May 7/8; Trondheim, Norway

Context, Terms, Models and Options

for

Digital Identity Management

Daniel "Dazza" Greenwood

Lecturer, Massachusetts Institute of Technology

Director, MIT eCommerce Architecture Program

Principal, CIVICS.com

http://ecitizen.mit.edu

http://www.civics.com

dazza@media.mit.edu

Presented at the OECD Workshop on Digital Identity Management *In Cooperation With* the Norwegian Ministry of Education & Research and Ministry of Government Administration & Reform

Global Identity Management

Digital Identity is Inextricably Part of Identity, Writ Large

Narrowly, Identity Management Speaks to the Life-Cycle Milestones, Data and Processes For Records Related to Individual User Accounts on ICT Systems.

Requirements & Constraints for ID Systems Differ Depending Upon the Context: The Types of Users Identified (vendor, customer, citizen, friend, congregant, whistleblower, etc), the Types of Transactions, Applicable Law and Custom, etc.

Agreed International Identity Infrastructures are Needed to Allow and Protect Interoperability, Integrity, Individuals

Three Clarifying Questions (and one key comment)

1. What is Authentication and Authorization? (Proving ID & What You Can Do With It)
2. What is Identity? (Who we authenticate - complex, evolving with blurred boundaries)
3. What is Identity Management in the Context of this OECD Workshop?

* The OECD Privacy Guidelines Structured Thinking and Propelled Good Policy for Decades – An International Identity Bill of Rights is Needed Now, to Safeguard Identity Autonomy, And Create a Global Infrastructure for the Interoperability and Integrity of Identity and Authentication in All Sectors

Old Concepts of Self: Names are "Significant" and the Power to Name is the Power to Control

Biblical names

In the Old Testament, the names of individuals are meaningful; for example, Adam is named after the "earth" (Adama) from which he was created. (Genesis 2)

A change of name indicates a change of status. For example, the patriarch "Abram" is renamed "Abraham" before he is blessed with children. His wife, "Sarai" is similarly renamed "Sarah." (Genesis 17)

Talmudic attitudes

The Babylonian Talmud maintains that names exert an influence over their bearers:

From where do we know that a name has a causal effect ("shama garim"). Says Rabbi Elazar: the verse says, (Psalms 46:9) "Go see the works of God, who puts desolation (shamot) in the earth." Read not "desolation" but "names" (shemot). (B.T. Berachot 7b)

Furthermore, a change of name is one of four actions that can avert an evil heavenly decree. (B.T. Rosh Hashana 16b)

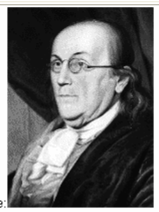
Commentators differ as to whether this influence is metaphysical - a connection between name and essence - or psychological. (See Meiri, Ritva to B.T. Rosh Hashana 16b)

Talmudic sage, Rabbi Meir, would infer a person's nature from his or her name. The Talmud also states that all those who descend to Gehennom will rise, except for three, including he who calls another by a derisive nickname. (B.T. Yoma 83b; J.T. Rosh Hashana 3:9; B.T. Yoma 38a; B.T. Bava Metzia 58a)

From Wikipedia Article on Names

File Edit View Favorites Tools Help

Core Identity Vs. Non-Core Identity Data

Benjamin Franklin	Static	Dynamic
Male Caucasian	+	
Born 1706 in Boston	+	
Tenth son of a soap and candle maker	+	
First job: work for his half-brother James, a printer	+	
Founder in 1721 of the New England Courant, the fourth newspaper in the colonies	+	
Adult appearance: 	+	
Publisher, the Pennsylvania Gazette (1730-48)		+
Common-law wife, Deborah Read	+	
Clerk of the Colonial Legislature (1751-64)		+
Member of the Colonial Legislature (1751-64)		+
Deputy Postmaster General of the colonies (1753-74)		+
Resident in England (1757-62) and (1764-75)		+
Founding father of the United States of America and signer of the United States Constitution	+	
Signature: 	+	
Passed away in 1790 at the age of 84	+	
Buried, Christ Church Burial Ground, Philadelphia	+	

From Economic Modeling and Risk Management in Public Key Infra--strutuctures, available at: http://www.masse.org/rsa97/index.html

Three Models of Identity Management Systems

1. Centralized Ownership and Decision Making

a) The people identified are not in charge of their identity within this system

b) The system adheres based upon command and control from the center

c) Nearly all X.500, LDAP, X.509 and other directory related identity management systems fall under this category.

2. Federated Ownership and Decision Making

a) The people identified are typically not in charge of their identity within this system,

3. Individual Ownership and Decision Making

The Pretty Good Privacy application is a good example of this model, allowing individual users to trade

Three Trust Models

1. Authority Based (agreement is based upon legal obligations sourcing from public law)

a) National Identity Card or National Passport, whereby a nation-state requires a particular approach according under the authority of national law.

b) Public Benefits programs (welfare) whereby the government identifies eligible recipients of a privilege according to enabling legislation, granting legal authority to that agency for such purposes.

2. Power Based (agreement is either based on adhesion or coercion)

a) Large buyer topping a supply chain dictates the authentication and identity management used for systems feeding into its eProcurement application.

b) Large industry player dictates standards and practices required to interoperate with it's systems or applications (however, note that even Microsoft was unable to leverage it's considerable market power to build Passport into an accepted standard).

c) Employer with large workforce may, of course, require use of on or more particular Identity Management solutions as a condition of employment (e.g. "We use Acme HR System here").

3. Agreement Based (agreement is based on free choice among equals)

a) Federated systems, whereby the participating organizations agree to play be common standards and practices.

b) Systems based upon individual agreement to participate (web of trust, etc).

Three Organizational Models

1. Funnel (Usually comprised of a single enterprise, perhaps containing many subordinate organizations, Taking all-comers and homogenizing them into a prescribed, assimilated amalgam, from many creating one, "Self to self").

2. Flock (Clusters of Participating Organizations, Opt-In/Scalable, Common Standards Connecting Heterogeneous Systems, "Open but Bounded", "Friend to Friend"). Liberty Alliance based federations are examples of these clusters, as are the few organizations that have attempted to "cross-certify" using PKI.

3. Fractal (Assertion-Based, No Prior Agreement Between Parties Needed, Permits Compex/Emergent Networks of Relationship, "Stranger-to-Stranger")[PGP, E-Mail]. [Note: MySpace and eBay type systems, while permitting serendipitous encounters among people, are not examples of this because each party has already opted to comply with an agreement (terms of service, terms and conditions, user contract, etc) and operate within a constrained artificial market created to contain, structure and enable certain types of activities – they are not "free range" systems, such as e-mail on the Internet or spontaneous agreement to exchange PGP keys or E-mail addresses – both forms of identity – between potentially any parties.]

Three Technical Architectures

1. CDLIS/Real ID "Pointer-System"

a) Central Pointer File, containing subset of key "disambiguating" information, comprised of records for each identified user

b) Each mini-record in the central file contains a "pointer" to the then current database where the entire record can be found.

c) The pointer information is updated, as the user record migrates from one to another backend databases (representing a move of the user from one jurisdiction to another)

d) The full record pointed to from a central file and residing in a local database is under the ownership and control of the local organization.

2. Probabilistic or Heuristic Systems

a) Based on scoring confidence a given user in fact has a given identity, and that the various partial element of identity in fact combine to a particular individual user.

b) May be based on complex algorithms, contextually weighting information of various types or sources, following contingent or decision trees, and leveraging simple inference or fuzzy logic.

c) Frequently includes query and response with user, posing various questions, using knowledge-based-authentication, and checking responses against a variety of backend or linked systems.

3. Credential Service Provider and Multiple Relying Party Systems

a) An authentication credential (replete with and sometimes merged into the identity information for the subject identified in the credential) is issued by a Credential Service Provider (CSP) to each end-user.

b) The token may be hardware, software or another approach. An X.509 certificate is a good example of such a token. A SAML assertion can also serve as such a credential. Of course, a username, physical token or other data, software or thing may serve equally.

c) The end-user, upon seeking authentication by a participating party, presents their credential and that party then validates the token by reference to the CSP or an outsourced repository of the CSP, and upon satisfactory confirmation may then reply upon the credential and the identity of the end-user. The context within which the end-users identity exists in one such system may, however, be quite different in another, hence affecting assumptions about authority or role from system to system.

Three Contexts of Identity

1. Digital Identity (Username, IP/MAC, E-Mail Address)
2. Physical Identity (Passport, Driver License, Club Card)
3. Dual Identity (RFID exemplar of "Converged Identity", HSPD-12, MIT ID applications – Real ID?)

Architecture of a Safe House for Identity Protection

An International Information Infrastructure for Integrity and Interoperability of Internet Identities (i7)(i5), creating in effect a "white-list" or “Safe Zone” to prevent spam and Identity Theft and unlawful tracking or other information sharing and abuse. In essence, every participating country or organization agrees to certain rules by contract (Operating Rules). The agreement include a commitment to operate or outsource a help-desk for how-to and complaints and commencing dispute resolution (from ID Theft, to tech problems to complaints about the stewards of the identity system).

Cluster of Rights and Duties Under Concept of Identity Autonomy Includes:

- Right to “Not Carry” (anonymity, absent particular non-trivial act)
- Right to Ombuds Attention and Follow Through and Public Reporting
- Right to Reclaim Identity and Start Anew (like bankruptcy)
- Right to Multiple Disposable Pseudonyms
- Right to Encryption of Personal Data
- Responsible for Reporting Suspected Compromise ASAP
- Responsible for Costs and Liability up to a Ceiling (e.g. Reg E, Reg Z)
- Responsible for Using Identity(ies) Without Intent to Deceive or Defraud

Identity Management Control Panel for Each Individual Made Possible by an Agreed International Guideline on Identity Autonomy

- Including “Relationship Management” Panel for Other Individuals or Organizations
- Including “Consent Assertion Markup Language” Management Panel
- Including Logs and Alerts for Prior and Pending Requests, Wizard for Future
- Including Location-Aware, Presence-Aware, Context-Sensitive Privacy/Access Filters for Tracking
- Link to Static Government Identity When Needed by User or for Lawful Demand, Never Otherwise.
- Provisioning of Pseudonyms on Real-Time, Disposable Basis and Real Time Swap-Out of Compromised Authentication or Even Identity

Alternative Title: $P/I+U=N$

or

*Does the "I" In **Identity** and the "U" in **User** Equal the "Person" in **Personalization**?*

*Solving for "N" in **Name***

Contact Information

For More Information:

http://ecitizen.mit.edu

http://www.civics.com

dazza@media.mit.edu

650-504-5474

Daniel J. Greenwood, Esq.

Lecturer, Media Lab, MIT

Director, MIT E-Commerce Architecture Program

Principal, CIVICS.com