Ontology Of Trusted Identity In Cyberspace

Harry Katzan, Jr., Savannah State University, Savannah, USA

ABSTRACT

The nation's digital infrastructure is in jeopardy because of inadequate provisions for privacy, identity, and security. Recent Internet activity has resulted in an onslaught of identity theft, fraud, digital crime, and an increasing burden to responsible citizens. The computer security and Internet communities have been generally responsive but apparently ineffective, so it is time for a third party to step in, take charge, and provide an infrastructure to assist in protecting individuals and non-person entities. This paper is a contribution to the domain of ontological commitment as it applies to a description of subjects, objects, actions, and relationships as they pertain to the National Strategy of Trusted Identity in Cyberspace initiative.

Keywords: Identity, trusted identity, identity management, cyberspace, Internet, ontology

INTRODUCTION

The nation's digital infrastructure is in jeopardy because of inadequate provisions for privacy, identity, and security. The "everyone is free to do anything" mentally that would appear to be prevalent in America and worldwide has resulted in an onslaught of identity theft, fraud, digital crime, and an unnecessary concern over cyber security by many individuals. It is patently necessary for careful participants to operate defensively in cyberspace in order to protect themselves from the evils just mentioned. Those that do not use the Internet responsibly do so at their own peril. In fact, digital crime has served as a precursor to and is associated with physical crime. (OECD 2008)

An essential component of secure transactions in cyberspace is effective identity management, to which the computer security and Internet communities have been generally responsive but essentially ineffective. It is time for a third party to step in, take charge, and provide an infrastructure to assist in protecting the citizens of the world. (White House 2010) Similar concerns prevail in other developed countries. Many cyber crimes are perpetrated from lesser-developed countries that do not possess cyber awareness from legal, political, economic, and technical perspectives, but nevertheless provide a basis for illegal activity. There is no good reason why developed countries should have to resort to extreme measures to protect their domain, lending credence to the idea that a globally accepted form of identity determination could be appropriate. The framework for a cyber ecosystem, presented here, is purported to be a lynchpin in the development of identity management systems designed to facilitate a secure Internet.

This paper is a contribution to the domain of ontological commitment as it applies to a description of subjects, objects, actions, and relationships as they pertain to the National Strategy of Trusted Identity in Cyberspace initiative. The initial section, entitled "Major Issues," supplies a context for the ontology of trusted identity.

MAJOR ISSUES

Most of the activities present in modern society are orchestrated by two fundamental concepts: rules and roles. There are rules for just about everything we do. There are rules of the road, rules of engagement, rules of law, rules of social behavior, rules of dress, and so forth. A subject applies certain rules in accordance with the roles adopted for a specific formal or informal interaction.

The adoption of particular roles is governed by authorization. A subject is authorized to address a task or perform a requisite function through informal social structures, a formal delegation, credentials, or certified identity. We are going to apply the rule/role paradigm to the development of an identity ecosystem for transactions in cyberspace.

IDENTITY

Identity is a means of denoting an entity in a particular namespace and is the basis of security and privacy – regardless if the context is digital identification or non-digital identification. We are going to refer to an identity object as a *subject*. A subject may have several identities and belong to more than one namespace. A pure identity denotation is independent of a specific context, and a federated identity reflects a process that is shared between identity management systems. When one identity management system accepts the certification of another, a phenomenon known as "trust" is established. The execution of trust is often facilitated by a third party that is acknowledged by both parties and serves as the basis of digital identity in Internet processing and other computer services. Access to computing facilities is achieved through a process known as authentication, whereby an entity makes a claim to its identity by presenting an identity symbol for verification and control. Authentication is usually paired with a related specification known as authorization to obtain the right to address a given service.

AUTHENTICATION

Authentication is a complex issue that affects the following classes of user accessibility in an Internet environment:

- A user that logs on to a single computer application.
- A user that logs on to a computer application that links to another computer application that requires authentication.
- A user that logs on to a computer application hosted by a service provider that deploys the application using a multi-tenant service model.

In the first instance, the end user would then have to log on to the local computer and then log on to the application at the service platform running in cyberspace. This is typically the case with consumer-oriented cloud-computing services and customer-developed application software. When the application requires an additional sign-on, it must maintain its own user accounts – a process known as *delegated administration*. This instance is depicted in Figure 1. When authentication requires a sign-on to an enterprise system running on the cloud and then on to a specific application, a multiple sign-on would ordinarily be required. With a trusted authentication system, as suggested by Figure 2, the user would sign-on to an authentication server that would issue a token accepted by a federated server as proof of identity, required by specific applications. A service provider with thousands of customers would prefer a trusted solution in lieu of establishing a trust relationship with each of its customers. Common authenticators are something you know, something you have, something you are, and where you are, or in many cases, a combination of the authenticators.

One of the major problems in cyberspace, how do you know with whom you are interacting? With trusted authentication, a trusted authority validates the physical identity of subjects and objects, and binds physical entities with digital identities. Trusted authentication is designed to minimize the risk of identity spoofing and masquerading.

AUTHORIZATION

Typically, *authorization* refers to permission to perform certain actions. In cyberspace, users are assigned roles that must match corresponding roles associated with a requisite computer application. Each application contains a set of roles pertinent to the corresponding business function. Access is further controlled by business rules that specify conditions that must be met before access is granted. The role/business-rule modality also applies to storage in the cloud, and this is where the practice of privacy kicks in.

In general, the combination of identification and authentication determine who can sign-on to a system – that is, who is authorized to use that system? Authorization, often established with access control lists, determines what functions a user can perform. A related measure, known as accountability, records a user's actions. Authorization cannot occur without authentication.

In general, there are two basic forms of access control: discretionary access control, and mandatory access control. With discretionary access control (DAC), the security policy is determined by the owner of the security object. With mandatory access control (MAC), the security policy is governed by the system that contains the security object. Privacy policy should, in general, be governed by both forms of access control. DAC reflects owner considerations, and MAC governs inter-system controls.

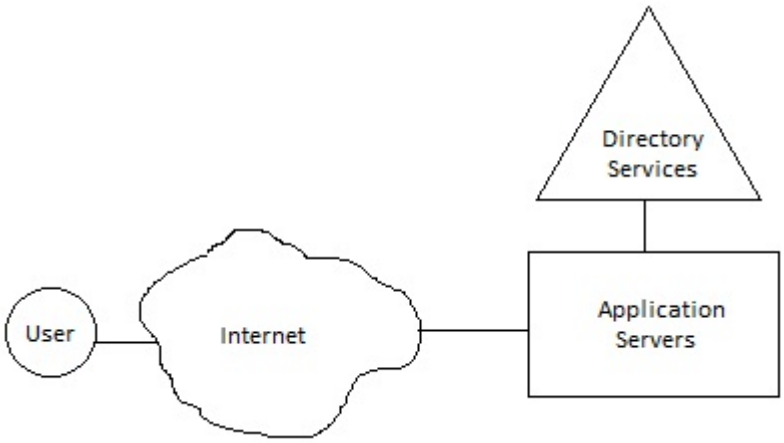

Figure 1. Delegated Administration

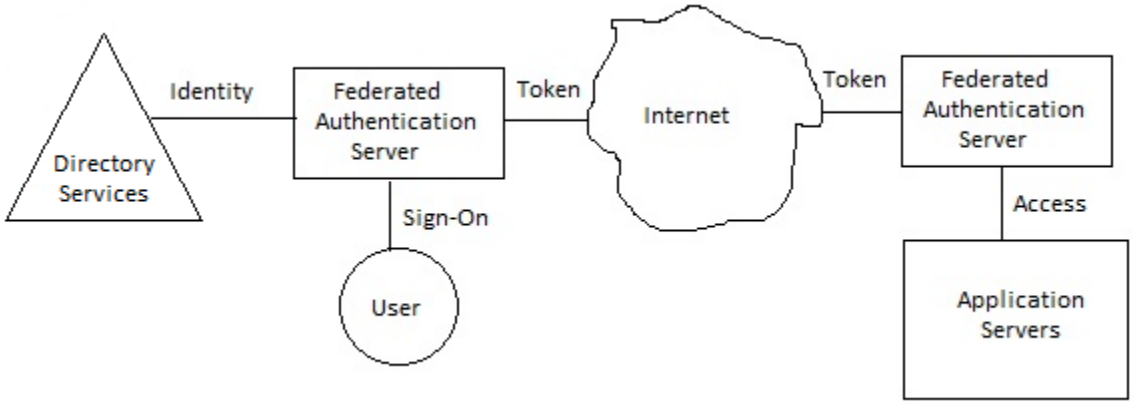

Figure 2. Trusted Authentication System

ACCOUNTABILITY

Accountability is determined by audit trails and user logs that are prototypically used to uncover security violations and analyze security incidents. In the modern world of computer and information privacy, accountability would additionally incorporate the recording of privacy touch points to assist in managing privacy concerns. Although the Internet is a fruitful technology, it garners very little trust. Why? It is very cumbersome to assign responsibility for shortcomings and failure in an Internet operational environment. Failure now takes on an

additional meaning. In addition to operational failure, it is important to also include "failure to perform as expected," as a new dimension.

TRUSTWORTHY COMPUTING

Trustworthy computing refers to the notion that people in particular and society as a whole can trust computers to safeguard things that are important to them. Medical and financial information are cases in point. Computing devices, software services, and reliable networks are becoming pervasive in everyday life, but the lingering doubt remains over whether or not we can trust them. Expectations have risen with regard to technology such that those expectations now encompass safety, reliability, and the integrity of organization that supply the technology. Society will only accept a technological advance when an efficient and effective set of policies, engineering processes, business practices, and enforceable regulation are in place. We are searching for a framework to guide the way to efficacy in computing.

As with many utilities, trustworthy computing should be intuitive, controllable, reliable, and predictable. In order to achieve these lofty goals, we are going to look to the framework developed at Microsoft (Mundie 2002) consisting of goals, means, and execution. The set of *goals* reflects a subject's perspective and is comprised of security, privacy, reliability, and business integrity considerations. The set of *means* refers to the computer industry's viewpoint and includes secure-by-design, secure-by-default, secure-in-deployment, fair-information principles, availability, manageability, accuracy, usability, responsiveness, and transparency. *Execution* concerns the manner in which an organization does business and includes intent, implementation, evidence, and integrity. One approach to using the framework is through the concept of a *trusted stack* constructed from five important elements: secure hardware, a trusted operating system, trusted applications, trusted people, and trusted data. (Charney 2008)

ONTOLOGY

Ontology is a specification of "what is." In philosophy, use of the term reflects the study of being (or existence) and describes and delineates a collection of basic categories, and defines the entities and classes of elements within a category. In service science, ontology is a specification of a conceptualization used to enable knowledge sharing. Since ontology concerns existence, an ontological definition of a subject – perhaps a service category – reflects a materialization of a concept obtained through a shared reality, and not what it is called or how it is made or used. In this paper, the definition of ontology, as "a set of representational primitives with which to model a domain of knowledge or discourse," will be adopted. (Gruber 2008) More specifically, ontology can be viewed as a data model that describes objects, classes, attributes, and relations.

One common approach to the delineation of ontological elements is to divide the extant entities into groups called "categories." These lists of categories can be quite different from one another. It is in this latter sense that ontology is applied to such fields as theology, service science, and artificial intelligence. In the naming of ontological elements, it is important to note that there are two approaches to the use of nouns. In one philosophical school, nouns should refer to existing entities. In the alternate school, nouns are used as a shorthand as reference to a collection of object or events. For example the word *mind* would refer to a collection of mental states, and society would refer to a collection of people.

Ontological engineering encompasses a set of activities conducted during conceptualization, design, implementation, and deployment of ontologies. (Dedvedzic 2002) Ontological engineering seeks to achieve the following goals in a given domain:

- Definition of terms
- Establishment of a body of domain knowledge
- Specification of coherent and expressive knowledge bases

In short, ontology defines the vocabulary of a problem domain and a set of constraints on how terms are related. It also gives data types and operations defined over the data types.

Most forms of ontology are expressed in an ontology language and share structural similarities, such as individuals, classes, attributes, relations, function, restrictions, rules, axioms, and events. The basic idea behind ontology languages is to allow software agents to communicate in a knowledge intensive computer-based environment: We are going to concentrate on the following components: (Guarino 1995)

- *Individuals* referring to instances and objects
- *Classes* expressed as sets, collections, and kinds of things
- *Attributes* giving features and characteristics of individuals and classes
- *Relations* that determine ways that individuals and classes relate

The components determine whether a specific ontology is a domain ontology or an upper ontology. In a *domain ontology*, a specific type would be relevant to particular category, such as in a medical or household category. In an *upper ontology*, a type would be applicable to all ontologies in the universe of discourse. In the service ontology, presented in the following section, we are going to be developing an upper ontology for trusted identity in cyberspace.

SECURITY CATEGORIZATION

Security categorization of information and information systems is a means of establishing a framework for information management and assessing operational risk of inherent entities. (FIPS 2004) Three security objectives are identifies:

- Confidentially
- Integrity
- Availability

Confidentiality refers to the preservation of restrictions on information access and disclosure. Alternately, a loss of confidentiality is the unauthorized disclosure of information. *Integrity* refers to controls that prevent improper information modification and destruction. Alternately, loss of integrity is the unauthorized modification or destruction of information. *Availability* refers to the insurance of timely and reliable access to the use of information. Alternately, loss of availability is the disruption of access or use of information or an information system. (FIPS op cit.)

The loss of confidentiality, integrity, or availability is known as the *potential impact* resulting from a breach of security. Impact assessments can be classified as low, moderate, or high. The potential impact is low if a loss of integrity, integrity, or availability would have limited adverse effect on a corresponding organization, asset, or individual. The potential impact is moderate if a loss of integrity, integrity, or availability would have serious effect on a corresponding organization, asset, or individual. The potential impact is high if a loss of integrity, integrity, or availability would have severe of catastrophic adverse effect on a corresponding organization, asset, or individual.

The synthesis of an impact grid for a specific unit of information or an information system would provide a measure of security for that entity. (FIPS op cit)

RISK MANAGEMENT

Risk management is a process to protect an organization and its ability to perform its mission and protect its assets. Defined informally, *risk* is the net negative impact of a loss of confidentially, integrity, or availability. It follows that risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level. (Stoneburner 2002)

Risk management incorporates the processes of risk assessment, risk mitigation,, and risk evaluation and assessment. (Stoneburner op cit.) A formal definition of risk is:

Risk *is a function of the* ***likelihood*** *of a given* ***threat-source****'s exercising a particular potential* ***vulnerability****, and the resulting* ***impact*** *of that adverse event on the organization.* (Stoneburner op cit., p. 8)

Three preliminary methods of assessing risk are system characterization, threat identification, and vulnerability identification. Trusted identity is a significant aspect of risk mitigation in information systems.

UPPER ONTOLOGY FOR TRUSTED IDENTITY

The ontology of trusted identity is a developmental artifact for the study, design, analysis, and application of governance to the complex subject of digital identity in an interdependent network of information technology components. Essentially, an identity ecosystem is required to tie the elements together, so that they are applicable to a wide range of operational scenarios. (White House 2010) The primary measure of an ontological determination is how it assists in delineating the value chain for trusted identity services, comprised of people, technology, and organizations, and its relevance to education, government, business, and other social phenomena. This ontology is distinct from and runs orthogonal to the ontology for identity credentials developed by the National Institute for Standards and Technology (NIST) and published in 2006. (MacGregor 2006)

CHAIN OF TRUST SCENARIO FOR CREDENTIAL DETERMINATION (EXAMPLE)

The basis of digital identity in a networked environment is a credential determined by a trusted source, where *credential*, in this instance is defined as an assertion about a subject issued by a trusted authority. Figure 3 gives a very simple example of a chain of trust for the issuance of a driver's license. The trusted elements in the example are the hospital and the DMV.

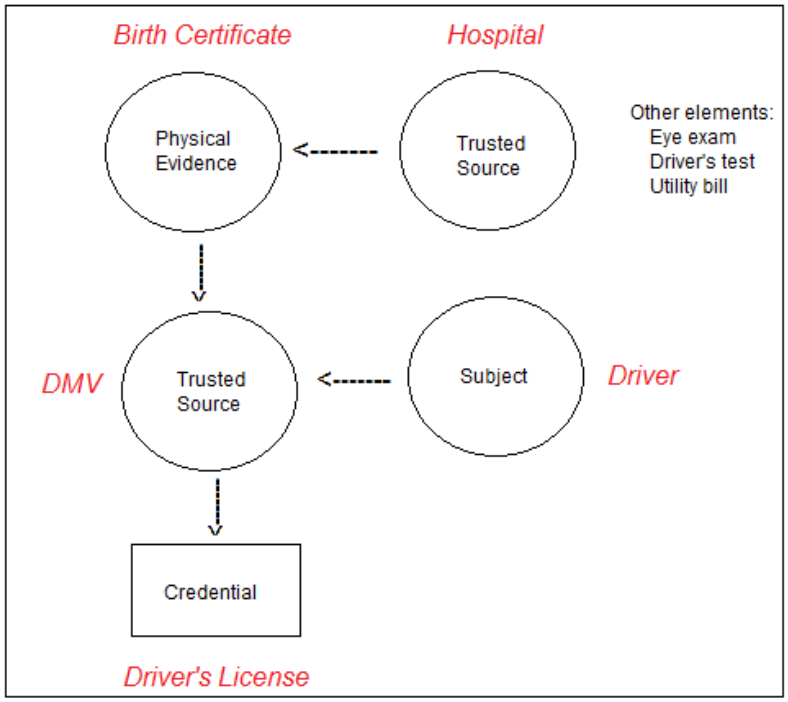

Figure 3. Chain Of Trust Scenario

While a driver's license might not be the best example, because it is a repurposed document serving as a government issued form of identification containing superfluous information, it does demonstrate the process of binding a personal identity with a physical artifact. Issuance of the license by the DMV (Depart of Motor Vehicles)

is an example of "identity proofing" and of the "governance" of a trusted authority, implicit but not mentioned in the scenario.

AUTHENTICATION MODEL

In the trusted authentication model, subjects are sponsored by a Granting Authority, perhaps the subject itself, to enroll with a Registration Authority as a Subscriber of a trusted service protected by a Credential Service Provider. The process is known as Registration whereby the subject, after being subjected to an Identity Proofing, is issued a Token, representing a binding between the subject and an authentication secret. Authentication factors, reflected in a Token, are one or more of the following:

- Something the subject knows
- Something the subject has
- Something the subject is

Categories of relevant identity documents of this genre are covered in the next section.

During the operation of a trusted authentication system, a prospective user, known as a Claimant, presents the token to Verifier for access to a protected service. The Verifier checks with the Credential Service Provider, through an identity registry, for identity verification. If the Claimant is authorized to engage in the requested transaction, it is registered as a Subscriber and an Assertion is forwarded to the Relying party to instantiate the operation.

The ontological elements presented here are summarized in Table 1.

Table 1. Ontological Elements for Trusted Identity

Element	Definition
Assertion	A statement from a Verifier to a Relying Party that contains identity information about a Subscriber. Assertions may also contain verified attributes.
Authentication	The process of establishing confidence in the identity of users or information systems.
Authentication Protocol	A defined sequence of messages between a Claimant and a Verifier that demonstrates that the Claimant has control of a valid token to establish his/her identity, and optionally, demonstrates to the Claimant that he or she is communicating with the intended Verifier.
Claimant	A party whose identity is to be verified using an authentication protocol.
Credential	An object that authoritatively binds an identity (an optionally, additional attributes) to a token possessed and controlled by a person.
Credentials Service Provider (CSP)	A trusted entity that issues or registers Subscriber tokens and issues electronic credential to Subscribers. The CSP may encompass Registration Authorities and Verifiers that it operates. A CSP may be an independent third party, or may issue credential for its own use.
Electronic Authentication	The process of establishing confidence in user identities electronically presented to an information system.
Identity	A unique name of an individual person. Since the legal names of persons are not necessarily unique, the identity of a person must include sufficient additional information (such as an employee or account number) to make the name unique.
Identity Proofing	The process by which a CSP and an RA validate sufficient information to uniquely identity a person.
Registration	The process through which a party applies to become a Subscriber of a CSP and an RA validates the identity of that party on behalf of the CSP.
Registration Authority (RA)	The trusted entity that establishes and vouches for the identity of a Subscriber to a CSP. The RA may be an integral part of a CSP, or it may be independent of a CSP, but it has a relationship to the CSP.
Relying Party	An entity that relies upon the Subscriber's credentials or Verifier's assertion of an identity, typically to process a transaction or grant access to information or a system.
Subject	The person whose identity is bound in a particular credential.
Subscriber	A party who has received a credential or token from a CSP.
Token	Something that the Claimant possesses and controls (typically a key or password) used to authenticate the Claimant's identity.

Verifier	An entity that verifies the Claimant's identity by verifying the Claimant's possession of a token using an authentication protocol. To do this, the Verifier may also need to validate credentials that link the token and identity and check their status.

Source: (Burr 2008), pp. 6-12.

CATEGORIES OF CREDENTIAL DOCUMENTS

Identity credentials identify the issuer and subject and document some qualities or characteristics of the subject, as known to the issuer. (MacGregor 2006, p. 12) Credentials are usually grouped into three categories:

- *Primary identity credentials*, resulting from significant life events, such as birth or marriage.
- *Secondary identity credentials*, issued in response to a request for authorization to perform an action, such as a driver's license.
- *Tertiary identity credentials*, issued by an authority for a limited purpose, such as an employee badge or program loyalty card.

Table 2 gives a summary of the categories of identity documents.

Table 2. Categories of Identity Documents

Category	Example
Identity	Driver's license, Military ID card
Entitlement	Medicare/health enrollment card, Veteran's benefit ID card
Privilege	Professional license, Voter registration
Travel	Passport, Visa
Life event	Birth certificate, Marriage certificate
Employment eligibility	Social security card
Employment verification	Company employee ID, Military ID
Building access	Company ID card, Federal ID card
Citizenship	Passport, Certificate of naturalization
Financial/credit	Bank account statement, Credit card, Vehicle title, Property deed
Obligation	Selective service registration, Military commission

Source: (MacGregor 2006), pp. 24-25.

REGISTRATION

Registration is the first of two major processes that delineate the operation of a trusted identity system. The interactions between the Subscriber, Registration Authority (RA), and the Credentials Service Provider (CSP) are given as follows: (Burr 2008, p. 14)

- An individual applies to an RA for registration.
- The RA identity proofs the applicant.
- On successful identity proofing, the RA sends a registration confirmation message to the CSP.
- A secret token and a credential are established between the CSP and the new Subscriber.
- The CSP registers the credential. The Subscriber preserves the token.

In some operational environments, an applicant may require a sponsor or possess membership in an appropriate organization.

VERIFICATION

Verification is the second major process in trusted identity, delineated as follows: (Burr 2008, p. 14)

- The Claimant proves to the Verifier that he or she is in possession of a required token through an authentication protocol.
- The Verifier contacts the CSP to verify that the token and credential have been conformed and the Claimant is a Subscriber of the CSP.
- The Verifier generates an assertion that is sent to the Relying Party to determine access control and authorization specifications.
- An authentication session is established between the Subscriber and the Relying Party.

The Verifier may not be distinct from the Relying Party. Depending upon the authentication protocol used, special features, such as digital certificates, may obviate communication with the CSP.

GOVERNANCE

A typical organization has a group of stakeholders who have something to gain of the organization is successful and something to lose of the organization is not successful. The stakeholders, often referred to as *principals*, give the right to manage an endeavor to *agents*, ostensibly qualified to do so and are rewarded accordingly, through the application of policies and rules that represent the principal's best interests. The process is generally known as *governance*. In the domain of trusted identity, governance is primarily concerned with risk management, as introduced earlier.

Risk involves potential harm or impact and the likelihood of such harm or impact. Categories of harm or impact include: (Bolten 2003, p. 5)

- Inconvenience, distress, or damage to standing or reputation
- Financial loss or agency liability
- Harm to agency programs or public interests
- Unauthorized release of sensitive information
- Personal safety
- Civil or criminal violations

Recommended procedures to mitigate risk would necessarily incorporate the following procedures:

- Conduct a risk assessment of the e-government system.
- Map identified risks to application assurance level.
- Select technology based on e-authentication technical guidance.
- Validate that the implemented system has achieved the required assurance level.
- Periodically reassess the system to determine technology refresh requirements.

(The terms e-government and e-authentication refer to electronic government and electronic authentication, respectively.)

Finally, and perhaps most importantly, the governance of trusted identity should operate within the 7 laws of identity: (Cavoukian 2010 and Mercuri 2007):

Law # 1: User Control and Consent

Technical identity systems must reveal information identifying a user only with the user's consent.

Law # 2: Minimal Disclosure for a Constrained Use

The solution that discloses the least amount of identifying information and best limits its use is the most stable long-term solution.

Law # 3: Justifiable Parties

Digital identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship.

Law # 4: Directed Identity

A universal identity system must support both "omnidirectional" identifiers for use by public entities and "unidirectional" identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles.

Law # 5: Pluralism of Operators and Technologies

A universal identity system must channel and enable the interworking of multiple identity technologies run by multiple identity providers.

Law # 6: Human Integration

The universal identity metasystem must define the human user to be a component of the distributed system integrated through unambiguous human-machine communication mechanisms offering protection against identity attacks.

Law #7: Consistent Experience Across Contexts

The unifying identity metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies.

A complete description of the 7 laws is given in (Mercuri op cit.) pp. 37-43.

SUMMARY

The paper is a contribution to the domain of ontological commitment as it applies to a description of subjects, objects, actions, and relationships as they pertain to the National Strategy of Trusted Identity in Cyberspace initiative. Further research would necessarily entail a formal definition of the ontological elements presented in the paper.

AUTHOR INFORMATION

Dr. Harry Katzan is the author of books and papers on computer science, decision science, and service science and is the founding editor of the *Journal of Service Science.* His current research interests are in service design and the National Strategy for Trusted Identity in Cyberspace (NSTIC).

REFERENCES

1. Bayer, C. 2008. Federated Identity Management. Avaleris Inc., (cbyer@avaleris.com).
2. Bolten, J. 2003. E-Authentication Guidance for Federal Agencies. Executive Office of the President, Office of Management and Budget, Memorandum M-04-04, (December 16, 2003).
3. Burr, W., Dodson, D., Perlner, W. Gupta, S., and E. Nabbus 2008. Electronic Authentication Guidelines. National Institute of Standards and Technology, NIST Special Publication 800-63-1.

4. Cavoukian, A. 2010. 7 Laws of Identity: The Case for Privacy-Embedded Laws of Identity I the Digital Age." Toronto: Information and Privacy Commission of Ontario (www.ipc.on.ca).
5. Charney, S. 2008. Establishing End to End Trust. *Microsoft Corporation*.
6. Dedvedzic, V. 2002. Understanding Ontological Engineering. *Communications of the ACM* 45(4):136-144.
7. FIPS 2004. Standards for Security Categorization of Federal Information and Information Systems. National Institute of Standards and Technology, FIPS PUB 199.
8. Gruber, T. 2008. Ontology. *Encyclopedia of Database Systems*, Liu, L. and M. Ozsu (Eds.), Springer-Verlag.
9. Guarino, N. 1995. Formal Ontology, Conceptual Analysis and Knowledge Representation. *International Journal of Human-Computer Studies*, 43(5-6):907-928.
10. Katzan, H. 2010. *Privacy, Identity, and Cloud Computing*, New York: iUniverse, Inc.
11. MacGregor, W., Dutcher, W., and J. Khan 2006. An Ontology of Identity Credentials Part I: Background and Formulation, National Institute of Standards and Technology, NIST Special Publication 800-103.
12. Mercuri, M. 2007. *Beginning Information Cards and Cardspace*, New York: Apress Publishing.
13. Mundie, C., de Vries, P., Haynes, P., and M. Corwine. 2002. Trustworthy Computing. *Microsoft Corporation.*
14. Salido, J. and P. Voon. 2010. A Guide to Data Governance for Privacy, Confidentiality, and Compliance: Part 1. The Case for Data Governance. Microsoft Corporation.
15. Stoneburner, G, Goguen, A, and A. Feringa 2002. Risk Management Guide for Information Technology Systems, National Institute of Standards and Technology, NIST Special Publication 800-30.
16. White House 2010. National Strategy for Trusted Identities in Cyberspace: Creating Options for Enhanced Online Security and Privacy, June 25, 2010, www.whitehouse.gov.
17. Windley, P. 2005. *Digital Identity*, Sebastopol: O'Reilly Media, Inc.

NOTES

