etc., whether to enter into a contract with such person, etc.

There are many different approaches to federated identity management, and the technical details and specifications of each approach can become quite complex, the following oversimplified summary of the generic process will help to put the legal issues in perspective:

- A party (called the *Identity Provider*) identifies a person (the *Subject*) and issues a digital identity credential to facilitate authentication of the Subject.

- Later, when the Subject wants something from a business or a government agency via a remote access (e.g., Internet access to a database or bank account), he uses that identity credential to assert his identity to that business as evidence of his right to obtain what he wants;

- Before the business or government agency (the *Relying Party*) grants the Subject's request, it wants to (1) authenticate the identity of the person claiming to be the Subject, and (2) in some cases, obtain certain information about the Subject (an *identity assertion*) before it allows the Subject to access its system or enter into a proposed business transaction. The Subject may, for example, be a customer 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 their financial account with the Relying Party. The information the Relying Party needs may be the Subject's account number, Social Security number, address, or membership status.

- To provide the required identity information, and facilitate the authentication process, the Identity Provider will then be asked to make an identity assertion about the Subject that contains the requested information.

- At the time of the transaction, the Subject is first authenticated by the Identity Provider[36] and then the identity assertion is communicated to the Relying Party (by either the Subject or the Identity Provider, depending on the system involved), the Relying Party validates the identity assertion to ensure that it is authentic and not revoked, and then relies on it to obtain the necessary information in order to grant access to a network or proceed with the proposed transaction.

A very common offline example of this federated identity process (although it was never intended as such) is the way we currently issue and use driver's licenses. Obtaining a driver's license begins with an in-person identification process conducted by a state's Department of Motor Vehicles (the Identity Provider), whereby selected identifying information (or attributes) about a person, such as name, address, date of birth, height, weight, and eye color, are collected and verified. Then following testing of eyesight and driving competence, the process culminates with the issuance of a driver's license (an identity credential) that identifies the individual with a unique driver's license number (the identifier), contains some of the identity attributes about the individual that were collected during the identification process (identity assertions), and includes a photograph of the person named in the license that was taken at the time the license was issued. The photograph functions as an authenticator – i.e., it is used to tie the person to the identity credential.

The person obtaining that license may later present it to a Relying Party (such as a security agent at an airport, or the bartender at a bar), claiming to be the person with the identity attributes stated on the driver's license. That third party will then attempt to verify that the person standing in front of him is the same person identified in the license by comparing the photo on the license to the person before him – i.e., he will attempt to "authenticate" the claimed identity asserted by that person. If successful, he will typically be willing to rely on the data stated in the identity credential (the identity assertions) for purposes of a transaction with such person. The bartender, for example, will rely on the identity assertion regarding age stated in the license to determine whether to serve alcohol to the license holder; the TSA agent will rely on the identity assertion regarding name stated in the license for purposes of determining whether such person is the same as the person named in the airline boarding pass, and thus entitled to enter the boarding area.

An online example of a federated identity arrangement (in a closed system) is the typical ATM transaction whereby an individual with an account at Bank A wants to obtain cash from an ATM machine operated by Bank B (with whom he has no relationship). The individual signs on to Bank B's ATM network using his ATM card (the credential) and password from Bank A. Through the ATM network, Bank B contacts Bank A to determine whether the individual is a valid customer of Bank A, to have Bank A authenticate the identity of the individual (i.e., did he

---

[36] Authentication can occur in various ways: the Relying Party can initiate an authentication request to the Identity Provider the Subject designates when logged onto an Relying Party, or the Subject can first authenticate at an Identity Provider and then access a Relying Party. In either case, the technology enables single sign-on in which the Identity Provider authenticates the Subject, thus allowing her access to protected resources at a Relying Party. Susan Landau, Hubert Le Van Gong, and Robin Wilton, "Achieving Privacy in a Federated Identity Management System," (2009) at Section 1.1; available at http://research.sun.com/people/slandau/Achieving_Privacy.pdf (hereinafter "Landau Article").

enter the correct password), and to obtain certain identity information about the individual from Bank A (e.g., whether his account has funds sufficient to cover the requested withdrawal, and the balance in his account so Bank B can print it on the transaction receipt).

In the future, a federated identity arrangement might allow a government agency, such as the Social Security Administration (as a Relying Party), to authenticate the identity of an individual (the Subject) seeking access to his or her Social Security records by relying on an identity assertion made by that person's bank (which has previously identified that Subject as part of its customer screening process, and thus is in a position to function as an Identity Provider). For the individual Subject, the online process would be simple. He might simply sign onto the SSA website using the user ID and password he uses to access his online bank account. The SSA would then send a message to the bank to verify that the individual's User ID and password is still valid, and to obtain an identity assertion from the bank that contains certain information confirming the Subject's identity. Then, when the process is completed and his identity authenticated, the SSA will grant him access to check his records or to redirect the automatic deposit of his Social Security payments. So long as a protocol exists for sharing the identity data between the bank and SSA, an individual can do business with SSA using the user ID and password (or other identity credential) issued by his bank, and the SSA can avoid the need for a costly identity proofing process for all citizens.

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

(b) Basic Roles, Functions and Duties

Three fundamental roles participate in every federated identity management ecosystem. These roles may be summarized as follows.

(1) Subject

The ***Subject*** is the human being, business entity, device, software application, or digital object being identified in a particular credential and that can be authenticated and vouched for by an Identity Provider. The person or thing being identified is often referred to as an "entity."

In the case where the Subject is not a legal person (such as device, software application, or digital object), a legal person (a human being or a legal entity such as corporation) must take responsibility for it, in which case it is often referred to as the "*Responsible Person*."

The conduct of the Subject (if a human being, or the Responsible Person in the case of devices, etc.) can directly affect the validity of the identification and authentication processes. Thus, to ensure accurate and reliable processes, the basic duties of the Subject typically include:

- Provide accurate information to the Identity Provider during the identification process (e.g., not omit or misrepresent any material fact, or otherwise engage in any identity fraud);
- Use the issued credential/token only for the purposes and types of transactions for which it was intended;
- Take reasonable steps to prevent the unauthorized use of the credential/token issued or registered to the Subject;
- Notify the Identity Provider [and Relying Parties where appropriate] if such credential/token is lost or compromised, used without authorization, and/or should otherwise be revoked (so that the Identity Provider can revoke or invalidate the credential/token and otherwise take steps to prevent someone from successfully using it to commit identity fraud);
- Assume responsibility for transactions where the credential/token was used by the Subject, or by a third party with authorization of the Subject

(2) Identity Provider

The ***Identity Provider*** (a/k/a credential service provider) has overall responsibility for the entire process of registering (enrolling) an applicant for an identity credential and for establishing the applicant's true identity through the identity proofing process, which involves the collection of identifying information and verification of identity against independent and authoritative sources.

The strength of the identity proofing process, and hence the trustworthiness of the resulting identification generally depends on four key factors:

- What – The applicant's identification documents or information being verified;
- Who – The person or ecosystem performing the collection and verification and the level of trust in each;
- How – The process of verifying the information and the authenticity of the identification documents
- Source – Whether the applicant's identification documents or information came from a trusted source.

The Identity Provider is primarily responsible for the validity and integrity of the identification process and the resulting identity credential, the accuracy of the identity assertions, and the privacy and security of the Subject's personal information in its control. Responsibilities often ascribed to the Identity Provider include:

- Properly and accurately identify Subjects in accordance with specified procedures, including –
  - Collect data of sufficient quality and quantity necessary to permit it to perform the proofing needed to issue the credential and token;
  - Ensure that all identity assertions are accurately based on current valid information that is properly authenticated (e.g., an employer should not issue an identity assertion for a terminated employee);

  - Where appropriate, use reasonable procedures to detect omissions or misrepresentations by the Subject;
- Properly issue each credential/token;
- Properly perform all identity assertion and authentication processes;
- Ensure that the transfer of the credential/token and identity assertion is secure to prevent interception or compromise by unauthorized persons, and to protect credential/token integrity;
- Provide to the Subject a capability to revoke a credential/token (to limit identity theft opportunities in the event that the Subject's token is compromised or the Subject no longer wants to participate);
- Provide to all Relying Parties a capability to validate each credential/token (so the Relying Party can determine whether the credential/token is still valid and can be relied upon);
- Where the Identity Provider retains and holds a Subject's credential/token –
  - Take reasonable steps to prevent the unauthorized access or use of the credential/token
  - Assume responsibility for third party unauthorized use of such credential/token;
- Protect the privacy and security of Subject's personal information (in all forms);
- Provide Subjects with appropriate notice, choice, access, and control of their personal data; and
- Comply with disclosed policies, practices and procedures for the identification and authentication processes (so that Relying Parties can identify assurance levels and determine the level of trust they should have in the resulting authentication and identity assertions).

(3) Relying Party

A ***Relying Party*** is any individual, business, organization or service that relies on identity claims made by an identity provider about a Subject. Such reliance often involves granting access to a service or database, or proceeding with a transaction. Examples include a website user relying on an SSL certificate that identifies the owner of a website he is visiting, a bank relying on a credential to identify a customer seeking to authorize a funds transfer, a business relying on a credential to grant access to a database, or a government agency relying on a credential to identify a citizen for the purposes of providing government services.

The Relying Party must ensure that its reliance on the identification and authentication processes are reasonable under the circumstances and that its use of the Subject's personal information is appropriate. Responsibilities often ascribed to the Relying Party include the following:

- Properly authenticate each credential/token and identity assertions before relying on it (e.g., by analogy, compare a claimant's face to the picture on the driver's license before relying on the data in the license);
- Validate the credential/token with the issuing Identity Provider before relying on it;

- Follow appropriate processes prior to relying on a credential/token and other Subject information received, and determine whether there are reasonable measures to reduce risk of inaccurate and fraudulent information;
- Limit its use and reliance on an identity assertion as appropriate for the circumstances (e.g., credentials issued with a low assurance level should not be relied upon in situations requiring a very high assurance level);
- Protect the privacy and security of the Subject's personal data, and restrict its use of that data in accordance with its disclosed privacy policy, practices and procedures, the requirements of the Trust Framework, and applicable law.

3. The Key Risks for Participants

The challenges of any identity management system fall into three general categories. First are the technological, process, and procedural challenges, such as implementing the required technology and establishing appropriate processes and procedures so that everything works properly, ensuring the inter-operability of identity assertion communications between Identity Providers and Relying Parties, and ensuring the security of Subject identity information. The second challenge is economic, and involves primarily dealing with the cost of deploying, coordinating, and using identity management systems. The third challenge is legal. It focuses on issues relating to the potential liability risk of the participants, the privacy and security of the Subject's identity information, and the mutual concerns of all participants (Subject, Identity Provider, and Relying Party) that everyone performs their obligations properly.

The legal risks to each participant in an identity system, and the significance of those risk will, of course, vary by the role such participant is fulfilling at any particular point in time. But as a general matter they fall into the following general categories:

(a) Technology Risk

Identity management relies on a variety of different technologies. These might include, for example, technologies used to create and secure data on various credentials and tokens, encryption technologies, data security technologies, and the like. While the technologies used in any given identity ecosystem will vary, it is critical to the operation of the system that the technologies utilized are appropriately designed to achieve the intended result, that they function properly and securely, and that they provide reliable and secure results. In other words, it is critical that they work properly.

Thus, one key risk to the participants in an identity ecosystem is the risk that one or more of the technologies employed for a particular IdM system do not function properly and/or do not achieve the intended result.

(b) Process Risk

In addition to technology, identity management relies on a variety of different processes and procedures, some of which are not technology-based, but rather consist merely of a series of steps performed by a person. Such processes and procedures might include, for example, the process for identity proofing an individual Subject, which might specify which identity

documents must be reviewed in person, or how identity might be verified online. Other processes relate to authentication,[37] verification of credentials, revocation of credentials, etc. While the processes used in any given identity ecosystem will vary, it is critical to the operation of the system that the processes utilized are appropriately designed to achieve the intended result, that they function properly and securely, and that they provide reliable and secure results. In other words, like the technology, it is critical that the processes and procedures work properly. For example, is the identity proofing process adequate to yield a trustworthy identification result?

Thus, another key risk to the participants in an identity ecosystem is the risk that one or more of the processes implemented for that particular identity ecosystem are not properly designed to yield a secure and trustworthy result.

(c) Performance Risk

Even if the technologies and processes used for an identity ecosystem are properly designed to yield a secure and trustworthy result, they will be of little value if they are not correctly implemented or properly followed by the persons responsible for using them.

Stated differently, an identity ecosystem model will not function properly, and the various participants will not be able to rely on it for online transactions, unless each participant adequately performs certain basic responsibilities. The failure of any participant to perform its obligations could lead to substantial harm to other participants. In fact, mere concern about the performance of a participant may lead to a lack of trust fatal to the overall ecosystem.

Thus, a key risk for all participants in an identity ecosystem is the risk that one of the other participants, on whose performance they rely, will not perform their obligations as required for the role in which they are acting. Only when this risk is reduced to an acceptable level will parties participate in an identity management ecosystem. Thus, for example, the security agent at an airport generally feels comfortable accepting the risk that a state has properly identified each person to whom it has issued a drivers license. If it did not, such identity credentials would not be accepted.

To mitigate this risk requires clearly defining the performance obligations of each role, utilizing a mechanism (e.g., statutory, contractual, and/or technological) to provide some assurance that the participants in each role will perform their obligations conducting performance audits where appropriate, and providing a remedy if someone does not.

(1) Identification

The foundation of any identity management ecosystem is the reliability of the identification of the Subjects. While the required identification attributes will vary depending on the circumstances, the reliability of that identification is critical for all parties. Failure of the identification process presents a major risk.

---

[37] See, e.g., Entity Authentication Assurance Framework, ISO/IEC 29115:2010 (Draft)

The risk of an improper identification can arise in several ways. First, there is the risk that the underlying identity documents and third party sources used by the identity provider are incorrect or fraudulent. Second, there is the possibility that the identity provider (or its subcontractor) will simply not do their job properly when performing the identity proofing process. And third, there is the possibility that the data collected during the identity proofing process will not be properly transmitted or transcribed when it is embodied in the resulting identity credential.

For Subjects the identification risk is a business concern (Will I be able to complete this online transaction, access this database, etc.?), an identity theft concern (Will someone be able to use my identity to successfully obtain a credential and complete a transaction in my name?), and a privacy concern (Will my personal information be protected?). For Identity Providers, the identification risk relates to the possibility that a flawed identification process may lead to a faulty identification (as well as an appropriate process that nonetheless results in a faulty identification) will result in harm to the Relying Party and/or the Subject, with the consequence that the Identity Provider may be liable for the damages incurred.

For Relying Parties, identification risk is both a liability concern (focused on the losses it will suffer if it relies on an inappropriate authentication or identity assertion),[38] as well as a legal compliance obligation. From a liability perspective, the Relying Party needs the assurance or trust necessary to enter into a particular online transaction, as well as some level of confidence that it can prove up the identity of the other party in court if that becomes necessary. At the same time, however, laws and regulations increasingly impose on businesses a duty to identify and authenticate the persons with whom they deal remotely. Thus, for many Relying Parties the use of identity management has become a legal obligation.

(2) Authentication

Even if the identification risk has been properly addressed, the parties must also address the possibility that a valid identity will not be properly authenticated. This could involve either the possibility that the identity of a legitimate subject cannot be properly authenticated, or alternatively, that a subject's identity can be falsely authenticated as applying to someone or something else. In the simple user ID and password scenario, for example, there is the risk that for whatever reason, the correct password does not work to authenticate the subject. Likewise, there is the risk that the correct password works, but has been stolen and improperly used by an imposter. In both cases the identification procedures were accurate, but the authentication procedures do not yield an accurate result.

Authentication risk can be affected by technology risk or performance risk. It can also arise independently, such as where a third party is able to unlawfully obtain a password or

[38] See, e.g., Steven B. Roosa and Stephen Schultze, "The 'Certificate Authority' Trust Model for SSL: A Defective Foundation for Encrypted Web Traffic and a Legal Quagmire," Intellectual Property & Technology Law Journal, Vol. 22, No. 11 at pp. 3-8 (November 2010) (noting the risk that a CA can easily issue an unauthorized yet technically valid SSL Certificate).

otherwise compromise the authentication system. At the end of the day, however, authentication risk refers to the risk that authenticating a claimed identity will yield an incorrect result.

The second key component of any identity management ecosystem is the ability to reliably authenticate identity. Thus, even where a Subject has been properly identified, participants in an identity ecosystem must address the risk that the authentication process can be compromised (e.g., the stolen password problem).

(d) Privacy Risk

By its nature, any form of federated identity management involves the collection (by an Identity Provider) and disclosure (to a Relying Party) of personal information about a Subject. Thus, "the foundational issue in approaching any [identity management] system is personal information – how it is collected, stored, shared, and used."[39] Moreover, by its nature, federated identity management "presents a new challenge to privacy," in that transfers of personal information routinely occur between organizations as well as between the individual and an organization, and may frequently cross industry sectors and jurisdictional boundaries in the process.[40]

Privacy risk focuses on the possibility that personal data collected as part of the identity proofing process will be misused by one of the parties who has access to it (typically the identity provider and subsequent Relying Parties), or that the personal information will be compromised or otherwise improperly disclosed. Privacy risk in many respects is a function of technology risk and performance risk. However, it may go beyond those two risks in that the use or protection of the personal information in certain ways may not be required by the applicable system rules, or, in addition to the rules, may be regulated by existing law.

The privacy risk for Subjects focuses on the protection and use of their personal information by Identity Providers, Relying Parties, and other third parties, the resulting possibility of inappropriate use, disclosure, and compromise, and the harms that may result, such as identity theft, unauthorized account access, embarrassment, etc. And this risk relates not only to the information provided by the Subjects, but also information about the Subjects collected from third parties, as well as metadata and transaction data about Subjects generated as a result of their online activities.

For Identity Providers and Relying Parties, the privacy risk involves navigating the challenges of compliance obligations and restrictions that might inhibit their ability to achieve their goals. Laws and regulations may regulate or restrict their collection and use of personal information, as well as impose a variety of obligations to protect the information.[41] In addition,

---

[39] Office of Science and Technology Policy (OSTP), National Science and Technology Council (NSTC), Subcommittee on Biometrics and Identity Management, "Identity Management Task Force Report 2008," (September 2008) at p. 16; available at http://www.ostp.gov/galleries/NSTC%20Reports/IdMReport%20Final.pdf (hereinafter "**OSTP Report**").

[40] Privacy Commissioner of Ontario Paper, at p. 7, 13.

[41] This includes, e.g., GLB, HIPAA, state data security laws, etc., as well as the data protection laws in other countries, including the EU, Argentina, Australia, Canada, Hong Kong, Japan, and South Korea.

restrictions on cross-border transfers and other forms of use or sharing of such information may have an impact. Failure to address these obligations may result in penalties and fines, as well as potential liability for any harms suffered by the Subjects themselves.

(e) Data Security Risk

Data security is critical to any identity management system. This includes not only the security necessary to protect the personal information collected and communicated to relying parties, but also the security of the other data and corresponding processes necessary to create secure identity credentials, communicate accurate identity assertions, and verify the status of identity credentials. Thus, security risk refers to the risk that an unauthorized party obtains access to personal data or is able to otherwise compromise the overall functioning of the system. For some participants, such as identity providers and relying parties, data security risk may also relate to the possibility of a failure to comply with existing applicable law.

(f) Liability Risk

Things that can go wrong in an identity management system typically result from faulty identification, faulty authentication, inadequate security for or misuse of personal data, or failure to follow appropriate procedures. They can lead to two primary harms. First, a Relying Party and/or a Subject may suffer damages when the Relying Party acts (a) in reliance on a false identity credential or identity assertion that it thought was valid (e.g., by granting access to, or entering into an unauthorized transaction with, an imposter), or (b) fails to act in reliance on a valid identity credential that it mistakenly believes to be false. Second, a Subject may suffer damages when (a) his or her personal information is misused or compromised by the Identity Provider or a Relying Party or other third party to whom it has been disclosed, or (b) when the Subject is improperly denied access or the ability to conduct a transaction he is otherwise entitled to do.

Thus, a primary concern of all participants in any identity federation is determining who will bear the risks associated with these problems and their consequences. All participants in an identity ecosystem must address the risk that they will be held liable for damages resulting from a problem from which they are deemed legally responsible.

Liability risk is frequently cited as a primary concern by businesses considering participation as an identity provider, and in some cases even as a relying party. It is also sometimes cited as a concern by potential subjects, who fear that obtaining an identity credential may simply lead to liability for its improper use in the event they are unable to adequately secure it.

It should be noted that liability risk refers not only to the possibility that a participant may be required to pay damages to another participant within the identity ecosystem. It also includes the possibility that a participant may have a responsibility for damages suffered by third parties outside of the identity ecosystem (e.g., victims) who might not be constrained by the rules of the legal framework governing the identity ecosystem.

Numerous statutory, common law, and contract theories have been advanced to identify, define, and clarify the source and scope of the potential liabilities of each of the participants in an identity ecosystem.[42] Yet, in many respects, federated identity management is a business model for which the law has not yet had time to adapt. Thus, a key aspect of the liability risk is the legal uncertainty regarding the responsibility that attaches to any given action or failure to act by a participant in an identity ecosystem. This uncertainty only enhances the nature of the liability risk and in many cases has dissuaded companies from participating in an identity ecosystem.

(g) Enforceability Risk

If one participant in an IdM system fails to perform as required, the other participants must consider their ability to (i) identity the fact of such failure of performance, (ii) stop and/or remedy such failure, and (iii) obtain redress and/or compensation for any losses suffered as a result. Concerns regarding each of these three elements are the focus of enforceability risk.

It should be noted that this risk applies not only when something goes wrong and someone seeks to recover damages, but also in situations where a problem has not yet surfaced, but a failure of performance on the part of one or more participants puts the system at risk. For example, the failure by an identity provider to properly perform the identity proving process, even though it has not yet resulted in any inaccurate credentials, is a concern for other participants in the identity system. In such case, enforceability risk refers both to the ability to detect that problem, as well as the ability to require the participant to remedy its performance or withdraw from the system.

(h) Regulatory Compliance Risk

In many cases, participation in an identity system raises legal compliance issues. In some cases, those issues relate to whether the conduct of the participant complies with applicable law. For example, the manner of collection, use, and storage of personal data by the identity provider, and the subsequent receipt and use of that information by a relying party, must comply with applicable privacy laws. Acting contrary to the requirements of those laws poses a compliance risk to the participant.

In other cases, participation in the identity system is, itself, done in an effort to comply with legal requirements imposed on a participant. For example, a financial institution may participate, and rely on identity credentials, in order to satisfy its legal obligations to properly authenticate persons granted online access to bank accounts and payment facilities. In such cases, whether the participant adequately satisfies its compliance obligations will depend, at least in part, on the trustworthiness of the identity system.

---

[42] See Thomas J. Smedinghoff, "Certification Authority Liability Analysis" (study for the American Bankers Association, discussing potential liability risks of an Identity Provider operating as a certification authority); available at http://www.wildman.com/resources/articles-pdf/ca-liability-analysis.pdf (hereinafter "**Smedinghoff CA Liability Analysis**").

4. Addressing Risks – The Need for a Legally Binding Trust Framework

There are many technologies and identity management standards[43] to ensure that personal information moving between organizations is securely transferred and can be read and understood by the systems of all parties. Encryption and digital signature technology, for example, is used to protect the security of the information flows, ensure the integrity of the identity credentials, and to authenticate the Identity Provider to the Relying Party. And technical standards are critical to ensuring the inter-operability of communications across various systems and networks. Without agreement on standards, different networks and systems would be unable to talk to each other and exchange information in a manner that can be understood by either system. But as one commentator has noted regarding the technology: "Ultimately, though, the protection here is legal. A rogue [Relying Party] or Identity Provider is in a position to violate a [Subject's] privacy and *technical protections can only reduce, not eliminate this risk*."[44]

The ultimate goal of any identity system is to provide identity assertions that are sufficiently reliable for the intended purpose,[45] and to do so in a manner such that all of the relevant parties are willing to participate and to rely on the results. Achieving that goal requires building a "Trust Framework" for each identity system that addresses both the operational requirements and the legal rules necessary to define a trustworthy identity system. This is sometimes referred to as the "tool and rules" of an identity system.

The concept of a Trust Framework is often referred to in discussions of identity management systems,[46] but usually without a detailed analysis and often in an inconsistent manner. Generally, however, a Trust Framework may be defined as follows:

---

[43] See, e.g., Liberty Alliance specifications at http://www.projectliberty.org/liberty/specifications_1; National Institute of Standards and Technology, Federal Information Processing Standards Publication FIPS Pub. 201-1 "Personal Identity Verification (PIV) of Federal Employees and Contractors" (March 2006); CA/Browser Forum, "Guidelines for the Issuance and Management of Extended Validation Certificates" (2008) at Part F; available at http://cabforum.org/EV_Certificate_Guidelines_V11.pdf.

[44] Landau Article, Section 3.2 (emphasis added).

[45] Recognizing that the intended use will vary, and thus so will the requirements necessary to make it sufficiently trustworthy *for that purpose*.

[46] Examples of the various definitions of a Trust Framework include: **CDT:** "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." See "CDT Discusses Key Policies Issues Surrounding User-Centric Identity Management" at http://www.cdt.org/policy/cdt-discusses-key-policies-issues-surrounding-user-centric-identity-management; **GSA-ICAM:** Definition of Trust Framework: "Trust Framework Provider processes and controls for determining an identity provider's compliance to OMB M-04-04 Levels of Assurance." See ICAM Trust Framework Provider Adoption Process (TFPAP) For Levels of Assurance 1, 2, and Non-PKI 3, at p. 42, available at http://www.idmanagement.gov/documents/TrustFrameworkProviderAdoptionProcess.pdf; **Kantara:** "In electronic communication, a *Trust Framework* (TF) is a complete set of contracts, regulations or commitments that enable participating actors to rely on certain assertions by other actors to fulfill their information security requirements." See Trust Framework Architecture webpage at http://kantarainitiative.org/confluence/display/idassurance/Trust+Framework+Architecture#TrustFrameworkArchitecture-WhatisaTrustFramework%3F; **NSTIC – June 25 Public Release:** Definition of Trust Framework: "The underlying structure of standards and policies that defines the rights and responsibilities of the various participants in the Identity System, specifies the rules that govern their participation, outlines the processes and procedures to

A Trust Framework is a set of documents developed or tailored for a specific identity system, which sets forth:

- the ***Operational Requirements*** for the identity system (such as technical and functional specifications, processes, standards, policies and rules) that have been developed to ensure the proper operation of the system and to provide adequate assurance regarding the accuracy, integrity, privacy and security of its processes;~~,~~ and
- the ***Legal Rules*** that govern the identity system and that make the Operational Requirements legally binding on and enforceable against the participants, regulate the content of the Operational Requirements, and define and govern the legal rights, responsibilities, and liabilities of the participants of the identity system.

The **Operational Requirements** of a Trust Framework will likely consist of several different components addressing a variety of key operational and policy issues. While the content and structure of these components will vary from one identity system to another, the Operational Requirements of each Trust Framework will likely include common core components, such as an identity proofing component,[47] an authentication component,[48] a credential management component, a privacy component,[49] a security component, an assessment/audit component.[50]

Each component of the Operational Requirements establishes the technical specifications, processes, standards, policies, rules and performance requirements necessary to address one or more issues of importance to the operation of the identity system. Taken together they form the Operational Requirements necessary to ensure that the identity system operates properly and in a manner that all parties trust will be appropriate for the task.

The **Legal Rules** complete the Trust Framework by rendering the various components of the Operational Requirements binding and enforceable.

---

provide assurance, and provides the enforcement mechanisms to ensure compliance." NSTIC, at p. 34; available at http://www.dhs.gov/xlibrary/assets/ns_tic.pdf; **OIX:** "In digital identity systems, a *Trust Framework* is a certification program that enables a party who accepts a digital identity credential (called the *relying party*) to trust the identity, security, and privacy policies of the party who issues the credential (called the *identity service provider*) and vice versa." http://openidentityexchange.org/what-is-a-trust-framework; http://openidentityexchange.org/how-it-works/what-is-a-trust-framework; and **OpenID:** A Trust Framework is "a set of technical, operational, and legal requirements and enforcement mechanisms for parties exchanging identity information" The Open Identity Trust Framework (OITF) Model, p. 2; available at http://openidentityexchange.org/sites/default/files/the-open-identity-trust-framework-model-2010-03.pdf

[47] NASPO is currently developing an ANSI standard for such an identity proofing framework.

[48] See, e.g., Entity Authentication Assurance Framework, ISO/IEC 29115:2010 (Draft)

[49] Kantara is currently developing a Privacy Framework component for a Trust Framework.

[50] See, e.g., _____.

The Legal Rules consist of both existing statutes and regulations (i.e., publicly-created law), and agreements between or among the participants (i.e., privately-created law). They affect the Trust Framework in three ways:.

- They make the specifications, standards, and rules comprising the various components of Operational Requirements legally binding on and enforceable against each of the participants.
- They define the legal rights and responsibilities of the parties, clarify the legal risks parties assume by participating in the Trust Framework (e.g., warranties, liability for losses, risks to their personal data); and provide remedies in the event of disputes among the parties, including methods of dispute resolution, enforcement mechanisms, termination rights, and measures of damages, penalties and other forms of liability.
- In some cases, they also regulate the content of the Operational Requirements.

The Legal Rules may be set out in numerous contracts at varying management and execution layers, depending on the governance structure used. In many cases they operate as gap-fillers with respect to issues not addressed by the existing law. Where existing laws address issues in a permissive rather than mandatory manner, the Legal Rules may also express the choices of the parties among legally permissible alternatives. And in both cases they can have the effect of providing the legal certainty and predictability necessary to encourage participation

The relationship between the Operational Requirements and Legal Rules of a Trust Framework is similar to the relationship between a contract and several sets of technical specifications attached to the contract as exhibits. Execution of the contract is what creates a legally binding relationship between the parties; the specifications in the exhibits detail the parties' expectations of how the contract will be performed. While it might be possible for the parties to work together with reference only to the specifications, by incorporating them into a contract, the technical specifications give rise to legally enforceable rights and responsibilities.

In some cases, Trust Frameworks may be developed by a single entity, often referred to as a Trust Framework Provider, which is established to provide both the Trust Framework and the governance infrastructure needed to support it. Such an entity may be established by a group of companies or an industry sector that require a legally binding Trust Framework in order to work together efficiently.

Examples of such Trust Framework Providers include IdenTrust, Inc.[51] which has established an identity Trust Framework for the financial sector, the SAFE-BioPharma Association,[52] which has established an identity Trust Framework for the pharmaceutical sector, and CertiPath,[53] which has established an identity Trust Framework for the aerospace sector. Trust Frameworks may also be established by a single entity for its own purposes. Examples of this approach include Trust Frameworks established by governments.

[51] http://www.identrust.com

[52] http://www.safe-biopharma.org

[53] http://www.certipath.com

Glossary

Attribute. Personal information concerning a specific category or characteristics of a given identity, such as name, address, age, gender, title, salary, health, net worth, driver's license number, Social Security number, etc.

Authentication. The process of establishing or confirming that someone is who they claim to be. The process by which a person verifies or confirms their association with an electronic credential. For example, entering a password that is associated with a UserID or account name is assumed to verify that the user is the person to whom the UserID was issued. Likewise, comparing a person presenting a drivers license to the picture appearing on the license verifies or confirms that he/she is the person described in the license.

Authenticator. Something (usually uniquely in the possession of a person) that is used to determine authenticity; usually an object, an item of knowledge, or some characteristic of its possessor that is used to tie a person to an identity credential (such as by demonstrating that such person has possession of the authenticator). Also called a token. A password functions as an authenticator.

Authenticity. The property that data originated from its purported source

Authorization - A process of controlling access to information or resources only to those specifically permitted to use them. The actions that an authenticated person or entity is permitted as a result of the authentication.

Claim. An assertion made by a person with respect to one or more identity attributes of a Subject, which assertion typically is disputed or in doubt.

Credential – A digital document that binds a person's identity (and optionally, additional attributes) to a token possessed and controlled by a person. Data that is used to establish the claimed attributes or identity of a person or an entity. Paper credentials are documents that attest to the identity or other attributes of an individual or entity called the Subject of the credentials. Some common paper credentials include passports, birth certificates, driver's licenses, and employee identity cards.

According to National Institute of Standards and Technology Special Publication 800-63 (NIST SP 800-63),[54] a credential is, ―an object that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a person.[55] Credential management

[54] NIST SP 800-63, Version 1.0.2, Electronic Authentication Guidance, April 2006; available at http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

[55] The credentialing process principals and elements can also be applied for NPE digital identities; however, steps may vary during the credential issuance process (sponsorship, adjudication, etc.) based on an organizations security requirements. For examples of an NPE credential issuance please refer to the X.509 Certificate Policy for the E-Governance Certification Authorities, available at www.idmanagement.gov/fpkipa/documents/EGovCA-CP.pdf

supports the lifecycle of the credential itself. In the Federal Government, examples of credentials are smart cards, private/public cryptographic keys, and digital certificates. The policies around credential management, from identity proofing to issuance to revocation, are fairly mature compared to the other parts of ICAM. The PIV standards [Federal Information Processing Standards 201 (FIPS 201), SP 800-73, etc.] and Federal PKI Common Policy are examples of documents which have been in place and are foundational to agency-specific credential implementations.[56] Credentials are a tool for authentication.

Enrolment. The process by which organizations verify an individual's identity claims before issuing digital credentials.

Identification. The process of verifying and associating attributes with a particular person designated by an identifier.

Identifier. Something that points to an individual, such as a name, a serial number, or some other pointer to the party being identified. Since a person's legal name is not necessarily unique, the identifier of a person must include sufficient additional information (for example an address, or some unique identifier such as an employee or account number) to make it unique. For a typical login account, the User ID is the identifier and the password is the authenticator.

Identity. A unique name of an individual person (an identifier), and any associated attributes; the set of the properties of a person that allows the person to be distinguished from other persons. [See also "Digital Identity"]

Identity Assertion. An electronic record sent by an Identity Provider to a Relying Party that contains the Subject's identifier (e.g., name, account number, etc.), authentication status, and identity attributes. The attributes are typically personal information about the Subject relevant to the transaction that is required by the Relying Party.

Identity Management. The combination of technical systems, rules, and procedures that define the ownership, utilization, and safeguarding of personal identity information. The primary goal of identity management is to establish a trustworthy process for assigning attributes to a digital identity and to connect that identity to an individual.[57] Identity management includes the processes for maintaining and protecting the identity data of an individual over its lifecycle.[58]

Identity Proofing. The process by which an Identity Provider validates sufficient information to uniquely identify a person.

Identity Provider. An entity that creates, maintains, and manages identity information for Subjects. It authenticates and vouches for the Subject to Relying Parties.

---

[56] FICAM Roadmap at pp. 10-11.

[57] Identity Management Task Force Report, National Science and Technology Council (NSTC) Subcommittee on Biometrics and Identity Management, 2008.

[58] FICAM Roadmap, at p. 9.

Relying Party. An entity that provides services to a Subject, or otherwise has a need to authenticate the identity of the Subject, and that relies on an Identity Provider for identity and authentication of the Subject, typically to process a transaction or grant access to information or a system. The entity or person that is relying on an identity credential or assertion of identity to make a decision as to what action to take in a given application context.

Role. A type of participant in a federated identity system, such as a Subject, Identity Provider, or Relying Party. Note that each such role does not necessarily represent a different entity. For example, with respect to the identification of its employees, an employer may function as both an Identity Provider and a Relying Party.

Strength. The technical and procedural basis on which to believe that a particular process or data attribute is accurate.

Subject. The person that is identified in a particular credential and that can be authenticated and vouched for by an Identity Provider

Token. Something that a person possess and controls (either a unique physical object or secret data or information) that is used to authenticate his or her identity (such as a secret password, PIN, cryptographic key, ATM card, USB token, etc.). Tokens are physical devices or electronic records designed for use in authentication systems and/or to hold authenticating information. These include smart cards and ATM cards as well as digital certificates. Also called an authenticator.

Trust Framework. A Trust Framework is a set of documents developed or tailored for a specific identity system, which sets forth:

- the ***Operational Requirements*** for the identity system (such as technical and functional specifications, processes, standards, policies and rules) that have been developed to ensure the proper operation of the system and to provide adequate assurance regarding the accuracy, integrity, privacy and security of its processes and data; and
- the ***Legal Rules*** that govern the identity system and that make the Operational Requirements legally binding on and enforceable against the participants, regulate the content of the Operational Requirements, and define and govern the legal rights, responsibilities, and liabilities of the participants of the identity system.

Trust Framework Provider. The entity or organization that creates or adopts the Legal Framework (and all of the other frameworks that comprise the Trust Framework), and then certifies various participants that are in compliance with that Trust Framework. Organizations such as Visa, MasterCard, and American Express fulfill a similar role in the credit card world. They make the rules enforce compliance.

List of Papers and Reports
Cited in Footnotes

1. Peter Alterman, "On the Reliability of Authentication of Identity;" available at http://www.cio.gov/fpkipa/documents/ReliabilityAuthenticationIdentity.pdf

2. European Commission, "Action Plan on e-signatures and e-identification to facilitate the provision of crossborder public services in the Single Market," COM(2008) 798 final (28 November 2008); available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0798:FIN:EN:PDF

3. **FFIEC Guidance:** Federal Financial Institutions Examination Council ("FFIEC"), "Authentication in an Internet Banking Environment," October 12, 2005; available at http://www.ffiec.gov/pdf/authentication_guidance.pdf

4. Jacques R. Francoeur and Edward Chase, "Digital Signature Assurance & the Digital Chain of Evidence," Version 1.0, January 2009; [copy on file with author]

5. **FTC SSN Report:** Federal Trade Commission Report, "Security in Numbers: SSNs and ID Theft" (FTC, December 2008); available at http://www.ftc.gov/opa/2008/12/ssnreport.shtm

6. Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors; available at http://www.dhs.gov/xabout/laws/gc_1217616624097.shtm

7. **Landau Article:** Susan Landau, Hubert Le Van Gong, and Robin Wilton, "Achieving Privacy in a Federated Identity Management System,**"** (2009); available at http://research.sun.com/people/slandau/Achieving_Privacy.pdf

8. **Liberty Privacy & Security Paper:** Liberty Alliance Project, "Privacy and Security Best Practices," v.2.0 (November 12, 2003); available at http://www.projectliberty.org/liberty/resource_center/papers/liberty_alliance_privacy_and_security_best_practices

9. **Liberty Circles of Trust Paper:** The Liberty Alliance Project, "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

10. **Liberty Identity Assurance Framework:** Liberty Alliance Project, Liberty Identity Assurance Framework, Version 1.1 (2008); available at http://www.projectliberty.org/resource_center/specifications/liberty_alliance_identity_assurance_framework_iaf_1_1_specification_and_associated_read_me_first_1_0_white_paper

11. National Security Telecommunications Advisory Committee, "**NSTAC Report to the President on Identity Management Strategy**," May 21, 2009; available at www.ncs.gov/nstac/reports/2009/NSTAC%20IDTF%20Report.pdf

12. **NIST Special Publication 800-63:** National Institute of Standards and Technology, "Electronic Authentication Guideline," Special Publication No. 800-63, Version 1.0.2, (April, 2006); available at http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

13. **NSTIC:** "**National Strategy for Trusted Identities in Cyberspace**," (June 25, 2010); available at http://www.dhs.gov/xlibrary/assets/ns_tic.pdf

14. Organisation for Economic Co-operation and Development (OECD) Recommendation on Electronic Authentication and OECD Guidance for Electronic Authentication, June 2007; available at http://www.oecd.org/dataoecd/32/45/38921342.pdf

15. **OECD Report**: OECD Working Party on Information Security and Privacy, The Role of Digital Identity Management in the Internet Economy: A Primer for Policy Makers**,** DSTI/ICCP/REG(2008)10/FINAL, (June 11, 2009); available at http://www.oecd.org/dataoecd/55/48/43091476.pdf

16. Thomas Olsen & Tobias Mahler, "Identity Management and Data Protection Law: Risk, Responsibility and Compliance in 'Circles of Trust,'" Computer Law & Security Report Vol. 23(4) (2007); available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1015006

17. **OMB Memo M-04-04:** Office of Management and Budget, **"**E-Authentication Guidance for Federal Agencies," OMB Memo M-04-04, (December 16, 2003); available at http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf

18. **OSTP Report:** Office of Science and Technology Policy (OSTP), National Science and Technology Council (NSTC), Subcommittee on Biometrics and Identity Management, "Identity Management Task Force Report 2008," (September 2008); available at http://www.ostp.gov/galleries/NSTC%20Reports/IdMReport%20Final.pdf

19. **Privacy Commissioner of Ontario Paper:** Information and Privacy Commissioner of Ontario, "The New Federated Privacy Impact Assessment (F-PIA): Building Privacy and Trust-enabled Federation" (January, 2009); available at http://www.ipc.on.ca/images/Resources/F-PIA_2.pdf

20. Mary Rundle and Ben Laurie, "Identity Management as a Cybersecurity Case Study," The Berkman Center for Internet & Society, Research Publication No. 2006-01 (September 2005); available at http://cyber.law.harvard.edu/node/418 and http://ssrn.com/abstract=881107

21. **Smedinghoff CA Liability Analysis:** Thomas J. Smedinghoff, "Certification Authority Liability Analysis" (study for the American Bankers Association, discussing potential liability risks of an Identity Provider operating as a certification authority); available at http://www.wildman.com/resources/articles-pdf/ca-liability-analysis.pdf

22. Thomas J. Smedinghoff, "The State of Information Security Law: A Focus on the Key Legal Trends," EDPACS, The EDP Audit , Control, and Security Newsletter (January – February 2008 Vol. XXXVII, Nos. 1–2); available at http://ssrn.com/abstract=1114246

23. **Transition Study Group Report**: Industry Advisory Council Transition Study Group, "Identity and Access Management," (December 9, 2008); available at www.actgov.org/knowledgebank/studies/Documents/Transition%20Study%20Group%20Papers/Identity%20and%20Access%20Management,%20IAC,%2012-9-2008.pdf

24. Heather West, Center for Democracy & Technology, "Issues for Responsible User-Centric Identity," (November 2009, Version 1.0); available at http://www.cdt.org/paper/issues-responsible-user-centric-identity.

25. Whitehouse "**Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure**," (May 2009); available at http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf