Authentication and Identity Management: Information Age Policy Considerations *

By Daniel J. Greenwood **

Introduction

For leaders in the public sector, the emerging debate over identity management and the selections of technology to authenticate citizens and business will be among the most important of all matters to shape the coming information age. Indeed, as with so many issues central to government leadership in the information age, the key ideas are as old – or older – than the country itself. So it is with the recently invigorated debate over identity management. The competing policy interests range from protecting citizen freedoms, privacy and other prerogatives on one end of the scale to ensuring law, order, national security, and institutional efficiencies on the other end. Indeed, the philosophical and political implications of choosing various proposed solutions cut to the core of the relationship between government and citizen – is creation and use of a person's identity flatly subject to central decree or must it be based upon consent of the governed? The current system of identity in the United States is, at best, a patchwork of different – sometimes inconsistent – processes, practices and rules of law.

Key Questions for Policy Makers

Among the key questions of the day: is it desirable to require a single national ID for all citizens? Whether or not it is desirable, is it necessary in order to preserve order and national security? Is it necessary to avoid such an ID scheme in order to preserve civil liberties and prevent inevitable misuse and abuse by centralized unaccountable authorities? Are there other creative ways to accomplish the legitimate business, law enforcement, intelligence and civilian government objectives that driving the need for more efficient identity management? What is the proper balance between the competing public policy interests at hand? How does the selection of technical architectures carry within it implied or explicit public policy choices – whether intended or not by the proper decision makers?

The Starting Point: Common Practice and Common Law

The advent of the networked age and ubiquitous computing is pressuring many areas of society to become more explicit about the existence, scope, meaning and usage of the otherwise largely implied depths of personal identity.

The status quo is that people are entitled to conceal their identity by being anonymous or to use other identities by using pseudonyms provided they do so with no intent to commit crime or other frauds. Here is an everyday example: When walking into a store in the physical world, a person has always had the discretion to identify herself if asked, or to decline to identify herself. In fact, there is generally no rule against giving a pseudonym to a store clerk or anybody else when you wish to keep your real identity private.

This can be done, for example, to prevent people from knowing your home identity and risking unwarranted and unwelcome later contact from that person. Unwelcome later contacts could include unsolicited marketing or even undesired contacts by people seeking friendship or romance. At the extreme end of the scale, some unfortunate people require help from their places of work and government agencies to conceal their whereabouts and other personally identifiable information from disgruntled former employees or ex-spouses,

stalkers or others who would do them harm. A milder example of lawful concealing of identity is the movie star who goes in public wearing a wig, using an alias, and trying to "keep a low profile". For a deep treatment of the laws and rules protecting the basic American right to remain anonymous or use pseudonyms, see Anonymity and Encryption in Internet Commerce (http://www.civics.com/content/cryptonon)

Here is the bottom-line: It is today the right of a citizen, absent a specific law to the contrary (as when exercising the right to buy a gun or when seeking a Passport) to use any name they desire at any time, without government approval, unless they do so with the intent to defraud. This has been the basic "common law" rule for hundreds of years (if not more). For that matter, a person is still at liberty to indicate that they are simply browsing or "window shopping" when approached by sales staff and need not even provide a pseudonym if they so choose. There is generally no law against saying "thanks, but I'm all set for now" when asked if you can be helped, or if someone insists on wringing a name out of you, you are at liberty to use an alias.

Some exceptions to this basic rule, beyond fraud, include certain states which allow the use of aliases but require that additional names used for business be registered typically at a town or city hall. Another example of a spin on this rule occurs in states that require citizens to go to court to request a formal change of name. States without such requirements simply extend the common law rule whereby anyone can change their name at will or use various names for various activities. States with statutes requiring a formal proceeding in order to effect a legal name change will also usually allow people to use other names even without specific approval. For example, in a 1969 New York court case, a judge ruled that while the petitioner was not granted a legal name change due to a technical rule, he was still at liberty to use his desired name in all the ways he had always done so. In that case, the person had been known by the single Sanskrit name Arindam for years by friends, family and business associates. In fact, he had registered for his Social Security and automobile club memberships under his chosen new name. This case demonstrates how of what little consequence a "legal" name change can be in states that require it as a formality. In a different court in New Jersey in 1996, it was ruled that a petitioner could effect a legal name change to a single name despite the record-keeping inconvenience to government agencies. In effect, the liberty of that person to enjoy a name change was paramount since, according to American Jurisprudence, the "state's computer programmer's and record keepers were capable of adjusting their systems to accommodate unusual names."

Even in states that require formal name change or "doing business as" registrations for aliases, the Supreme Court has held the general national rule is that any person may communicate political speech anonymously or with an assumed name. This freedom derives from the First Amendment and is necessary to prevent the chilling effects of having to identify oneself with potentially unpopular political views, possible retribution from employers or other personal attack. Whether a given state requires a formal proceeding to change "legal" name or not, people remain at liberty in general to use any identity they wish. When this liberty is coupled with the common practice of using cash to effect transactions in physical environments, it is easy to see how creating stricter management of identity poses challenges for policy makers.

e-Tailing and the Drive for "Usernames"

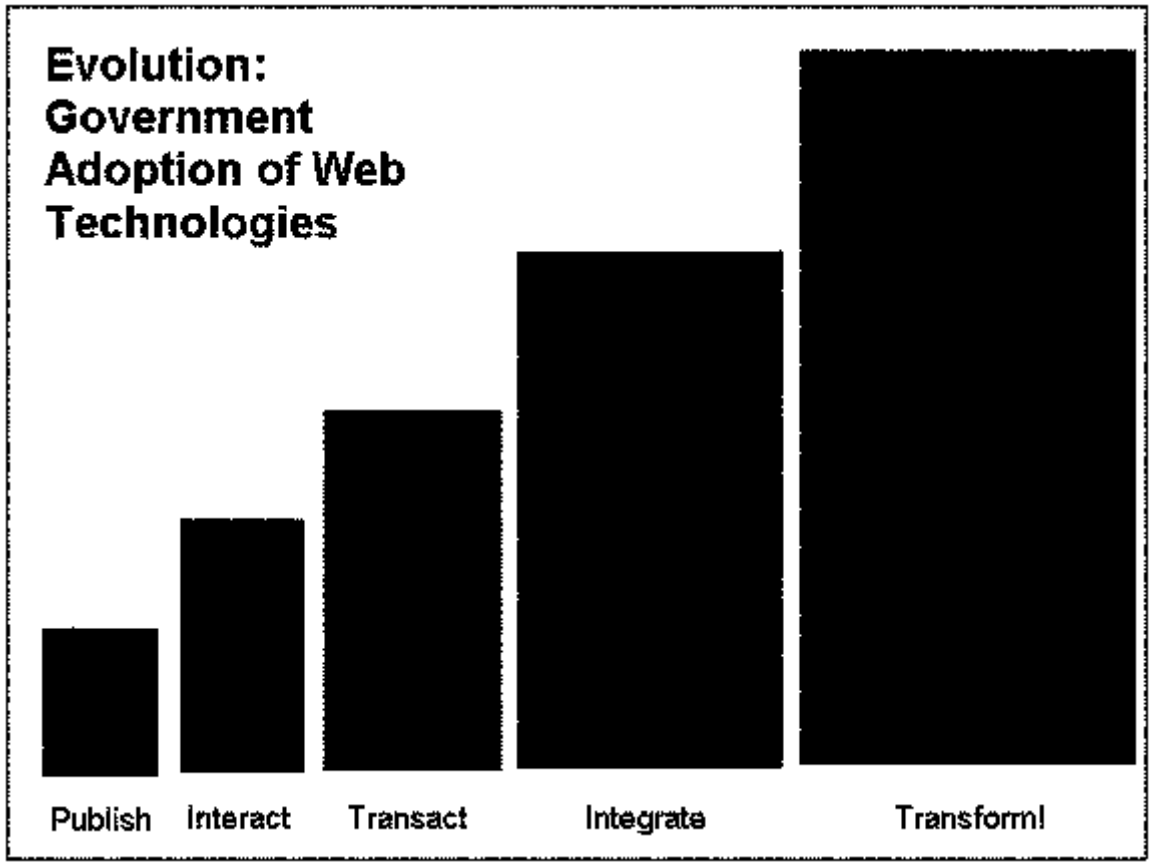
When the same type of retail transaction mentioned above (person "window shopping" at store) is accomplished electronically, it is quite likely that the individual will be required to complete a new user registration process, agree to lengthy terms and condition, in the process, and use a form of payment (typically credit card) that provides a high degree of certainty as to the user's identity. Leaving aside the related policy issues of undesired direct marketing and the process of consenting to have one's personal information shared among business affiliates, it is simply important to note that the business transaction environment for personal identity is potentially

dramatically different when conducted online versus offline. The reasons for these differences, in the retail environment at least, are fairly clear: immediate transactions require immediate electronic payment options; the opportunities for fraud and misuse of automated systems are potentially different in terms of scale and velocity (e.g.: hackers can potentially conduct many fraudulent transactions in a short time) and a perceived business value is assigned to so-called “Customer Relationship Management”, whereby a business web site operator can track the activities and communications with a customer over time to provide higher levels of service and better manage market expectations. But these modern methods of identifying and continually authenticating customers throughout an online relationship have consequences far beyond the initial business drivers.

e-Government and the Drive Toward Integration

The same types of transitions are occurring (albeit more slowly) in the public sector. State government portals are increasingly offering or requiring a “user id” for citizens or businesses to access parts of the public sector web presence. The specific drivers in the public sector are better understood with reference to the diagram below illustrating the 5 stages web enabled evolution in the public sector. The usual first step in adopting a web presence for a government agency is to public a “static” web site. That means a site that simply displays straight text about such things as the agency mission, hours of operation and address and other helpful information. This is like a brochure or infomercial, in that it is “one size fits all” and “one to many” “broadcast style”. The next stage of evolution in adoption of web technologies will often involve the incorporation of interactivity into the web site. For example, a user might be able to input her zip code to get a dynamically generated screen showing all the widget registries in her area. This technology involves use of a data base and some way to generate new screens of information on the user’s web browser according to the information queried or input by the user.

The next stage of development is to turn some of those interactions into transactions. In other words, allowing users to conduct a formal or business type of transaction via the web with the agency. Tax filings, license renewals and grant applications area examples of these types of transactions. In this context, the term transaction does not necessarily have to involve the transfer of money – though it typically does. Filling out an official form or making official statements should be considered a transaction because such conduct changes the rights and responsibilities of the parties in important ways and can lead to serious consequences. After enabling a number of transactions, one or more agencies will feel pressure to begin to make it easy for the user and for the back-office personnel and systems to start to integrate some of the related transactions. For example, it is common for a business to have to file forms with many state (and other) government departments when hiring a new employee. Rather than making the business start fresh on each agency web site, and fill out much of the same information multiple times, integrating the process into a single interface and transaction is more convenient, faster, and less expensive. Theoretically, once enough transactions and interactions have been integrated from the point of view of the citizen or business, then in a very real sense, the government as an entity is transformed. This is certainly true in the eyes of the persons dealing with government. But it will also be true in that these sorts of front-end integrations will force back-end government changes like interoperability of systems, work flows, mergers and other reorganizations that would otherwise not occur. The dream is that this will constitute a transformation of government from a rigid, bureaucratic, inward-looking industrial style organization to a more agile, responsive, accountable and transparent citizen-centered organization.



Governmental, Law Enforcement and Intelligence Interest in Single Identity

One of the prerequisites for integrated transactions is integrated ways of dealing with the identity and authentication of a user who conducts the linked transactions. In this way, the drive toward eGovernment has become one of the drivers for better identity management and authentication of citizens. Tying the various usernames of citizens from different agency systems together becomes one of the keys to achieving integration.

Other public sector drivers toward Identity Management include a desire to better detect, track and catch terrorists – especially in the post attack period in which we now exist. Federal legislation has been enacted to tighten identity document requirements for certain members of the transportation sector. Civilian air travel and boarder crossing has all become the subject of greater scrutiny of identity. In addition, basic law enforcement techniques are also being enhanced by the availability of user authentication data. Combating identity fraud may become one of the biggest drivers for better citizen identity management systems in the future. Ironically, more tightly linked identity systems can also serve as a large problem for those citizens that become the subject to identity theft, or worse – the victim of mistakes or abuse by those who control the systems. This unintended consequence has not been sufficiently considered in the major schemes put forward to date.

Criminals and fraud artists, however, use computers in ways that far exceed simple online fraud. Being able to piece back together trails of digital activity and attribute it to a defendant is an invaluable arrow in the quiver available for crime fighting. The basic concept is that getting the bad guys is easier when all the different identities they use to evade detection can be linked back to them.

Fair Information Practices: Citizens Managing Their Own Identity

Interestingly, another driver behind the concept of "Identity Management" comes from people themselves, and those advocates who support the right of people to protect their privacy and other personal prerogatives. In a sense, citizens are assured better management of their own identity and identity information by each statute or regulation that requires holders of personally identifiable information to be responsive to the wishes of the subject of the data. For example, the privacy rights afforded consumers in the financial sector by the federal "Gramm-Leach Bliley Act" can be seen as enhancing an individual's ability to better manage their identity and use of their identity information. So-called "fair information practices", like assuring the right of people to prevent the sharing of their identity information with third parties without their prior, explicit consent, is a core principle of citizen-centered identity management. These types of policy imperatives animate much state, federal and European law.

Technology Architecture

There are any number of technologies that can accomplish the type of identity management and authentication mentioned above. Technologies are not neutral. They frequently imply a range of practices, legal relationships and other social or business assumptions.

Theoretically, at least, the combination of technologies, legal arrangements, practices and business models that are required to enable so-called "Public Key Infrastructure" (PKI) are supposed to result in a means to manage user identity across various computing systems. Unfortunately, PKI has failed to catch on in the market due to the high cost, difficulty of implementation, user-resistance and mismatched implied business models and practices that go along with it. For more information on the difficulty related to PKI, as it had been proposed in initial form, please see: www.civics.com/pki

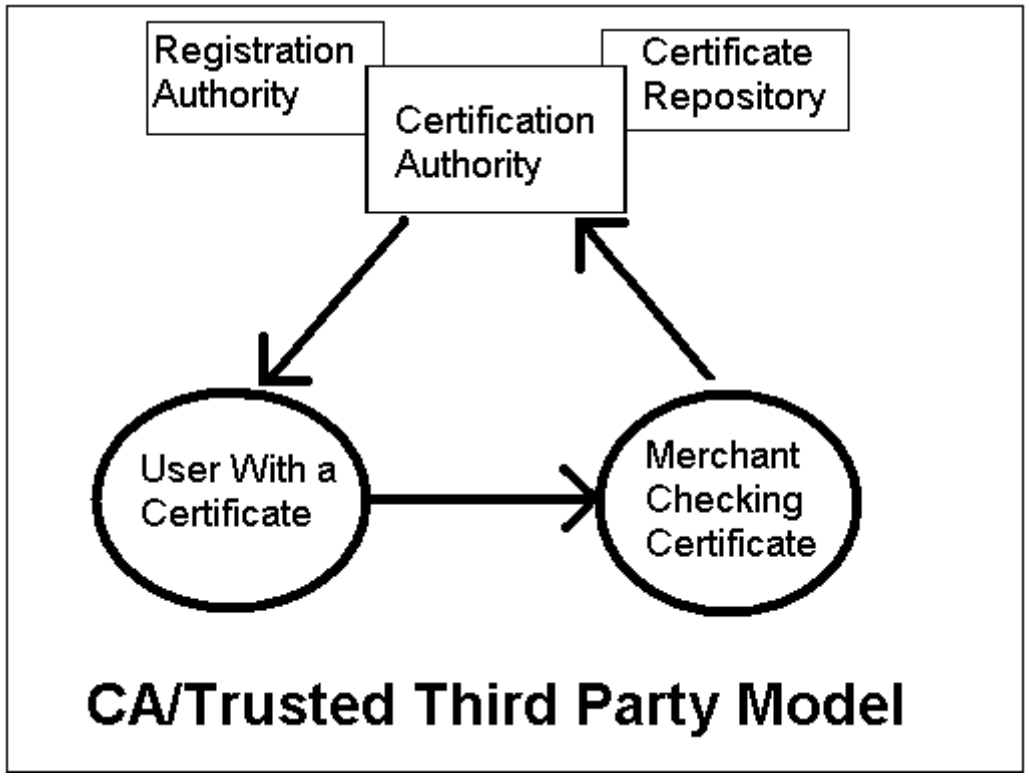
Of course, the use of various public key based cryptographic technologies can be very effective as part of an authentication and security system. For example, the use of Secure Sockets Layer (SSL) is widely used to encrypt web traffic between users and organizations and it is a very good technical protocol. Part of the reason it works so well and is so widely adopted is precisely because it does not require explicit recognition of the PKI preferred business model of a "trusted third party" or any special user software configuration or – more to the point – any user authentication at all. PKI, by sharp contrast, assumes that each individual user is identified once for every subsequent transaction facilitated by that person's "digital certificate". This, in turn, assumes that each person has become subject to a complex set of legal contracts or other agreements and that an overarching set of intertwined global hierarchies of business exist to identify, certify and consistently attest to the name of the person and perhaps their role or authority as well.

Obviously, no such system is widely in use today. More importantly, the very essence of the presumed business problem that PKI was designed to address is a perceived need for one stranger to suddenly do trusted business with another stranger. This so-called "stranger to stranger" commerce was to be addressed by the "trusted third party" who would, in essence, introduce and verify the identity of each stranger to the other. This process stands in such stark contrast to the way business relationships are accomplished today that it has primarily been met in the marketplace with a combination of confusion and rejection.

The vast majority of businesses and governments that use electronic authentication today do so without PKI. This is because the way transactions are primarily done in the private and the public sectors are through business processes that inherently address the question of whether or not the parties should trust each other. The intermediation of a new business party who exists solely to identify and vouch for the identity of another party has no place in existing business processes and does not directly respond to the questions one must ask in order to strike up a trusted relationship with another party. The many-fold issues that accompany business relationship initialization include: market reputation, solvency of the other party, quality of service or product, and so forth.

The methods by which this type of data is collected are all important inputs into the perceived risk and value of accepting a newly identified business partner, supplier, buyer or other affiliate. If the reputation is based upon a testimonial from a trusted friend, that may be even more important that a bond rating. Once the decision to accept a newly identified party has been made, there is a second-order mechanical problem of assuring that communications with that party have not been impersonated or otherwise compromised. Information security technologies, including public key cryptosystems, are good tools to assure these lower-level types of information assurance. These technologies are not, however, a good substitute for the existing elements of due diligence and common sense that underpin the creation of a business or other important relationship between parties that were formally strangers.

The diagram below illustrates the presumed role of a “trusted third party” technology provider of digital certificates called a “certification authority”. Notice that in the utopian world assumed by this model, the user (say a customer of a merchant) and the business may have no other basis of risk assessment or trust building other than the intermediation of the technology provider. This is called the “three cornered model of PKI”, because on one corner there is the user who was issued a digital certificate, on the opposite corner is the party conducting a transaction with the user and who identified the user through her certificate, and on the top of all the market places that might participate in this model exists the certification authority. A slight variation of this three cornered model is the four cornered model of PKI, in which the certificate repository (the technology service whereby a person can check the validity of a digital certificate) could be split off and performed by a different company in a peer relationship with the certification authority. From a business model perspective, there is little difference in whether the technology providers of public key systems services are one or several fold.



By way of contrast, examine the diagram below. This illustration reflects some of the types of business and other relationships that exist in various markets today. Notice that the common thread in all of these (and many other) important relationships is that they are not initiated or continued by the imposition of a trusted third party technology provider. Rather, in the case of a bank, for example, an account can be set up for a customer after careful examination of the bona fides of that applicant. Once an account is created, the authority for issuing an online user id rests squarely with the bank and not with a third party that comes between the bank and the account holder. Similarly, once certain types of relationships exist, it would be awkward, impractical or simply undesirable for the identity process to be under the authority of a third party. Rather, the process of identification and naming is a very "context-specific" affair. Former Speaker of the House Tip O'Neil used to say that all politics is local. Similarly, it can be said that all identity is local as well. Not necessarily geographically local. A parent can have children across the country and a bank for example can have account holders all over the globe. But they are "logically local" in the sense that they are all "home grown" and make sense largely only in their internal context. The account number by which each banking user is primarily known and the attributes surrounding that number are not similar to the naming and identity scheme required by medical clinical systems, for example. One size does not fit all because the subtle contours and content of identity is not monolithic.

It would, of course, be possible with enough effort, money and force to create a single identity system that all parties were compelled to use. But the mere availability of technologies like PKI that make such a system possible do not address the underlying political, policy, legal, business and practical reasons why the world is currently comprised of many different, overlapping or totally separate identity systems. Nation ID styled identity management in reality would require management of all the underlying processes and practices in which people engage and that names are simple byproducts of.

Risk Tolerance and Risk Management:

In making a decision about whether a given online identification is adequate to permit a transaction, one must make a risk assessment. It is the unusual transaction that would require close to 100% certainty as to the identity of a party. Consider that transactions – even important ones – in the physical world are laden with opportunities for fraud, error and other confusions. Paper is not especially secure, as a technology. Virtually no system is immune to abuse by motivated people on the inside of an institution or process. In the end, there is no 100% solution to security. Rather, subtle judgments about acceptable risk must be made. This is certainly true with respect to online authentication of identity.

It should be recognized that risk assessment is fundamentally subjective. It is a reflection of how much risk the assessor is comfortable taking and how one perceives the odds and varieties of future possibilities. This is – in a sense – real guess-work. There are, however, predictive models that can assist. The best model is the brain of a person who is very experienced in a given field of activity and who can extrapolate from that experience. The insurance industry has done a good job of formalizing this type of experience into actuarial and other tables and models. In the end, however, much opinion and nuance is input into the risk management process.

Some state jurisdictions are frankly less tolerant of risk and fraud than others. Of course, the less tolerant of risk one is, the more one must be prepared to spend and do to manage the risk. Every state should apply risk management and principles of acceptable rates of risk, at a minimum, for transactions where only money is at stake. Other transactions that carry policy implications – like citizen privacy, or political implication are less easy to subject to a risk equation. Additional layers of security and controls may be appropriate based upon political and social values. These softer types of values can and should be assigned monetary numbers or other objective measurement as part of an explicit process of risk management.

The following process is one way to establish and manage risks of all types of systems, including authentication and identity management systems.

Risk Identification and Quantification (e.g. Spotting relevant risks and assessing the probability and severity of the prospective harm that would result. These include the risk of initial mis-identification, the risk of later forgery or identity theft, and the risk of internal abuse.). This initial evaluation must be done first, and then the following 5 steps can be applied and repeated until the risk is acceptable or it is determined that the plan is too risky to commence at this time.

1. Risk Avoidance (e.g. Strategically choosing and structuring the business model or transaction types and technology selection in such a way that the business value remains but some of the identified risks are not implicated in the first place.);

2. Risk Reduction (e.g. Implementing the chosen business transactions and technology architecture in such a way that the remaining identified risks are mitigated in terms of probability of occurrence or severity of loss. Also known as Risk Mitigation);

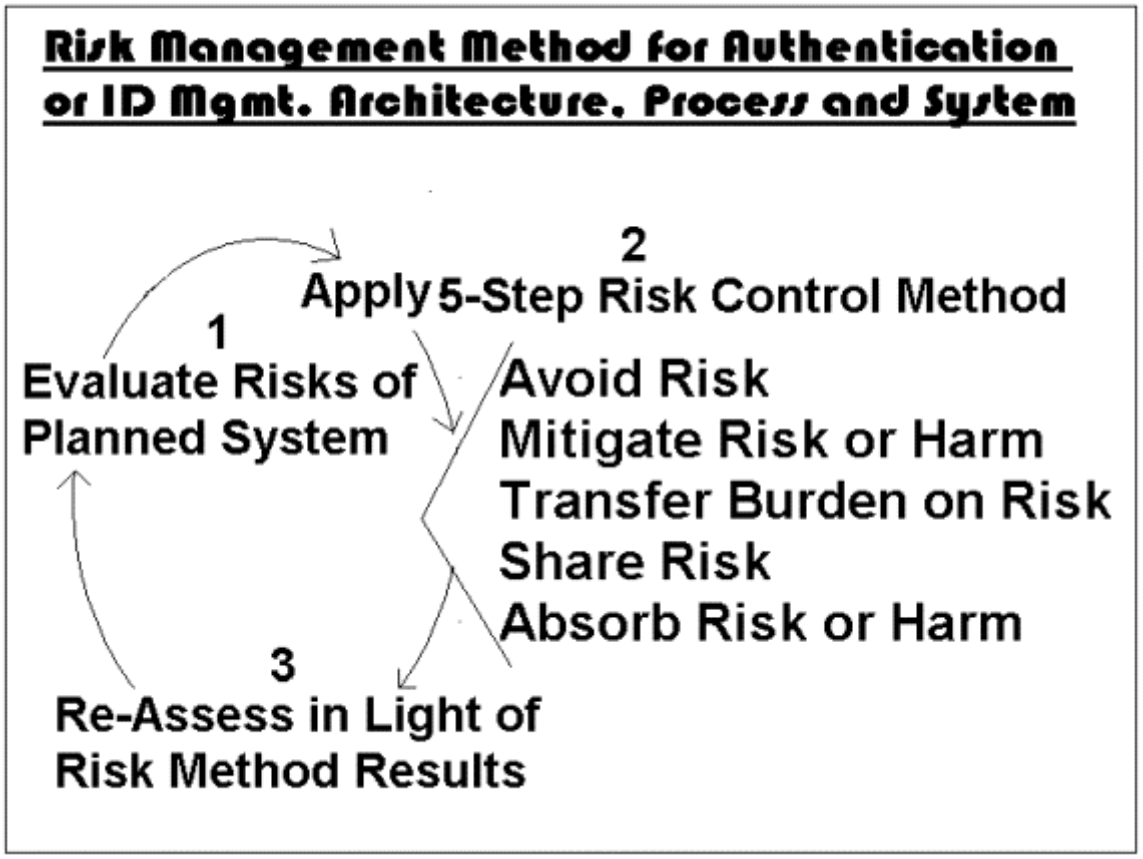
3. Risk Sharing (e.g. Creating a so-called “captive” – that is, a group of parties who shoulder certain risks and who are willing to fund a private group capital reserve among themselves to insure against those risks. This is a private, closed insurance pool. Note, unlike “Risk Transfer”, where the risk is shifted to other parties as completely as possible, with “Risk Sharing”, all the member parties agree up front to contribute capital to the shared reserve.);

4. Risk Transfer (e.g. The most obvious measures include prior use of financial instruments like insurance or bonding and the use of contract terms whereby liability and other risk of loss is shifted to other parties. Risk transfer can also be accomplished by structuring the business in such a way that a different body of law applies whereby other parties are subject to certain risks without the need for private contracts [this “transfer” strategy is actually best accomplished prospectively as part of “Risk Avoidance”]. This is also known as Shifting the Risk);

5. Risk Absorption (e.g. Recognizing that the harm that would result from risks that have not been avoided, mitigated or shifted will have to be born outright. Strategies for dealing with this residual risk include the creation of strategic capital reserves or more formal “self-insurance” programs. Note that even if insurance or “captive” arrangements are made, the scope of the risks that are shared will

still be limited in some way, and hence there will be residual risk potentially to be absorbed by any given party. In some situations, a state government will be immune to some legal liability based on the principle of sovereign immunity and implementing laws allowing capped tort claims. These types of limits should be considered as part of initial risk assessment and when calculating remaining risk to be absorbed).

The following diagram shows how to apply this method.



Internal vs. External Systems

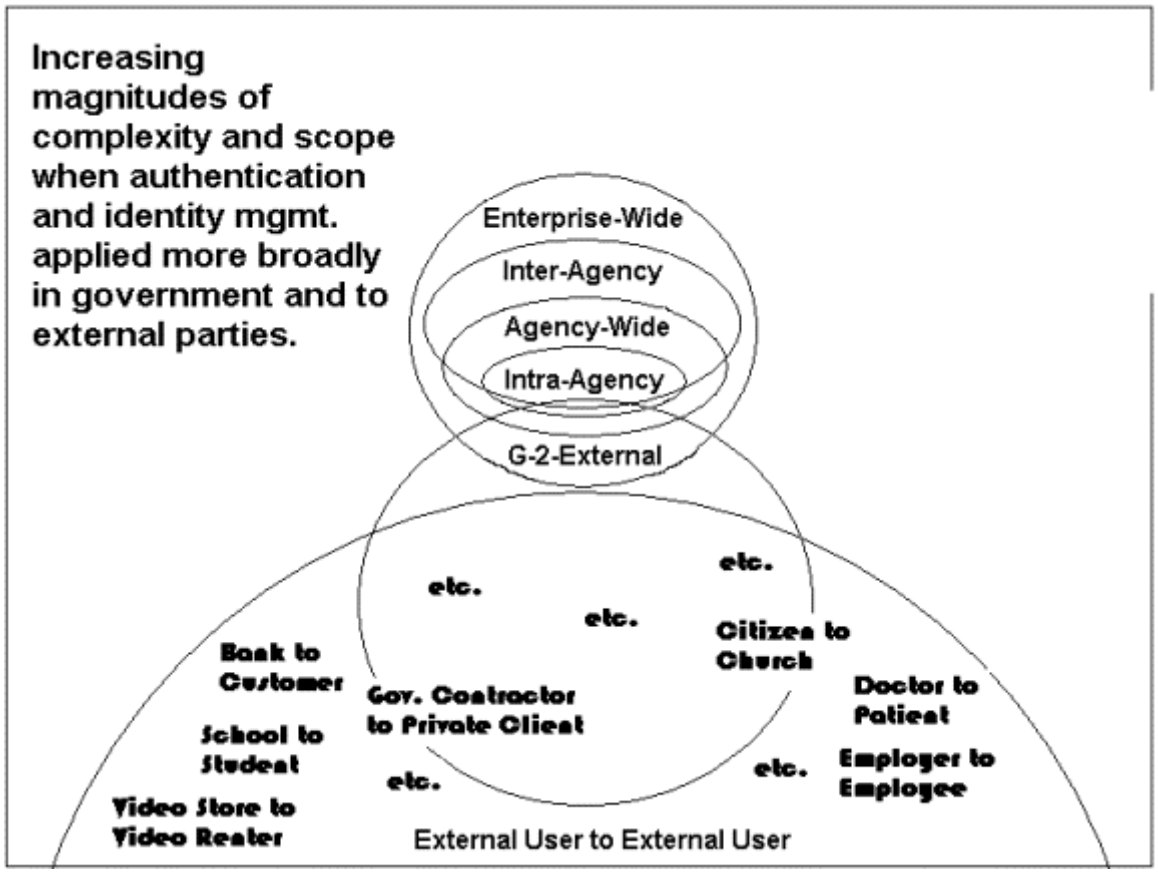
When evaluating the cost, benefit and risks of a planned system of identity management, it is critical to consider the scope of the system. The availability of technologies using web browsers temps planners to assume a system can and will eventually be used by everybody, everywhere. This assumption should be challenged because it carries with it much in the way of business, legal and policy baggage. The broader a system of identity, the more complexity, expense and potent exposure to liability flows from it. Beyond those practical considerations, deeper governance and policy implications also lurk just beneath the project plan.

The following diagram illustrates domains of authentication and identity management from an institutional and organizational perspective. The smallest oval in the middle depicts an intra-agency system for authentication or identity management. Such a system would probably include only employees and/or contractors in one part of a larger agency. You can imagine an e-mail system, set of project management applications with user accounts linked to the e-mail, and an intranet for discussion also linked to the same authentication of users. People who operate in teams on projects and use group-ware benefit from linking identities across applications in this manner.

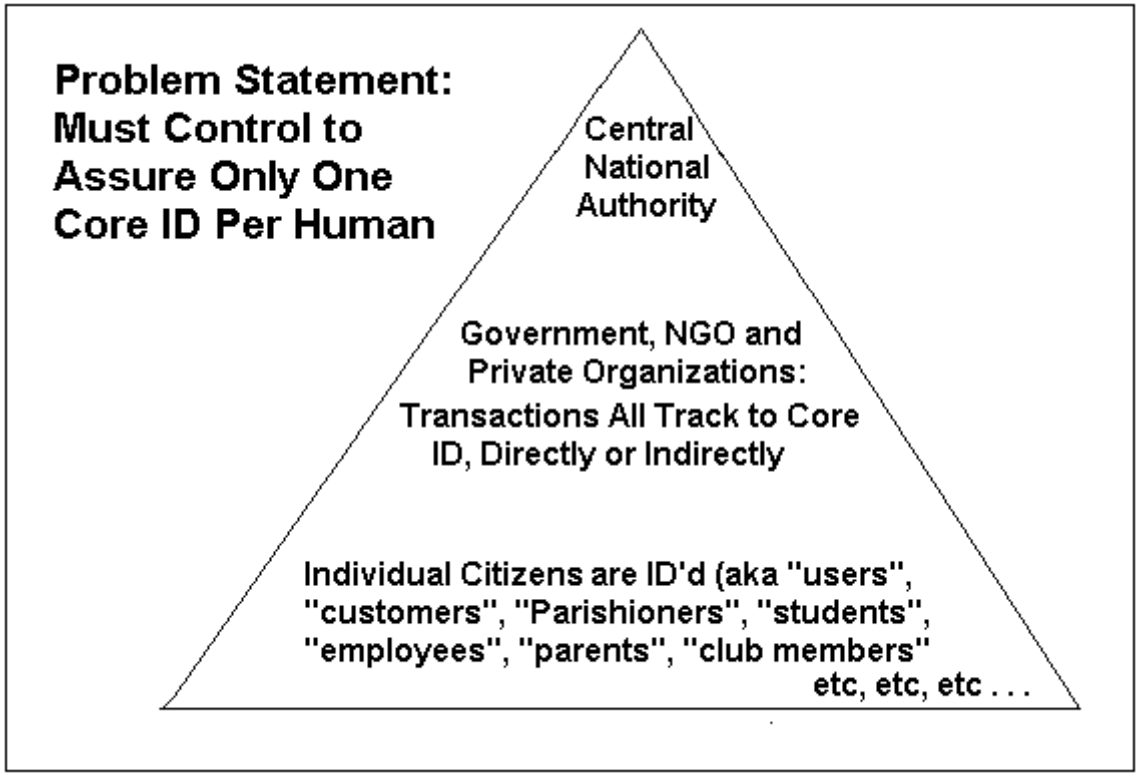
The next level up is the agency-wide application. This is similar, but includes everyone in the organizational unit. Common e-mail systems are the best example at this level, as well as the inter-agency and enterprise-wide levels. Inter-agency applications may include all or only some of the constituent agencies, which is why the oval does to subsume the entirety of the agency and sub-agency ovals. Enterprise-wide identity systems, by contrasts, are larger than and cut across all lesser-included subdivisions at the agency, department or unit levels. The orders of magnitude of complexity in getting more than one agency to use the same systems, business processes and command structure necessary to enable such systems is far in excess of what is necessary to accomplish the same plan at the sub-agency level among colleagues. This is because the business units involves people who are on the peer level and who frequently have different business objectives and processes that must be respected. Someone – or everyone – must change to accommodate these new types of systems. This, among other things, causes additional difficulty. That difficulty is magnified at the Enterprise level of planning and requires direct leadership and intervention in order to be accomplished.

All of these increasing levels of hardship, however, pale in comparison to what occurs when systems of identity and business processes from internal operations come into contact with those from external entities. Whether those external entities be other states, other levels of government or private sector organizations, they are all difficult. Of course, when the other levels of government are localities that can be directed to act by the state (as is the law in some jurisdictions), the difficulty is greatly reduced. In fact, it is a qualitatively different type of difficulty. This is because there is a hierarchical relationship that exists and one party can demand action by the other. By contrast, when an organization like a state government seeks to create an identity management system with an external organization that it can not directly control, like another state, a private company, or even a cluster of companies, then a strategic approach is needed. The interests, preferred technologies and approaches of the other parties become critical to accommodate. Similarly, the underlying rights and obligations flowing from identity control will need to be apportioned among the stakeholders with the responsibility to stand behind them. That suggests that a federated system of some kind is needed rather than a command and control system.

Notice that the government to external systems (g-2-external) involves two ovals that can be thought of as equally large (or perhaps the external system is larger, in that it can not be ordered around). Nonetheless, assuming there is some specific business reason for the government and external systems to interoperate, then it is possible to assign a value to the benefit of that synergy. For example, if each organization saves $100 million, then even a few million dollars in cost and hassle in combining the systems may be worth it. More typically, while technology makes many interoperations and shared identity transactions possible, the business and legal demands that must be answered make it infeasible. In addition, it is necessary to create governance layers to manage such inter-enterprise systems whereby the stakeholders all have a proportional say in the structure and rules. This means it is best to only attempt planning identity management systems when there is a clear business case for them, and to leave more global systems for future phases of development when more is known. Notice also that the creation of an Identity System by government that would be used by purely external parties can be seen as much larger than state government and immeasurably more complex and difficult to create. Arguably, such systems should be the result of many more decades of experience and practice rather than built now, in advance of the business, governance and legal regimes necessary to support them.



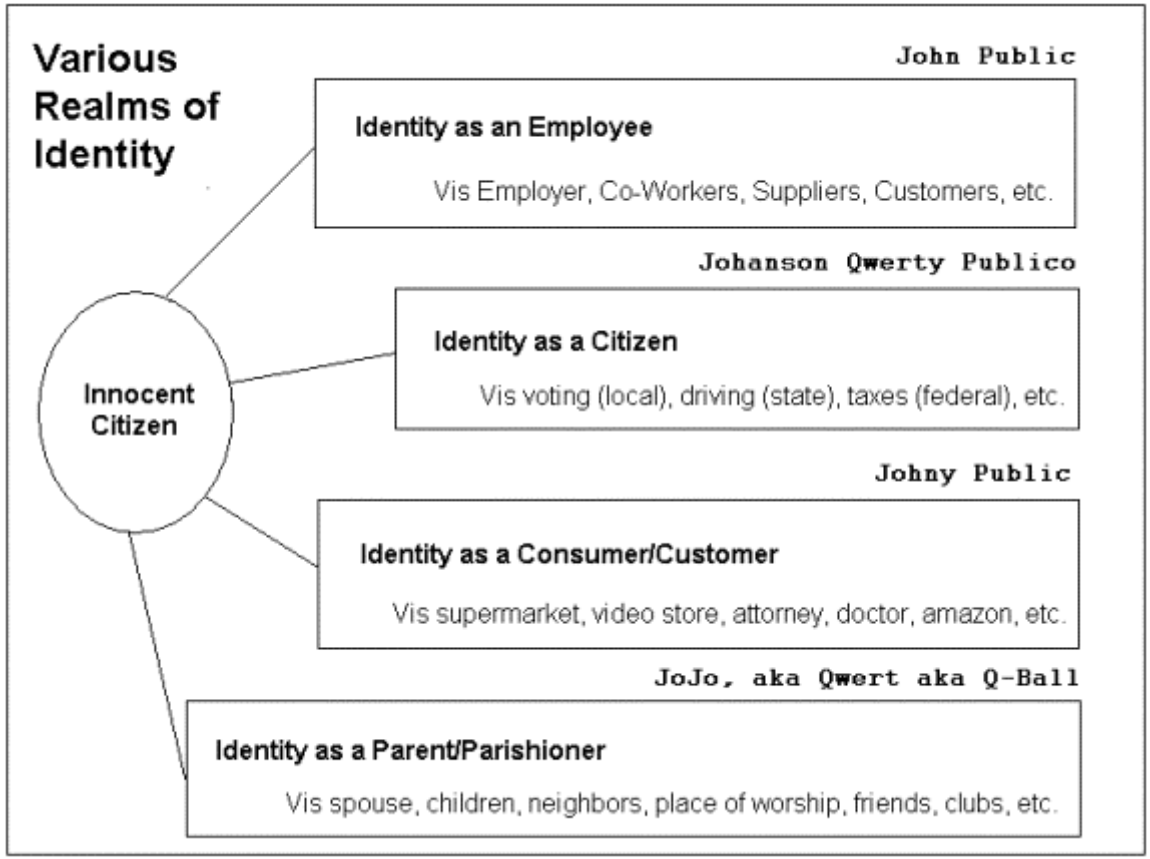
Consider the following diagram. This is a more explicit visual statement of the presumed model of a “core identity” as part of “identity management”. In this model, while people may continue to enjoy several different identities, every ID must track back to a single “core identity”. This would assume that all sectors of the economy and society will operate by or on behalf of a central identity management authority of some kind. Such a central authority would be responsible for providing the technical and business rules whereby all other identity systems are capable of interoperation and traceability back to each user’s single core ID.



Such a global system, while potentially attractive for certain commercial and law enforcement applications, carries with it tremendous hurdles. It is, in effect, the eternal to external problem illustrated in the previous diagram.

Realms of Identity

The next diagram illustrates another approach. It shows the existing world of many identities held by an individual – none of which necessarily must intertwine with others.



The above diagram shows a type of user-controlled identity management that allows for many different types of systems and relationships, depending upon context. This approach is supported and reflected in the Liberty Alliance technical specification for identity. This type of technology allows for single sign-on across different enterprises by an individual, but linking identities would have to be done based on the consent of the individual and it would be possible to maintain more than one different ID. This is another example of how choosing a given technology architecture carries with it policy and legal choices as well. The Liberty architecture is a worthy first step toward creating better, more flexible methods of using today's legal and societal norms while also allowing better identity management from an individual and an institutional or inter-institutional perspective.

Reasonable minds will (and apparently do) differ on which principles should guide the policy, legal, business and technical architectures for identity management systems and practices. In the end, it will be necessary to devise creative methods and approaches that support and a balanced reflection of each of the competing interests.

* Please note that this paper is a draft of a more formal article to be published in 2003. Suggestions, corrections or other reactions are welcome. The final version will be linked from www.civics.com.

** Since 1998, Daniel Greenwood, Esq. has been a lecturer on eGovernment and eCommerce policy and information architecture at the Massachusetts Institute of Technology (MIT) School of Architecture and Planning and since 1999 has been Director of the MIT eCommerce Architecture Program (http://ecitizen.mit.edu). For nearly 6 years, Mr. Greenwood had served as Deputy General Counsel and later as Acting General Counsel to three Chief Information Officers of the Commonwealth of Massachusetts. Daniel Greenwood has testified several times before the U.S. House and Senate on matters of electronic commerce, electronic signatures and public policy in a federalist system. Currently, Mr. Greenwood consults to government and private companies on authentication and electronic transactions system, policy and law in association with the **CIVICS.com** consultancy.