# Best Practices in Managing Identity in Digital Government

Identity management is an infant science, with very real uncertainty. Therefore the most important recognition is that no initial implementation will be flawless at first implementation. Flexibility and the capacity for incremental change are therefore  the lynchpins of a successful identity management plan for e-government.

The uncertainty in identity management exists on three dimensions: technology, privacy, and processes.

*Technologically* there are emerging cryptographic methods, biometrics, mobile devices, and secure hardware.

Emerging cryptographic methods include threshold systems that can be secured according to the different needs of distinct authentication providers. Many of these are options unimaginable in the paper realm. Group cryptography, for example, allows for the proof that a person or device is part of an authenticated group without providing unique identifying information.

Biometrics offer much promise, yet there are significant risk with a biometrics design based on misperceptions.

The processing power and mobility of devices also changes issues of authentication.  Communications and computing devices can be associated with a specific person, a particular role of that person, or may be shared by multiple people who all fulfill the same role. Devices also change hands, often with personal authenticating data remaining on the devices.

Secure hardware solves technical problems but creates policy problems.  The largest use of secure hardware is currently to implement tying of products and reduce customer choice. Therefore that secure hardware exists dow not necessarily make it in the interest of e-government providers to use it.

*Privacy* constraints are not yet determined for provision of services on-line. Citizen expectations of privacy may be in conflict with citizens' desire for efficient on-line service.  Citizen risk perception, and thus policy responses, are not altogether rational. For example the Personal Earnings and Benefits Systems offered personal reports on-line using slightly more authentication than the long-practiced phone version. In response to the privacy concerns the system was suspended, then canceled, then replaced with a less secure method using only a purchased mailing list without user authentication. The Social Security Administration was trapped between two conflicting dimensions of privacy: making information available to the data subject and ensuring that data about one person are not released to another.

The *processes* for security risk management are not defined in terms of process across digital government. The economics of security are uncertain, and is in fact only an emerging area of research. There are not formal quantifiable metrics that are useful for comparing conflicting goals; for example, the risk of information disclosure and the risk of denial of service to an authorized user.

Finally, good definitions are key. Identity as a solution cannot solve an under-specified problem.

## Technical Best Practices

A critical element of authentication is that the *authenticator must also be authenticated*. If the system is not configured to authenticate itself to the citizen then effective attacks can be used to misdirect the citizen into disclosing their own authentication information inappropriately. Currently the only method to implement this is to institute an SSL connection upon the first request from the browser. Digital government services may choose to develop their own key hierarchies. However, this may decrease trust in the system if the result is a warning that the key is not from a pre-installed root. Digital government practitioners may choose to purchase a verified key; however, this results in a situation where the citizen trust the government because the government has paid a company to extend trust.

*Technology neutral specifications* are optimal for two reasons. First, risks cross technological boundaries. Loss of data is loss of data regardless of platform. Authenticating information may be lost from physical devices or software failures. Second, focusing on a single technology may result in a focus on a set of particularly well-understood risks or may result in unnecessary bundling of functionality based on a assumed implementation.

Beyond the technological neutrality, biometrics are often touted as the solution to the authentication problem.

*Biometrics do not necessarily provide unique universal identifiers*. Biometrics may not identify individuals uniquely; for example facial recognition. Some biometrics (e.g., handprint geometry) are useful only to verify a claimed identity. Some biometrics can be used to identify anyone enrolled in the system (e.g., fingerprints and iris scans) yet there will be some who cannot enroll.

In order to minimize risk of loss d*o not store raw biometric data for authentication.* When biometric data are used as pass phrases, the security of the data are critical. Once biometric data are compiled into a database or accessible over a network biometric information is simply data and data can be stolen. For example, if the connection to a fingerprint reader over the network is not completely secure false data may be fed into the connection.

Biometric authenticators pose particular problems once subverted. Thus any design based on biometrics must include the possibility that there is a loss of control over the authenticating data. *Biometric systems require measures of loss recovery.*

Finally, biometrics are available to any entity with a reader. Therefore it is impossible to control the security of a raw biometric. The authenticating entity can control the template, and the encryption method of the biometric but never the raw authenticating data.

In any authentication system, including biometric systems, the temptation is to manage for the false positive rate. The false positive rate is the rate at which impostors are allowed into the system. Conversely the false negative rate is the rate at which authorized users fail to authenticate. In all systems it is critical to *be as rigorous with the acceptance of false positives as with false negatives*. Biometrics systems in digital government pose a particular challenge as minorities are more likely to experience false negatives; and the more e underrepresented the population the more likely is the false negative.

## Privacy Best Practices

Privacy is a problem that is easier to solve with consideration beforehand. Privacy by design is better than post-hoc liability. The phrase from the workshop is that *privacy is better built-in than bolted on.*

Privacy enhancing technologies can resolve the conflict between citizens' desires for efficient service and an expectation of privacy. *Privacy enhancing technologies are most effective when integrated in the design stage.*

Privacy has many dimensions. Some people may want to be left alone; and a simple lack of follow-up contact is adequate. Others are concerned about their autonomy and fear a digital Big Brother. In order to address different concepts of privacy, *use the principles of data* *protection.* In most cases if the data are protected privacy is inherently addressed.

The essential principles of data protection can be summarized as:

1. No sharing
2. All data collection requires advanced permission
3. Justification required, including a clear specification and minimum use of data
4. User review and correction of data

This requires, above all, *knowing what information is needed for any given task.* Note that the requirement for justification of data compilations will be echoed in the process best practices for managing security risks. Limiting data compilations decreases security as well as privacy risks.

Both for privacy and particularly for authentication data, *be aware of the lifetime of the data.* Data that are no longer useful may become a liability. Keeping data with no specification for use is hazardous to privacy and risky in terms of security management.

Data protection provides a minimal threshold for protecting privacy. Anonymity provides the highest degree of privacy. Thus implementing data privacy does not remove the need to create anonymous alternative to services when possible.

## Process

The most critical element of implementing an identity management system is to *have an exit strategy.* Given the range of uncertainty, there will be some strategic failure. Even the most perfect plan can be improved and must be upgraded over time. Even a perfect, flawless strategy that predicts exactly citizen response, diffusion, and integration with current systems will require upgrades as processing power and thus key lengths are altered.

*An exit strategy requires avoiding lock-in.* Lock-in can result from any part of the technology. Examples of problematic lock-in within computer networks range from the centuries old lock-in by knowledge eternality of the QWERTY keyboard to the modern shortage of Internet Protocol numbers created by IPv4. Lock-in can result from the technical implementation, the user base, or the the protocol.

*Data formats will be an increasing cause of lock-in.* The use of digital rights management mechanisms for protecting data formats may offer improved security for the user. However, given the Digital

Millennium Copyright Act, creating interoperable software with a format protected by encryption is a felony. Therefore *selection of open formats is critical*.

*Open code provides the greatest flexibility and prevents lock-in.* Open systems, when available, prevent forced upgrades, prevent loss of control over data, and enhances long term strategic flexibility. Interoperable

A critical part of any strategy addresses *initial rollout and the diffusion of upgrades*. The ability to change or grow in an organic or by degrees will complement any exit strategy. The ability to have a limited rollout distinguishes the failed X.509 and successful Pretty Good Privacy methods for key distribution.

An understanding of both an initial rollout strategy and the issue of upgrades creates the ability to *plan on post-production changes. Pilots and gradual phase-in is risk-averse and allow for institutional learning.*

*Risks can be evaluated against an ideal or a historic baseline*. The historic baseline can be misleading as with the PEBES case mentioned above. In order to evaluate risks in digital government the Standards for Security in Federal Information and Information Processing, which were released in draft form by NIST in May 2003, provide a baseline for evaluating risks in security. The FIPS proposes three questions that must be answered:

1. What security controls are necessary?
2. Are the security controls properly implemented?
3. What is the desired level of assurance that the implementation is functioning as designed?

Within this framework NIST recommends particular attention on confidentiality, availability, and integrity. However, as noted in the false positive and false negative recommendation above there can be a conflict between assuring access to the authorized (availability) and preventing access by the unauthorized (confidentiality).

One way of avoiding unanticipated risks is to *actively pursue early engagement with as many stake holders as possible*. In digital government the privacy community will be one of those stake holders.

In addition to understand risks, *digital government has a unique burden requiring it to communicates risks to citizens*. Of course, the focus should not be entirely on the risks.

*Communicate the value of the service*. Do not hesitate to advocate a service that has been examined and found to be likely to serve the community. Digital government can both provide services, and provide information about the availability and value of services.

Risk communication should be one element of the necessary trust-building in digital government. *Digital* government web sites should build trust through communicating the value added to citizens in every digital interaction. Illustrating the value of the organization is critical in building trust. Agencies as well as companies need to seek citizen trust. Trust can be built by advertising services, reminding users of the value of the services, and then building more services on the basis of trust.

Digital government brings the potential to transform the citizen/government relationship. To implement dramatic changes and effective transformations requires citizen opt-in. Citizen opt-in requires evolving technology, consistent privacy, and continuous information flow on the investments and services provided by government – on and off line.

## Additional Resources

*The Cryptography Snake Oil FAQ*

http://www.interhack.net/people/cmcurtin/snake-oil-faq.html

This is an user friendly guide for evaluating the sometimes purposefully obtuse and technical language claims of providers of cryptographic systems. These rules of thumb have been tested by time, practice, and extensive review.

*NIST Federal Information Processing Standards*

http://csrc.nist.gov/publications/fips/

This site includes both the preliminary report for *Standard for Security*, which offers a set of high level questions for evaluating risk in creating a secure system. Other FIPS include cryptographic standards, security evaluation tools, and authentication management guidelines.

*Evaluation Criteria for Security Mechanisms*

http://www.notablesoftware.com/checklists.html

Provided as a public service by security expert Rebecca Mercuri this longer, and more detailed set of questions will focus the answers to the questions suggested by NIST. Prof. Mercuri offers an additional set of detailed questions for digital voting systems.

*IDs: Not That Easy*

http://www7.nationalacademies.org/cstb/pub_nationwideidentity.html

A National Academy of Science report about the problems with identity systems.

*egov eAuthentication Portal*
*http://www.whitehouse.gov/omb/egov/ea.htm*
A portal for those implementing Federal digital government systems with a focus on authentication.

*Digital Government research sponsored by the National Science Foundation*
http://www.digitalgovernment.org/
Research and findings targeted for digital government practitioners.

This is a consensus document developed at the Harvard Workshop on Digital Identity sponsored by the National Science Foundation. The contents of this document do not reflect the opinions of the US government, NSF or Harvard University.