ARTICLE:

# FEDERATED IDENTITY MANAGEMENT: ENABLING LEGAL CONTROL OVER DIGITAL PROPERTY IN THE CLOUD

By **Timothy S. Reiniger, Esq.** and **Dr Richard J. Hansberger, Esq.**

Cloud computing raises important security considerations concerning data at rest, in use, and in transit especially with respect to the manner in which content level protective controls are enforced while data is moved from the data holder to the cloud provider.[1] While operational responsibility shifts from data holders[2] to the Cloud Service Provider (CSP), the data owners and holders still have legal responsibility for setting and implementing the necessary data level protections, including access and usage controls.[3]

The strategic management of information assets in the cloud must be based on fundamental evidentiary requirements for proving authenticity and reliability.[4] In particular, cloud computing poses three critical legal problems that are related to the current crises involving identity authentication, data authenticity and use authority.

First, there is the crisis involving the capability of authenticating identity remotely or on-line. The globalization system is built on integration and speed.[5] Both of these require trust in the capability to identify and authenticate individuals who seek to obtain access to networks, share information, and sign documents. Therefore, proving attribution and custodial control are the main evidentiary concerns for archived documents, especially when physical connection is not practical or even possible due to the possession of data by third parties.[6] It is necessary to know who has access to the digital information held by the cloud provider and whether alterations were made by that person or entity.

Second, there is the crisis involving the authenticity of data.[7] Because of the ephemeral nature of digital data, unlimited copying and geographic locations of digital information, and ubiquity of network access to documents, distinguishing between authentic and forged digital records is a central evidentiary concern. It is useful to know the nature of the evidence that is required to establish authenticity of digital information in the cloud.

Third, there is the matter of dealing with the current crisis regarding authority and control over proprietary data and information.[8] The interconnected global digital

1 *Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing V2.1 (December 2009) at 21.*

2 *For reference, see the discussion in "Determining Cloud Access and Use Levels" section of this article concerning the relative rights and duties of data holders and the associated level of Dominium. The term 'data holder' includes 'data owners' and 'informational rights owners,' all of whom have a relative level of legal control or Dominium over the digital information. In nearly all states in the United States, the pre-founding prevailing English common law is a legal source in the absence of statute. See, e.g. VA. CODE ANN. § 1-200. Currently, cloud computing is not statutorily regulated at the federal or state levels.*

3 *Cloud Security Alliance at 41-42; Wayne Jansen and Timothy Grance, NIST Draft Special Publication 800-144, Guidelines on Security and Privacy in Public Cloud Computing, (January 2011) at 3-6, 17, and 24-25.*

4 *Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing V2.1 (December 2009) at 9-10 and 35-36; Wayne Jansen and Timothy Grance, NIST Draft Special Publication 800-144, Guidelines on Security and Privacy in Public Cloud Computing (January 2011) at 14-16 and 24-25. See also, Internet Security Alliance and the American National Standards Institute, The Financial Management of Cyber Risk: An Implementation Framework for CFO's (2010) at 31-38 and Thomas J. Shaw, Information security and Privacy: A Practical Guide for Global Executives, Lawyers, and Technologists (American Bar Association, 2011) at 2-13 (describing the control requirements for the information security and privacy lifecycle).*

5 *Thomas L. Friedman, The Lexus and the Olive Tree (Anchor Books, 2000) at 8 and 10.*

6 *For instance, see Office Depot Inc. v. Zuccarini, 596 F.3d 696, 701 (9th Cir. 2010) (the location or situs of intangible property is context-specific and varies depending on the purpose to be served).*

7 *George Paul, Foundations Of Digital Evidence (American Bar Association, 2008) at xxvi (' Society must come to grips with whether it currently has an ability to learn the truth about everyday communications, agreements, transactions, and indeed all types of records of digital information…The problem is its untestability' ; George L. Paul, ' The 'Authenticity Crisis' in Real Evidence', 15 PRAC. LITIGATOR No. 6 (2004) at 212-13. For an historical comparison, see the discussion in the twelfth and thirteenth centuries of common law evidentiary proof standards for authenticating paper writings in M. T. Clanchy, From Memory to Written Record (Blackwell Publishing, 1993) at 324 (' [W]ithout defined standards of authenticity, there could be no definite criteria for distinguishing forgeries from authentic documents.' ); Harold Berman, Law and Revolution: The Formation of the Western Legal Tradition, (Harvard University Press, 1983) at 4-8 and 39. The historical development of the common law provides an important and continuing basis for legal analysis of new technologies.*

8 *Jeremy Rifkin, The Age of Access (Tarcher Putnam, 2000) at 11-15 and 177-79; Rod Beckstrom and Magnus Graf Lambsdorff, The Starfish and The Spider: The Unstoppable Power of Leaderless Organizations (Penguin Portfolio, 2006) at 5 and 35, and Thomas L. Friedman, The Lexus and the Olive Tree, at 8. And, of course, US Representative Weiner's now infamous attempt to claim his Facebook account had been hacked rested entirely upon the fact that such accounts are commonly hacked.*

network-based economy has served as a decentralizing force.[9] No person or entity is in charge.[10] Therefore, proof of control over network access and digital information is an important evidentiary requirement for establishing legal responsibility when the data is in the possession of third parties.[11] This is further complicated by social networking sites used to create and distribute content. It is necessary to know how the data holder exercises legal control over digital information held by the CSP, and how the legal control of business records and public documents held by CSPs can be enforced.

## Federated identity management as a solution

Identity and access management is crucial to being able to use any information technology (IT) resource. Federating the identity management function becomes essential to provide access to the unlimited IT resources of multiple providers in the open cloud network environment. The need for federated identity management (FIdM) is caused by the emergence and growth of a global digital network-based information economy. Using the term 'Open Government,' President Obama's administration has called for government to use information technology, including cloud computing[12] and web service platforms, to promote greater participation by the citizen.[13] An important component is the 'National Strategy for Trusted Identities in Cyberspace,'[14] which recognizes that it is necessary to ensure all industries and legal entities can rely on trusted identity credentials to enable them to obtain secure access and remain in control of their data.[15]

Additional problems that must be considered include issues pertaining to jurisdiction.

FIdM is understood to mean a technology framework for providing trustworthy and convenient identity credentials for Single Sign On (SSO) open network access and identity portability.[16] The purpose of FIdM is to ensure that remote access to networks, whether for viewing, sharing information, signing documents, or completing transactions, is based on one secure credential that verifies the identity of the credential holder and can be trusted by relying parties across independent security domains.[17] Without a FIdM system that is aligned to the various national signature laws and emerging industry access control and secure messaging requirements, individuals everywhere would need to be in possession of a number of different identity credentials.[18] For example, the bio-pharmaceutical industry[19] and the aerospace and defense industry[20] already require the use of different digital certificates to participate in secure network communications.

To utilize a SSO across a number of CSPs and cloud consumers, an FIdM system requires at least three entities to establish a level of trust: the credential holder, the identify provider and the service provider (i.e. the CSP), as shown in Figure 1.[21] To communicate among themselves and establish the necessary trust, these entities will require a common protocol. Leading protocols include SAML (Security Assertion Markup Language), OpenID, and WS-Federation. They also utilize the Public Key Infrastructure (PKI) that employs public and private key pairs and standards based (e.g. ITU-T X.509) digital certificates to authenticate users

9 *Rod Beckstrom and Magnus Graf Lambsdorff, The Starfish and The Spider: The Unstoppable Power of Leaderless Organizations, at 6-7 and 98.*

10 *Thomas L. Friedman, The Lexus and the Olive Tree, at 8 ('…in the globalization system we reach for the Internet, which is a symbol that we are all increasingly connected and nobody is quite in charge.').*

11 *Joseph Vining, From Newton's Sleep (Princeton University Press, 1995) at 287-290. Identity and property are closely linked in determining legal responsibility.*

12 *Wayne Jansen and Timothy Grance, NIST Draft Special Publication 800-144, Guidelines on Security and Privacy in Public Cloud Computing (January 2011) at 3 and Charles Babcock, Management Strategies for The Cloud (McGraw Hill, 2010) at 4-16 and 221-225, cloud computing is generally defined as computer services, including infrastructure, software applications, platforms, and archiving maintained by third party providers utilizing virtualization and distributed computing services offered via servers that are designed to satisfy the rise and fall in demand, not necessarily in any single or known location, and typically sold on demand or on an "as used" basis.*

13 *For example, see ' Executive Office of the President, analytical perspectives, Budget of the U.S. Government, Fiscal Year 2010' at 158 (26 February 2009) at 158, available at http://www.gpoaccess.gov/usbudget/fy10/pdf/spec.pdf (' Initial [Cloud computing] pilots conducted in collaboration with Federal agencies will serve as test beds to demonstrate capabilities, including appropriate security and privacy protection at or exceeding current best practices, developing standards, gathering data, and benchmarking costs and performance.').*

14 *National Strategy for Trusted Identities in Cyberspace (draft 2010), available at http://www.nist.gov/nstic/.*

15 *National Strategy for Trusted Identities in Cyberspace at 5-8 and 33-4. See also Directorate for Science, Technology and Industry Committee for Information, Computer and Communications Policy, ' The Role of Digital Identity Management in the Internet Economy: A Primer for Policy Makers,' Organisation for Economic Co-operation and Development (OECD) (2009) at 4.*

16 *Jeff Nigriny and Randy V. Sabett, ' The Third-Party Assurance Model: A Legal Framework for Federated Identity Management' , Jurimetrics (Summer 2010) at 511.*

17 *Jeff Nigriny and Randy V. Sabett, ' The Third-Party Assurance Model: A Legal Framework for Federated Identity Management' , at 510.*

18 *The European Union electronic signature Directive is an example of an attempt at a regional approach: Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, OJ L 13, 19.01.2000, p 12.*

19 *See the digital certificate requirements of SAFE-Biopharma Association, available at http://www.safe-biopharm.org.*

20 *See the digital certificate requirements of CertiPath, Inc., available at http://www.certipath.com and the Transglobal Secure Collaboration Program, http://www.tscp.org.*

21 *Directorate for Science, Technology and Industry Committee for Information, Computer and Communications Policy, ' The Role of Digital Identity Management in the Internet Economy: A Primer for Policy Makers,' Organisation for Economic Co-operation and Development (OECD) (2009) at 11.*

and web sites on the internet between otherwise unknown entities.

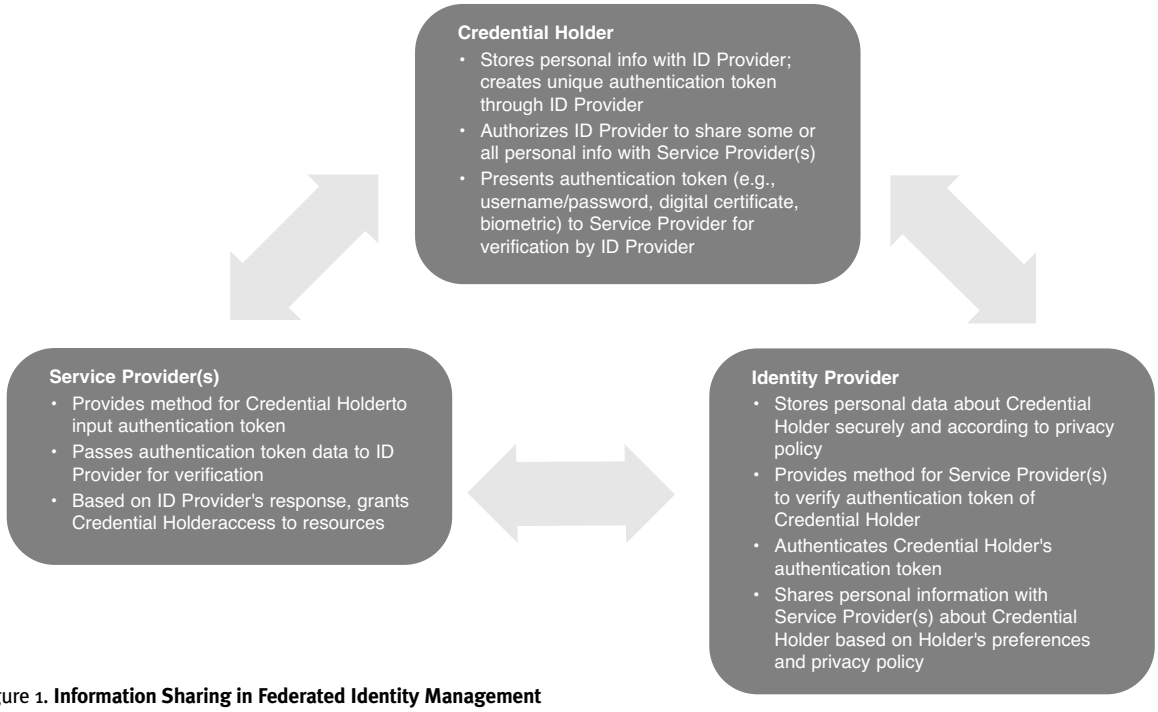



Figure 1. **Information Sharing in Federated Identity Management**

FIdM contemplates a system of decentralized decision making and control with respect to credential issuance and rights of access.[22] Therefore, determinations of legal rights and duties are necessarily *contextual* according to the relative access controls of each data holder;[23] control and reliability of the credential; and the nature and superiority of the property interests in the digital information being collected, used, or disseminated.[24] In this respect, the cloud poses three legal control challenges to FIdM, set out below.

## Legal controls

A legal problem relates to what might be termed ubiquitous access to digital information in shared computer networks – and how the data holder with superior interest asserts sufficient legal controls to manage and protect digital information assets in the cloud.[25] The term 'data holder' includes 'data owners' and 'informational rights owners,' all of whom have a relative level of legal control or dominium over the digital information. The trend for economic value to move away from goods and services to data collection and analysis reinforces the need to protect digital data assets.[26] FIdM recognizes that data level control built on strong assurance of user identity and secure authentication is necessary in the cloud.[27]

## Controlling access

Where access is based on the issuance of credentials by a third party, which in turn relies on decisions by the relying party, it is a matter of grave concern as to who

22 *Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing, V2.1 (December 2009) at 63-65; Wayne Jansen and Timothy Grance, NIST Draft Special Publication 800-144, Guidelines on Security and Privacy in Public Cloud Computing (January 2011) at 22.*

23 *See discussion in "Determining Cloud Access and Use Levels" section of this article concerning the relative rights and duties of data holders and the associated level of Dominium.*

24 *For a comparison to the contextual nature of information security duties, see the white paper by Thomas Smedinghoff, 'The State of Information Security Law: A Focus on the Key Legal Trends' (2010) at 15-17, available at http://wildman.com/.*

25 *Lucy L. Thomson, ed, Data Breach and Encryption Handbook (American Bar Association, 2010) p. 13; Internet Security Alliance and the American National Standards Institute, The Financial Management of Cyber Risk: An Implementation Framework for CFO's (2010) at 36-38.*

26 *Ludwig Siegele, 'It's a smart world: A special report on smart systems', The Economist, 6 November 2010 at 15; Anssi Hoikkanen, Margherita Bacigalupo, Ramón Compañó, Wainer Lusoli and Ioannis Maghiros, 'New Challenges and Possible Policy Options for the Regulation of Electronic Identity', Journal of International Commercial Law and Technology, Volume 5, Issue 1 (2010), at 6 (arguing that identity can also be valued as a capital asset or property); Peter F. Drucker, The Age of Discontinuity (Harper & Row, 1969) at xi, 24-28, 263-65 (Drucker described it as the emergence of the 'knowledge economy').*

27 *Jeff Nigriny and Randy V. Sabett, 'The Third-Party Assurance Model: A Legal Framework for Federated Identity Management', at 510.*

controls the credentials and sets the access rights to networks and data.[28] This involves security of identity. FIdM attempts to protect users' identity information by establishing the identity provider as a trusted third party, minimizing the amount of users' personal data when obtaining access to multiple systems, and removing the need for relying parties (or service providers) to view private data.[29] Both the private and public sectors recognize the fundamental need for *trust* by consumers in the cloud network-based global marketplace.[30]

### Access levels

It is necessary to establish the legal basis to enable a decision to be made when a person seeks to obtain access to a service, given that such relationships are based on the relativity of the data holder's rights and duties in digital property.[31] Establishing who has the duty to protect personal information is vital.[32] FIdM is intended to enable the participants in the identity system to determine the context and relevance of digital information for the purposes of access rights, usage rights, and duties of protection.[33] Identification enables third parties to recognize an individual's identity in the context of such relationships.[34] Therefore, considerations for determining liability and the allocation of risk necessarily revolve around the relationships of access control to the digital data and the required levels of protection given to the data.

## Legal controls for identity federation in the cloud

FIdM establishes minimum criteria for issuing, managing, validating, and securing electronic identity credentials.

### The identity credential

FIdM processes bind the identity of an individual to an electronic credential. This is crucially important for a service provider such as a CSP, because it must trust the origin and integrity of the sender's electronic record, including the electronic signature.[35] Accurate e-identity, in turn, rests on the quality of the mechanism used to obtain the identifying information during the credential registration and issuance process.[36]

The use of an identity credential has three purposes: access, authentication, and attribution. First, an identity credential can be used as, in effect, a key to allow authorized individuals to electronically obtain access to secure networks such as public registries. Second, an identity credential should authenticate the origin of a message so that the recipient can better trust the integrity and identity of the sender as an approved member of a network or federation. While no foolproof system exists to guarantee integrity and identity of electronic data messaging, a higher degree of trust is required and possible in FIdM than is possible in, for example, plaintext messaging protocols. Strong and generally reliable integrity and identity assurance protocols are vital to secure information exchange. Third, an identity credential provides a legal means for an electronic signature to be attributed to the individual and enables proof of intent to render a legal signature. We stress that by 'legal means' we mean only a contractually binding mechanism for signature attribution and presumptive proof of intent.

It follows that the identity credential must be issued with clear and unambiguous management policies, such as unique number identifiers, hashing capabilities, and public revocation lists, so that relying parties anywhere in the world can have a much higher degree of

28 *Jeremy Rifkin, The Age of Access (Tarcher Putnam, 2000) at 11-15 and 177-79.*

29 *' The Role of Digital Identity Management in the Internet Economy: A Primer for Policy Makers,' Organisation for Economic Co-operation and Development (OECD) at 16-17.*

30 *Stephen Covey, The Speed of Trust (Free Press, 2006) at 10-13 and 261-71; Scott Charney, ' Establishing End to End Trust,' Microsoft White Paper (2008) at 5; Rod Beckstrom and Magnus Graf Lambsdorff, The Starfish and The Spider: The Unstoppable Power of Leaderless Organizations at 126 and 163; ' The Role of Digital Identity Management in the Internet Economy: A Primer for Policy Makers,' Organisation for Economic Co-operation and Development (OECD), at 5-6; National Strategy for Trusted Identities in Cyberspace, at 5-8, 15 and 17.*

31 *Greg Lastowska, Virtual Justice: The New Laws of Online Worlds (Yale University Press, 2010) at 3-5; ' The Data Deluge' , The Economist, 27 February 2010 at 11, ' Rather than owning and controlling their own personal data, people very often find that they have lost control of it.'*

32 *Daniel J. Solove, ' "I've Got Nothing to Hide" and Other Misunderstandings of Privacy' , 44 San Diego Law Review 745 (2007); ' Data, data everywhere: A special report on managing information' , The Economist, 25 February 2010 at 16 (' Privacy laws were not designed for networks.' ).*

33 *Anssi Hoikkanen, Margherita Bacigalupo, Ramón Compañó, Wainer Lusoli and Ioannis Maghiros, ' New Challenges and Possible Policy Options for the Regulation of Electronic Identity' , Journal of International Commercial Law and Technology, Volume 5, Issue 1 (2010), at 9 (referred to the 'contextualization of information' relative to the data types and use contexts).*

34 *Anssi Hoikkanen, Margherita Bacigalupo, Ramón Compañó, Wainer Lusoli and Ioannis Maghiros, ' New Challenges and Possible Policy Options for the Regulation of Electronic Identity' , at 4; International Telecommunication Union, Recommendation ITU-T X.1252 ' Baseline identity management terms and definitions' (04/2010) at 3 (' Identification: The process for recognizing an entity by contextual characteristics.' ).*

35 *Ed Chase, ' Eunomic Solutions in a Commonly Used Application' in George Paul, Foundations Of Digital Evidence (American Bar Association, 2008), Appendix A at162.*

36 *Patrick McKenna, ' The Probative value of digital certificates: Information Assurance is critical to e-Identity Assurance' , Digital Evidence and Electronic Signature Law Review 1 (2004) at 55-60; Nicholas Bohm and Stephen Mason, ' Identity and its verification' Computer Law & Security Review, Volume 26, Number 1, January 2010, at 43-51.*

confidence that the individual's credential-based signature belongs to the credential holder and not an imposter. Ideally, the identity credential will add a layer of protection against forgery for the content of the document by means of encryption, hashing, and other content controls.

### Proof of control: Trustmarks

Both public and private sector participants in FIdM require a visible indicator of third party certification providers to trust on-line access to networks.[37] In particular, for electronic documents to be reliable over time, an enduring document-level control and protection mechanism in the form of a self-verifiable electronic seal or 'trustmark' is considered necessary.[38] To maintain its integrity, 'the trustmark itself, and the way it is presented, will be resistant to tampering and forgery; participants should be able to both visually and electronically validate its authenticity.'[39]

The identity assurance system necessarily depends on the existence of a legally trustworthy and reliable foundation of document authenticity.[40] Accordingly, the trustmark is a significant component of the identity system that provides visible evidence of protection against forgery in much the same way as an official seal. The trustmark, as an indicator of ownership, control, or origin, is also self-authenticating under Rule 902(7) of the U.S. Federal Rules of Evidence.

### Registries: verification capability

A critical prerequisite before any identity credential should be relied upon is the verification of its authenticity. This is achieved by validating the identity credential with the identity provider or an existing registry, both of which with FIdM can be accomplished on-line at the time of use.[41] Relying parties need not know anything (e.g. about PKI) or do anything, such as make configuration changes to their communications interface or make any judgments about whether to trust the digital certificate and its source. The identity credential should be self-proving, with liability flowing to the issuer of the credential as a result. The issuer of the credential, in turn, includes standard indemnification and hold harmless clauses in its contractual relationship with the holder of the identity credential to ward against fraudulent or unauthorized use. Necessarily, such clauses are subject internationally to conflicts of law analyses and sovereign claims of authority that may weaken or entirely destroy legal protections or obligations. Nonetheless, such clauses are fundamental to the issuance of identity credentials, and treaty obligations or similar international compacts may, in time, supersede such contractual limitations.

This concept has a tested foundation in the self-authenticating acts of the notary public. Third parties relying on electronic notarizations, for example, must be able to independently verify that the notary's electronic credential, in the form of a digital certificate, is actually being or has been used only by the individual to whom the notary commission was issued by the appropriate jurisdiction.[42]

For validation to be automatic, critical information relating to the trust to be given to the document must already be included in the signature itself and the application in which the document is created.[43] It is possible to achieve this by using the current improvements of the most recent versions of the relevant application (for instance, Adobe). Ideally, the signature validation process should simply involve two steps – opening the document and looking for the 'valid' indication icon that states the document is authentic (normally a green check mark). Any actions beyond this are more than the relying party should be expected or legally obligated to do. As stated above, compromises of this system of trust (by malware or other third party attacks) can be legally protected against contractually, which carries certain limitations and risks internationally. International standards of encryption

37 *National Strategy for Trusted Identities in Cyberspace, at 21-27.*

38 *National Strategy for Trusted Identities in Cyberspace, at 22 and 24-27.*

39 *National Strategy for Trusted Identities in Cyberspace, at 22.*

40 *Joseph Vining, From Newton's Sleep (Princeton University Press, 1995) at 46.*

41 *ABA Information Security Committee, Science and Technology Section: Digital Signature Guidelines (American Bar Association, 1996) at 14-15 and sections 1.8, 1.22, 1.29, 1.36, and 1.37. The certificate status information is included in the digital signature as either a time stamped Certificate Revocation List (CRL) which indicates indirectly that the certificate of the signatory was not revoked prior to the time the signature was created or an Online Certificate Status Protocol (OCSP) response which checks the actual validity status of the signatory's certificate.*

42 *National e-Notarization Standards, Standards 14 and 15 (National Association of Secretaries of State, 2006) available at http://www.nass.org/index.php?option=com_docman&task=doc_download&gid=29; First International Forum on e-Notarization and e-Apostilles, Conclusions 15 and 18 (National Notary Association, 2005) available at http://www.e-app.info. See also, e.g., Code of Virginia, §47.1-14, which imposes a "duty of care" on notaries public to keep and maintain the instruments of office under the exclusive control of the notary at all times, including any registered device or algorithm used to create an electronic notary seal or signature. Every State in the United States has a similar statutory provision.*

43 *Jacques Francoeur and Ed Chase, 'Digital Assurance and the Digital Chain of Evidence', at § 3 (SAIC and Adobe, 2008) (providing a neutral technical description of these requirements) available at http://www.saic.com/news/resources.asp#.*

and hashing algorithms and corresponding secure messaging standards help alleviate this issue technologically, but the legal problem of the recognition of secure electronic signatures internationally remains to be resolved legally and technologically.

## Controlling access to the cloud

### Legal control of the credential

The subject or credential holder has the right to use the credential, and therefore has some form of control over the credential, pursuant to a contractual agreement with the identity provider.[44] The credential provider controls the access rights, including usage restrictions and revocation. In effect, the credential provider licensees use of the credential to the credential holder, who maintains physical possession.[45] The credential holder must immediately notify the provider should the credential be lost or stolen. As with credit cards or other similar credential policies governed both by domestic statutes and contracts between the issuer and holder of the credential, a credential holder should not be held liable for the unauthorized and unknown use of an identity credential, providing the credential holder exercises reasonable care in safeguarding access to the credential. Further, technological policies and procedures must be in place and testable by reliable audit procedures to protect the continued use of a reported lost or stolen credential.

Credential legal control requirements also may be met by the use of trusted third party registries approved and audited by federation operators such as CertiPath, SAFE, Kantara, and FiXs.[46]

### Credential governance in existing identity federations

#### U.S. Government: PIV-I

The Personal Identity Verification – Interoperable ('PIV-I') smartcard can be issued by non-federal identity providers while taking advantage of the federal high identity assurance standards.[47] Widespread adoption is expected because of federal government requirements for federal employees and contractors;[48] federal requirements for the full implementation of electronic medical records in the healthcare system,[49] and commercial availability of smart telephones with PIV-I authentication and signing capabilities.

The PIV-I credential is issued and secured in accordance with an assurance level equivalent or greater to what the U.S. federal authorities refer to as Medium Assurance Hardware -- Federal Bridge Cross Certified.[50] An understanding of the reliance on the certificate for this assurance level includes the following:

1. 'This level is relevant to environments where threats to data are high or the consequences of the failure of security services are high. This may include very high value transactions or high levels of fraud risk.'[51]

2. 'Relying Parties must evaluate the environment and the associated threats and vulnerabilities and determine the level of risk they are willing to accept based on the sensitivity or significance of the information. This evaluation is done by each Relying Party for its application and is not controlled by this CP.'[52]

3. 'A Relying Party uses a Subscriber's certificate to verify the integrity of a digitally signed message, to identify the creator of a message, or to establish confidential communications with the Subscriber. The Relying Party is responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information. A Relying Party may use information in the certificate (such as certificate policy identifiers) to determine the suitability of the certificate for a particular use.'[53]

That certification level is based on a high standard of reliability defined by the Federal PKI Management Authority.[54] PIV-I assumes that the operational reliability

44 *For examples of this arrangement, see the certificate policies of CertiPath, Inc. and SAFE-Biopharma Association.*
45 *For examples of this arrangement, see the certificate policies of CertiPath, Inc. and SAFE-Biopharma Association.*
46 *Possible future work on electronic commerce – Proposal of the United States of America on electronic transferable records, United Nations Commission on International Trade Law (June 18, 2009) at 5 (pertaining to electronic transferable records). See also, UNIF. ELEC. TRANSACTIONS ACT (' UETA' ) § 16 Comment 3 (National Conference of Commissioners on Uniform State Laws 1999). The UETA has been adopted in every state and the District of Columbia except Illinois, New York, and Washington.*
47 *Smart Card Alliance, ' Personal Identity Verification Interoperability (PIV-I) for Non-Federal Issuers: Trusted Identities for Citizens across States, Counties, Cities, and Businesses,' (January 2011) at 4, available at http://www.securitysales.com/files/PIV-I-White-Paper-012811.pdf.*
48 *For which, see OMB 11-11 and HSPD 12.*
49 *Health Information Technology for Economic and Clinical Health Act, (HITECH ACT) of the American Recovery and Reinvestment Act (ARRA).*
50 *Appropriate uses for relying parties are described in the X.509 Certificate Policy for the Federal Bridge Certification Authority (Version 2.17 June 10, 2010) Section 1.4.1, available at http://www.idmanagement.gov/fpkipa/documents/FBCA_CP_RFC3647.pdf.*
51 *1.4.1, p 10.*
52 *1.4.1, p 8.*
53 *1.3.6, p 8.*
54 *http://www.idmanagement.gov/fpkia/.*

of the issuing Certificate Authority can be determined and meets a specific assurance level. The reliability of the Certificate Authority is in part defined by its governing Certificate Policy or Certificate Practice Statement and independent third party audit assessments, which states that 'when a PKI cross-certifies with the Federal PKI Architecture, and is an affiliate in good standing, a Relying Party operating an on-line application that utilizes digital certificates for electronic identity authentication may choose to trust that PKI's digital certificates at the Level(s) of Assurance asserted by those certificates. No other trust requirements are needed for the Relying Party to make that determination.'[55] PIV-I is intended to enhance the privacy of the citizen in the process of establishing a credential by protecting against loss, alteration, or destruction of personal information.[56]

#### Private sector identity federation implementations

Control requirements for credentials are being met in some industries with the use of trusted third parties in the form of federation operators such as CertiPath, SAFE, FiXs, and Kantara.[57] All of these entities set rules and commercial terms that enable participants to evaluate trusted identity.

Certipath and SAFE are examples of open FIdM business system models in which participants must contractually agree to comply with all the rules governing the issuance of use of the identity credentials.[58] In the open system, the rules are not publicly available to nonmembers, and the parties have flexibility to use the credentials in ways that are not envisaged by the federation operator. Certipath develops and oversees digital certificate policies for the aerospace and defense industry largely for purpose of secure information sharing. SAFE performs this role for pharmaceutical and healthcare industries and approves member use of digital certificates that will meet global regulatory compliance requirements.

FiXs and Kantara are examples of closed FIdM business system models in which the federation operators have greater ability to limit both participation and credential usage. FiXs performs this role for government contractors and denies benefits to any third party that is not contractually bound with the federation operator. The Kantara Initiative federation model does not use a registry or third party audit or enforcement procedures.[59] Nor does it actually operate as a federation. Rather it recommends a policy framework for 'circles of trust' that participants must agree to in some unspecified contractual form.[60]

ACES (Access Certificates for Electronic Services) was created and sponsored by the federal Government Services Administration to enable secure on-line access to GSA services and other government entity services. ACES relies on the use of digital certificates and a public key infrastructure to identify participants and digitally sign data in an attempt to make transactions non-repudiable. ACES transactions can occur between business and government and consumer and government, and government agency participation is voluntary.

### International – Notaries

Civil law notaries generate large amounts of data that is entered and stored in a variety of public and private registers.[61] Moreover, cross border circulation and recognition of notarized non-public documents, especially powers of attorney, is a regular notarial practice greatly facilitated by the use of electronic registers.[62] Parties in other jurisdictions can rely on the notarized document and may verify the notary's identity and office holder status through the use of an FIdM system of smartcards issued by certificate authorities owned by a notary society, and cloud-based centralized data management services.[63] Estonia, Italy, and British Columbia currently use cloud-based notarial services that undertake the execution and filing of electronic land records.

The notary society or organization in each country

55 *Note the explanation provided by the Federal Bridge Certification Authority, available at http://www.idmanagement.gov/fpkia/crosscert.cfm.*

56 *Smart Card Alliance, 'Personal Identity Verification Interoperability (PIV-I) for Non-Federal Issuers: Trusted Identities for Citizens across States, Counties, Cities, and Businesses,' at 5.*

57 *See the digital certificate requirements of SAFE-Biopharma Association, available at http://www.safe-biopharma.org/ and the digital certificate requirements of CertiPath, Inc., available at http://www.certipath.com and the Transglobal Secure Collaboration Program, http://www.tscp.org. See also FiXs Trust Model Version 3.0, September 1, 2010.*

58 *For further information about existing open systems, see The Four Bridges Forum available at http://www.the4bf.com/ (FIdM examples in aerospace, defense, biopharmaceutical, healthcare, and higher education).*

59 *Jeff Nigriny and Randy V. Sabett, 'The Third-Party Assurance Model: A Legal Framework for Federated Identity Management', at 519.*

60 *Jeff Nigriny and Randy V. Sabett, 'The Third-Party Assurance Model: A Legal Framework for Federated Identity Management, at 519-520'.*

61 *Ugo Bechini and Dominik Gassen, 'A New Approach to Improving the Interoperability of Electronic Signatures in Cross-Border Legal Transactions', 17 Michigan State Journal of International Law, Issue 3 (2009) at 4.*

62 *Ugo Bechini and Dominik Gassen, 'A New Approach to Improving the Interoperability of Electronic Signatures in Cross-Border Legal Transactions', at 14-15.*

63 *Ugo Bechini and Dominik Gassen, 'A New Approach to Improving the Interoperability of Electronic Signatures in Cross-Border Legal Transactions', at 5. Leading examples have been are the Notaries of Italy, France, and Estonia.*

must issue the digital certificates to the member notaries.[64] The notary societies also are responsible for creating procedures to determine how those credentials will be managed, renewed, and revoked. The International Union of Latin Notaries (UINL) has specified that 'Notaries should obtain an electronic signature with a high level of security, accredited by a recognized certificate, using a safe signature creation device. To do so, it will be advisable to proceed to generate the signature verification and creation data, by the certification authority, and its delivery to the notary under the control of the competent notarial authority.'[65] This mirrors the practices currently used by Notary Societies in many nations, including Italy, Germany, Argentina, Spain, Estonia, Brazil, Mexico, and Austria. Notaries Societies in the United Kingdom, Australia, and Turkey plan to implement similar electronic notarial practices.

To preserve a trustworthy authentication function for the digital certificate, UINL policies make the notary responsible for the use, protection, and control of the digital signature.[66] Specifically, notaries must use a secure electronic signature creation device.[67] Notaries risk recall or suspension of their certificates upon disclosure of the confidential password that controls use of the digital signature.[68] No one other than the named notary may use the digital signature.[69]

The UINL has also taken the position that the notary societies of each country must give relying parties the ability to verify the notary's digital signature: ' Whereas for the free international circulation of electronic notarial deeds there must be a general method for verifying the signature and the capacity of the presiding notary, we request that the certification of the notary's digital signature remain under the control of the member notariats, whilst observing the principals and methods which are developed for such verification on a global level.'[70] This verification capability should also be quick and simple and permit real-time authentication of the notary's digital signature.[71] The Council of the Notaries of the European Union (CNUE) has already developed and piloted an internet platform that will allow relying parties to verify the digital signatures of European notaries.[72]

## Limitation of liability for credential governance

The National Strategy for Trusted Identities in Cyberspace has identified liability limitation for identity credential providers as an important issue for FIdM. Specifically, the National Strategy posed the question whether there should be limits on liability or monetary damage caps on identity providers in the event of fraudulent use of the tokens.[73] Currently, risk allocation and any attempted limitation of liability amongst the participants in FIdM is achieved through contract.[74] No state level statutes in the United States currently address risk allocation other than in the context of the electronic signatures.[75] A model for federal statutory limitation of liability exists in maritime law with respect to ship owner and charter liability for loss and damages involving cargo and passengers.[76] On the basis of this provision, loss claims with respect to the sinking of the Titanic were limited to the value of the remaining lifeboats.[77]

Virginia has become the first U.S. state to introduce legislation to clarify and limit the liability of private federation operators, identity credential providers, and credential holders.[78] The legislation[79] would give federation operators and identity providers immunity from legal action for identity credentials issued 'in accordance with the specifications of the U.S. Federal Bridge Certification Authority' unless they were grossly negligent or engaged in willful misconduct. However,

64 *See the ' Certification Policy for the Notarial Electronic Signature of Member States of the International Union of Latin Notaries (U.I.N.L)' from the 2004 Congress held in Mexico City. The notarial electronic signature 'should be protected by a certificate issued under the control and responsibility of the notarial authority in each member state of the U.I.N.L.'*

65 *XXIV International Congress of Latin Notaries, Conclusions of the Working Group for Theme II ' The Notary and electronic contracts' (2004), available at http://www.uinl.org.*

66 *See the Code of Virginia, §47.1-14, for a corollary US statutory provision.*

67 *' Certification Policy for the Notarial Electronic Signature of Member States of the International Union of Latin Notaries (U.I.N.L),' policy number 2, from the 2004 Congress held in Mexico City and available at http://www.uinl.org.*

68 *' Certification Policy for the Notarial Electronic Signature of Member States of the International Union of Latin Notaries (U.I.N.L),' policy number 7.*

69 *' Certification Policy for the Notarial Electronic Signature of Member States of the International Union of Latin Notaries (U.I.N.L),' policy number 7.*

70 *XXIV International Congress of Latin Notaries, ' Conclusions of the Working Group for Theme II' (2004), available at http://www.uinl.org.*

71 *Bernard Reynis and Ugo Bechini, ' European Civil Law Notaries Ready to Launch International Digital Deeds' , Digital Evidence and Electronic Signature Law Review 4 (2007) at 14-18.*

72 *Ugo Bechini and Dominik Gassen, 'A New Approach to Improving the Interoperability of Electronic Signatures in Cross-Border Legal Transactions' , 17 Michigan State Journal of International Law, Issue 3 (2009) at 14-18.*

73 *National Strategy for Trusted Identities in Cyberspace, at 31.*

74 *Jeff Nigriny and Randy V. Sabett, ' The Third-Party Assurance Model: A Legal Framework for Federated Identity Management' , at 512, 521-22 and 534.*

75 *5 ILL. COMP. STAT. ANN. § 175/5-110 and WASH. REV. CODE ANN. § 19.34.320 and 321 (digital signatures only). Note the comparative international discussion of electronic signature risk allocation in Stephen Mason, Electronic Signatures in Law (Tottel, 2nd edn, 2007) Chapter 9.*

76 *46 U.S.C.A § 183. Note Paul M. Barrett, ' Success is never having to say you're sorry' , Bloomberg Businessweek, 4 July 2011 at 56 and 59, Transocean, the company that owned and ran the Deepwater Horizon oil drilling vessel that exploded and sank on April 20, 2010, has invoked this statute in an attempt to cap the company's liability for resulting deaths and personal injuries.*

77 *Oceanic Steam Navigation Co. v. Mellor (The Titanic), 233 U.S. 718 (1914).*

78 *HB 2259, available at http://leg1.state.va.us/cgi-bin/legp504.exe?111+ful+HB2259.*

79 *Incorporated in the form of amendments to the Uniform Computer Information Transactions Act.*

identity credential providers would be liable for damages for failure to revoke after notice or for failure to terminate after expiration. The legislation would also make the credential holders liable for failing to notify the identity credential provider of loss of control or unauthorized access. The identity credential provider would bear the risk of loss in the event that the credential holder is not aware that the credential has been compromised.

### Maritime law as model for determining legal control

Maritime law provides a useful example of an existing global commercial network that has allocated liability based on legal control factors.[80] Overseas shipping, including the transport of cargo and passengers as well as fisheries and offshore resources, is the oldest commercial network and one with an extensively developed body of law and practices.

The maritime model has implications for determining the allocation of risk in the context of CSPs and third party outsourcing.[81] For example, the federation operator functions, in effect, like a ship registry in setting standards for and certifying participants. The federation operator also signals to relying parties the assurance levels and associated Certificate Policies to which the token is bound, analogous to the manner in which a vessel's flag indicates the set of national laws under which it is operating. Similar to the requirement of seaworthiness, for parties relying on credential tokens, determination of the applicable assurance level is highly contextual.

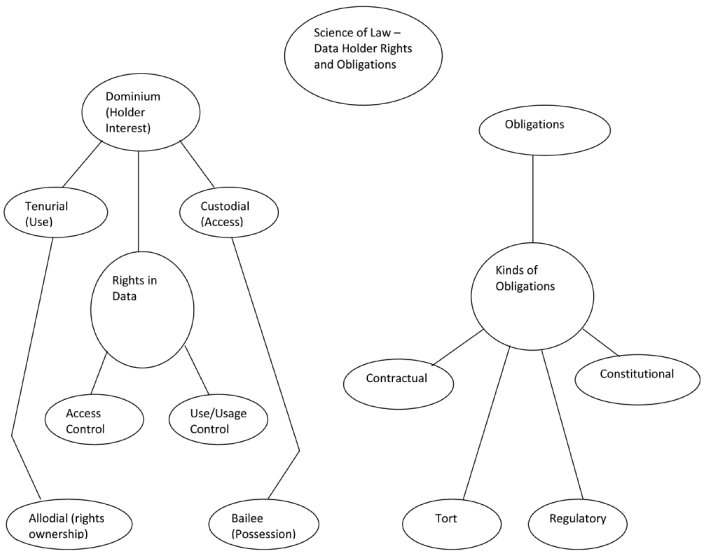
Adapting the maritime model to FIdM has interesting law and policy implications. First, the maritime model suggests that control rights over digital data in a commercial network are determined by the relative ownership interests and access control relations of persons and entities (e.g. the various data holders). Second, by analogizing ownership and control of a vessel to that of an identity credential, the maritime model provides a framework that separates out the risk allocation involving the credentials themselves, the relative data holder access control status, and any required protection duties for the particular data being accessed, used, or transmitted. Finally, the maritime model provides examples of regulatory liability limitation approaches that could be used in the FIdM scheme.

## Determining cloud access and use levels

### Dominium: data holder control rights

Digital data is property.[82] Dominium over property has the following aspects: possession or hold, use, and disposal.[83] Data holder rights are contextual according

**Figure 2. Digital Data as Property**




80 *For instance, see United Nations Commission on International Trade Law, United Nations Convention on Contracts for the International Carriage of Goods Wholly or Partly by Sea (United Nations, Vienna 2009); United Nations Convention on the Carriage of Goods by Sea (Hamburg Rules) (1978).*

81 *John R. Pagan, 'English Carriers' Common-Law Right to Reject Undeclared Cargo: The Myth of the Closed-Container Conundrum', 23 William and Mary Law Review, Issue 4, (1982) at791 (' The shipper-carrier relationship is a species of bailment for hire.').*

82 *See, e.g. VA CODE ANN § 18.2-152.2; Thyroff v. Nationwide Mut. Ins., 8 N.Y.3d 283, 292-293 (2007); Clark Street Wine & Spirits v. Emporos Systems Corp. (E.D.N.Y. 11-29-2010); Anssi Hoikkanen, Margherita Bacigalupo, Ramón Compañó, Wainer Lusoli and Ioannis Maghiros, 'New Challenges and Possible Policy Options for the Regulation of Electronic Identity', at 6; domain names are intangible property under California law. Kremen v. Cohen, 337 F.3d 1024, 1030 (9th Cir. 2003) (as with the majority of states to have addressed the issue, California law recognizes a property interest in domain names making them subject to conversion claims), to this end, 'courts generally hold that domain names are subject to the same laws as other types of intangible property.' Jonathan D. Hart, Internet Law: A Field Guide (Bna Books, 2008) at 120. See, also, Office Depot Inc. v. Zuccarini, 596 F.3d 696, 701-02 (9th Cir. 2010) (domain name is subject to receivership in the district of domain name registrar) and Greg Lastowska, Virtual Justice: The New Laws of Online Worlds, at 5 (discussion of evolving application of property law to virtual world and on-line gaming context).*

83 *E.g. Smith v. Furbish, 68 N.H. 123 (1894) at 144; Harold J. Berman, Law and Revolution II: the impact of the Protestant Reformations on the western legal tradition, (Belknap Press of Harvard University Press, 2003) at 167-170. In the development of the common law, dominium had formally meant not only rights in land or chattels but also lordship over persons. Property was not 'owned' in the modern sense but rather 'held' in a form of tenure with the rights of possession, use, and disposal depending on the relationship between the landholder and duties owed to superiors or privileges owed by subordinates in the hierarchy. In the fifteenth and sixteenth centuries, the concept of ownership was separated from lordship. A similar system of multiple property interest holders in the same property has existed in Japan, for which see Peter Duus, Feudalism in Japan, (Knopf, NY, 1976) at 34-35. The hierarchy of Shiki rights enabled a large number of people to share in the agricultural surpluses in the land, which was the chief economic value. See also, J. H. Baker, An Introduction to English Legal History (London Butterworths, 1979) at 194-97.*

to the relativity and overriding nature of property interests and the nature of the data itself.[84] There are four categories (See Figure 2 on previous page.)

1. Allodial (information rights ownership and title ownership not subject to intellectual property, licensing, privacy, confidentiality, constitutional, regulatory, or other restrictions)[85]

2. Tenurial (copyhold ownership, possession and control, subject to intellectual property, licensing, privacy, confidentiality, constitutional, regulatory, or other restrictions)[86]

3. Custodial (care or charge of another's property)[87]

4. Bailment (lawful possession for hire and protection of another's property)[88]

The rights of the data holders to exercise persistent control over the data (legal ability to set authorization and access rights to digital data) have been grouped into two categories:

*Access* (encryption and preventive viewing/disclosure controls; authorization controls; strong authentication; audit capability; and, binding of access rights policy to data), and

*Usage* (rights management, copying, print screen, expiration, editing, saving, sending, and retention).[89]

## Obligations to control: the holder of the data

Obligations to protect data that can be viewed in use, at rest, or transit over open networks arise from four main sources:

1. Contract (bailment, license use, and Service Level Agreements).

2. Tort (conversion[90] and confidentiality laws).

3. Regulatory (privacy and data protection laws governing authorized access and usage).

4. Constitutional (right to informational privacy).[91]

These protection duties function as limitations on the data holder's status and property interests. Accordingly, all data holders are subject to these contextual obligations.[92]

Similarly, identity information and privacy challenges

84 *Greg Lastowska, Virtual Justice: The New Laws of Online Worlds, at 127 ('A web of overlapping and complex legal interests in things is preferable to an atomized regime of single owners with absolute private rights.'). Harold J. Berman, Law and Revolution II: the impact of the Protestant Reformations on the western legal tradition, at 170. In the modern common law, these are characterized as dominium or a right in a thing and the law of obligations. This could also be described as a relativity of ownership similar to the holder status found in the feudal system: Sir Frederick Pollock and Frederic William Maitland, The History of English Law Before the Time of Edward I, Volume 2 (2nd edn, 1899) at 80-81.*

85 *Black's Law Dictionary (9th edn, 2009), 88. Allodial is defined as 'held in absolute ownership.' See also, UNIF. COMPUTER INFORMATION TRANSACTIONS ACT ('UCITA') § 102 Comment 34 (National Conference of Commissioners on Uniform State Laws 2002) (Informational rights 'includes 'intellectual property' rights. It also includes rights created under any law that gives a person a right to control use of information independent of contract, such as may be developing in privacy law.'). The UCITA has been adopted in Maryland and Virginia.*

86 *J. H. Baker, An Introduction to English Legal History, at 194: 'The notion of tenure, though it no longer affects the ownership of land, has been the foundation of the law of real property for nine centuries' See, e.g., UCITA § 501 Comment 2 ('Ownership (title) to a copy is distinguished from ownership of intellectual property rights…While obtaining ownership of a copy may give the copy owner some rights with respect to that copy, it does not convey ownership of the underlying intellectual property rights in a work of authorship, a patented invention or other intellectual property. The copy is merely a conduit for use, but not ownership, of rights.').*

87 *Black's Law Dictionary, at 441. Custody is defined as 'the care and control of a thing or person for inspection, preservation, or security.' A record custodian has been given charge of a document.*

88 *Black's Law Dictionary, at 161. A bailee is defined as 'a person who receives personal property from another, and has possession of but not title to the property. A bailee is responsible for keeping the property safe until it is returned to the owner.'*

89 *Cloud Security Alliance Security Guidance for Critical Areas of Focus in Cloud Computing V2.1 (December 2009). See also, VA CODE ANN 59.1-501.2 (38).*

90 *The CSP that loses data or has processes that alter data without authorization may be liable for conversion: for instance, see Thyroff v. Nationwide Mut. Ins. Co., 460 F.3d 400, 403-04 (2d Cir. 2006) (a digital data owner is unable to retrieve customer and other personal information in the possession of a third party storage provider). Conversion is the 'unauthorized assumption and exercise of the right of ownership over goods belonging to another to the exclusion of the owner's rights' (quoting Vigilant Ins. Co of Am. v. Housing Auth., 87 N.Y.2d 36, 44 (1995). This includes an unauthorized exercise of dominion over the property or interference with it, in derogation of the data owner's rights.*

91 *Harold J. Berman, Law and Revolution II: the impact of the Protestant Reformations on the western legal tradition, at 169-70 and 216-17. In the modern common law, these are classified as contractual, quasi-contractual, tort, and regulatory obligations.*

92 *For an example of Levels of Protection geared specifically to the protective needs of identity information, see the white paper entitled Levels of Protection (LOP) by Mary Rundle and Susan Glueck (2010), available at http://www.microsoft.com/mscorp/twc/endtoendtrust/vision/lop.aspx. See also, OIX Advisory Board and the OIX Legal Policy Group, 'Fair Information Practice Principles (FIPP) Comparison Tool.' Draft 0.5 October 7, 2010, at 7-25 (using the terms 'data handler' to denote a party that 'performs an action with respect to data, for which a duty is imposed' under a privacy provision'). Another example is the lawyer's ethical duty to preserve the confidentiality of client information from inadvertent or unauthorized disclosure, discussed in James McCauley, Cloud Computing – A Silver Lining or Ethical Thunderstorm for Lawyers? VIRGINIA LAWYER, Vol. 59 (February 2011) at 49-52.*

are best approached in a contextual manner.[93] For example, in the credential issuance process, an information privacy interest is not violated when a government credential provider requires the disclosure of personal information concerning criminal and medical history and professional references.[94] It is important to note that violation of privacy protections does not implicate rights and duties of property ownership. 'A claim of privacy is not the same as a claim of ownership.'[95] However, a privacy interest in the control of personal information is recognized as giving a data holder the duty to protect from unauthorized use and dissemination.[96]

## Practical guidance

The challenge facing the global move toward the cloud is establishing a uniform and trustworthy approach for issuing and managing individuals' electronic identity credentials and usage rights. The benefit to an end user is simple: access to numerous applications and services provided across domains and organizations using the same authentication credential. With FIdM, the users and service providers can rely upon a single identity provider to manage the credential and on-line identity securely.

For the economic and secure functioning of the cloud network-based global economy, it will be useful to develop standardized e-identity credentials. Without this, it is likely that individuals will be faced with having to purchase a number of different credentials to perform a variety of tasks. Private credential issuers, governmental users, and existing federation operators are in the best position to create such a uniform, global standard that will give the cloud the necessary degree of security, trust, and reliability.

The identity credential can also provide for the encryption of data with a key that only the user is in possession of before uploading it to on-line storage or other applications. This should be done in a manner such that the CSP does not possess the private key to obtain access to the encrypted data.[97] A CSP should 'claim no ownership rights in customer data and should use customer data only as its customers instruct or to fulfill contractual or legal obligations,' and so in effect, function as a bailee with responsibility to protect the digital information owned by another.[98]



**Timothy Reiniger** is an attorney specializing in information security and digital evidence, licensed to practice in California and the District of Columbia. A director of the Digital Services Consulting Group at FutureLaw, LLC, in Richmond, Virginia, he contributed a chapter on electronic notarization in George L. Paul, *Foundations of Digital Evidence* (ABA, 2008).

**Richard Hansberger** is an internationally recognized leader in electronic signatures and records, especially electronic notarization and apostilles under The Hague Conference Apostille Convention. He has drafted numerous laws, regulations and industry technical guidelines on the topic of secure electronic signatures and records. Richard is a licensed attorney in California.

**http://www.futurelaw.net/digital-services-group.htm**

**http://www.nist.gov/nstic/**

93 *For a discussion of the contextual nature of identity, see the comments of Nicholas Bohm, 'Watch what you sign!', Digital Evidence and Electronic Signature Law Review, 3 (2006) at 45-49. For an analysis of the contextual nature of privacy disruptions as broken down into the categories of information collection, information processing, information dissemination, and invasion of privacy, see Daniel J. Solove, Understanding Privacy (Harvard University Press, 2008) at 9-10, 103-5.*

94 *National Aeronautics v. Nelson, 131 S.Ct.746 (2011) (United States government employee background check does not violate any constitutional right to information privacy or privacy interest in avoiding disclosure because it was reasonable in light of internal security interests and the substantial statutory protections against public dissemination).*

95 *Daniel J. Solove, Understanding Privacy, at 28.*

96 *Ostergren v. Cuccinelli, 09-1723 (4th Cir. 7-26-2010) at 32-34 (recognizing a protected informational privacy interest in the use and dissemination of personal information).*

97 *Peter Ferenczi, The Cloud Has Eyes, LAPTOP, April 2008 at 20.*

98 *James McCauley, Cloud Computing – A Silver Lining or Ethical Thunderstorm for Lawyers?, at 51-52.*