Authentication and Government-Issued Digital Credentials

Identity management is a central problem for cyberspace. Digital network technologies introduce ambiguity by removing an assertion of identity from any context in which we could judge its validity. There are neither external clues nor any opportunities for the subconscious process of judgment that often accompanies the review of physical credentials. Ambiguous identities are a major source of uncertainty and risk in the digital networks that span the globe. Reducing this uncertainty and risk has been a goal for governments and companies since the Internet began its dramatic expansion.

The source for trust begins with governments. Governments confirm identities and issue documents (birth certificates, social security numbers) that are used to confirm assertions of identity and to issue new credentials. The processes used by most governments, however, remain better suited for paper than for digital networks. Meshing these paper-based processes to a digital environment (and to digital credentials) has proven to be difficult

Identity management and authentication will only grow in importance as networked applications and services are further integrated into business and consumer activities. Governments are attracted to the online delivery of services because of the potential for lower costs and improved performance, but expanding the online delivery of services requires robust authentication. Two of the central public policy issues for achieving robust authentication are how to improve digital credentialing processes and how to increase the interoperability and cooperation among autonomous and heterogeneous authentication systems.

These are problems of policy and governance, not technology. Multiple, independent actors will need to cooperate to achieve success. This will not happen spontaneously. How governments meet these public policy challenges will determine the pace and scope for the spread of digital credentials. This essay identifies issues for public policy in managing digital authentication.

1. Improved Enrolment Processes

Identity and authentication are based on documents issued by governments and on transaction histories. Digital authentication will require governments to improve the processes they use to issue birth certificates, social security numbers or driver's licenses. Governments will need to improve and strengthen the issuance and revocation process. Weak processes at the start create the opportunity for fraud and misuse in cyberspace and will retard public acceptance. The current processes used in the U.S. are not sufficient for digital purposes, given the higher potential scope for fraud and misuse. At a minimum, these will require better collection and use of vital statistics. Checking requests for credentials or services against a directory of death certificates is an example of the benefit of better and networked vital statistics.

The digital credential issuance process will also need to be more robust than the process

used for paper credentials. Some countries have used existing processes used for national ID cards (not an option for the U.S.). Others have looked at passport issuance as a model, and data suggests that Americans are willing to appear physically to obtain digital credentials. Agencies need to think about how they will fund what could eventually become a major expenditure, if millions of credential comes into widespread use. Governments and the private sector will need to consider how to use existing identity processes for digital identity and whether to seek legislation or other remedies to improve the issuance of core identity documents.

2. Personal Data protection and Authentication

Trustworthy credentials require either sufficient information for the recipient to make an informed judgment or an acceptance of liability for error by some verifying third party. Transaction histories can provide this information and reduce fraud and error, but they also require some access to personal data. Governments face a trade-off between data protection and fraud. A blanket exclusion on the use of personal data during the authentication process increases the risk of fraud. Authentication systems that are detached from personal data will face hurdles to acceptance. Agencies may need to adjust their privacy policies to allow use of transaction histories while still protecting personal data from unapproved release.

Governments will also need better processes for revocation of digital identifiers and some way to share revocation data with the private sector in a timely and accurate fashion. This is not something governments have done before. One key issue will be the question of access to databases and directories and whether or how to allow commercial identity service providers to access directories that support government-issued digital identifiers.

Effective digital credentials create new risks for privacy in terms of the ability to track online behavior. Agencies will need to consider whether new regulatory or legislative protections are needed for commercial activities that take advantage of federally-issued digital credentials. Major privacy failures will set back public acceptance of government authentication systems.

3. Liability

Governments traditionally do not assume liability for identity documents they issue, but digital authentication will challenge this precedent. Liability protections are necessary for authentication systems to be widely adopted. A failure to resolve liability issues has been a major obstacle to the widespread use of authentication. This is a larger problem that probably requires legislative solutions.

Liability may need to be assigned and limited for both consumers and service providers. The best approach is legislation to allocate liability for both users and issuers using a blend of practices already in commercial use. For consumer-level systems, provisions similar to those that apply to credit cards (U.S. legislation limits consumers liability to $50) will be necessary to manage risk in the use of digital identifiers. If liability is

limited only for consumers, service providers will be unwilling to offer authentication, as the bulk of the risks would have been shifted to them. Legislation that limits liability for service providers, similar to statutes that limit the liability of airlines for loss or accidents, will be necessary.

Creating a floor and a ceiling for liability will limit the kinds transactions that use open authentication systems, but will also enable 'open' authentication systems where there is no previous binding legal commitment among parties to a transaction. People will be unwilling to use open authentications system for transactions whose value is much greater than the legally established liability thresholds. Higher value transactions will move to closed authentication systems based on contracts.

4. Funding New Public Services

Authentication and digital credentials are a new public service. Governments will need to fund this service, and in particular decide if there will be any fees for commercial service providers who use government credentials or directories to confirm identity, or for citizens who use government-issued credentials for private activities (a credential used only for public activities will probably need to be provided free of charge).

Unlike paper credentials, digital credentials will require active management after they are issued. Verification and revocation alone means that governments will face a new set of expenses to support authentication activities. Private use of the government credentials will increase the resource requirements for a system by expanding the number of requests that government computer systems will need to service. Governments will need to either fully subsidize authentication costs or develop a fee structure, such as the transaction fees charged by credit cards.

Outsourcing some government authentication activities could solve some resource and management problems. Most governments will not allow private parties to issue identity credentials. However, governments could outsource other activities, such as managing the verification/revocation process. Governments could pay firms to provide these authentication services, or they could allow companies to pay to provide authentication service and then charge fees for private transactions, letting the private use of government credential partially subsidize public authentication needs. Governments could allow commercial authentication systems to add management of government credentials to the credential services they already provide. This latter approach would provide useful interoperability benefits but would also raise important privacy concerns and could likely require new legislation or regulation.

5. Private Use of Public Credentials

Digital credentials are a new public service. The value of this new service will depend on how broadly governments accede to private and commercial use. Restricting government issued credentials to official use may be a good starting point, but allowing private use would increase cyber security and promote e-commerce.

Governments create identity documents for one purpose, but they are rapidly adopted by markets (and other agencies) for other uses. In the United States, drivers' licenses and social security numbers have become essential all-purpose identifiers, and there will be pressure for a government-issued digital credential for social services (potentially millions of credentials) to be used in a similar fashion. Over time, those governments that issue digital identifiers but do not intend them to be used for private purposes will face increasing political (and budgetary) pressure to reverse this decision. A decision on the private use of government-issued digital credentials is unavoidable, as once they are provided to citizens to access government services, it will be difficult (and inefficient) to limit them to official use.

6. Managing Cooperative Public-Private Processes

Early thinking about Internet policy assumed that market forces would lead naturally to the deployment of trustworthy public networks. Understanding why this did not occur is important for future efforts. Effective governance for authentication will require combining private and governmental efforts. This will include cooperation with both private authentication systems and with other governments. At a minimum, a formal vehicle for discussion and coordination among authentication systems is required. The issues for coordination will be the rules for authentication and interoperability (and this might ultimately lead to some sort of hierarchy or ranking system based on thresholds for enrollment processes, revocation and in the use of personal data.

Developing this framework for governance is one of the principle challenges for the widespread and effective use of authentication systems. Getting a large (but unknown and expanding) number of independent systems to cooperate effectively in authenticating digital network identities will require an agreed set of common elements; transparency in processes; a framework for creating, implementing and enforcing rules. The important elements for cooperation among independent systems are framework and transparency. No single approach will work for all activities. For some issues, government or national processes alone will be sufficient, but for others, a larger multinational framework will be required. The G-7 efforts on Internet security or the Financial Action Task Force are models for building cooperation and common approaches.