

## ***Identity the Civic Scenario***

A report by L Jean Camp of a Digital Government Workshop on Identity

### ***The Problem***

The problems of authentication, identity, and access are difficult when combined. These combined problems are exacerbated by the difficulties of authentication, identity and access in government. Using identity as a method for risk management creates a reliance on all other parties that use the same identifying information. The result is a loss of control over institutional risk, as well as a loss in individual privacy.

When a single set of data is used for multiple functions this creates the problem of wildly varying management practices for the same data. Those who obtain low but nonzero value from identifying data obtain such data, and store it according to their own value calculations. In terms of identity and identifiers there is a tragedy of the commons. Very high-value transactions and decisions --employment, professionals managing large transactions -- use the same identity-specific data as very small transactions. Yet when the value of the transactional records is low the level of protection is low. Use of this data resembles use of the proverbial common -- all parties have incentive to use the data but only one has incentive to protect it according to the highest value.

In the paper-based environment transactional histories were sparse and accessible to few. Computerization has made transactional histories detailed, and networks have made them available to many. The increased detail and availability of transactional history has made the data on each specific transaction lower, while making the value of the entire compilation of data higher. Community mechanisms for physical spaces and communities break down for digital communities; similarly identity information used for authentication is no longer secret.

### ***The Process***

The scenario method was developed in business schools to address severe problems where the critical variables and the order of magnitude of the variables were in dispute. The use of the method in the public realm is usually dated to the Mont Fleur event in South Africa in 1991-92. Other notable examples include Colombia where in 1997-98 "Destino Colombia" aided in the leaders in coming to a common vision of peace, and Guatemala, where 1998-2000 "Vision Guatemala" offered a path out of the nation's nightmare.

The civic scenario process typically requires a two day meeting with the construction of a set of scenarios. Usually groups at the workshop first construct and then critique the scenarios. However, in this case the scenarios were constructed in advance by a teams containing private sector, public servants, and academics from hard and soft sciences. This was because of the technical intricacies that complicate each scenario. Building scenarios on differing technological assumptions in real time would have been to risk a workshop blown off-course by those well-established technological debates closer to religious than scientific argument. Advance scenario development increases the probability of remarkable success in the workshop.

Each scenario was be subject to breakout groups, with each group looking at each scenario once. The second was used to define areas of agreement and areas of disagreement.

There were five scenarios.

#### ***1. Single national identifier***

The idea of a national identifier gained popularity in the wake of 9/11. The national identifier program is moving forward through the coordination of the fifty state drivers licenses' authorities. A similar implementation can be seen in some identity management systems, which concentrate all data in a single account. Currently the Social Security Number is widely used as an identifier but it cannot be said to be ubiquitous and universal. This proposal will draw heavily on the secure hardware technology group.

## *2. Sets of attributes*

The previous scenario offers a single credential. In this proposal each person has a set of identifiers stored in secure hardware or in a series of devices. If the single credential is analogous to a signature, then the set of attributes is analogous to the key ring. In this case the multiple PKIs and devices will have some limited interoperability and potentially complex risk cascading issues. This scenario will draw heavily on the reputation technologies work.

## *3. Business as usual*

In this scenario there will be a continuing growth of ad-hoc identifiers in the business world. The identifiers and practices in the business world are adopted unaltered for e-government. Such adoption is most likely in the form of closed code.

## *4. Ubiquitous anonymity*

Under this scenario the tools of crypto-anarchy serve the ends of e-government. The most effective tools for ensuring anonymity are linked with particular assertions, for example, the assertion of Veteran status. Yet financial transactions and information requests can be made entirely anonymously.

## *5. Ubiquitous identity theft*

As the control on intellectual property collide with the expectations of use, a national tracking system raised fears of big brother. Combined with the fact that most people were already identity theft victims, identities continued to be relied upon without being reliable.

## ***The Results***

The outcome was a report defining the research agenda and a best practices report. The best practices report is summarized here as in the research report. The research agenda including an extended version of these best practices is available at <http://www.ljean.com/files/identity.pdf>. The following is taken from that report. Best practices covers technology, privacy and organizational variables.

**Technologically** there are four major technological trends.

Threshold systems can be calibrated according to the needs of various applications. Anonymous credentials can prove a particular relationship or attribute; while group cryptography can prove group membership without certification of identity.

The promise of biometrics is simultaneously being fulfilled and destroyed. Secure biometrics are being developed, yet large databases of raw biometrics undermine the secrecy that is necessary for some of the systems to be useful.

Mobile computing and ubiquitous computing offer particular challenges for dimensions of identity, including location information, that have no previously been subject to misrepresentation.

Secure hardware solves technical problems. Yet configuration of the hardware can threaten privacy and autonomy.

**Privacy** is under dispute. For some it is autonomy, a basic human right. For others it is seclusion, the right to be let alone. For others personal data are simply valuable bits to trade on the network. Not only can citizen expectations of privacy be in conflict with citizens' desire for efficient on-line service; groups of citizens may have conflicting concepts of privacy. There are conflicting dimensions of privacy: making information available to the data subject and ensuring that data about one person are not released to another.

**Processes** for security risk management must be integrated into process terms in digital government. Economics guides many decisions in the public sphere, yet the economics of information security is inchoate.

Finally, good definitions are critical. Identity as a solution cannot solve an under-specified problem. Identity is a misused word and the definitions were a major contribution of the workshop.