July 2002

Managing Digital Identities

Managing digital identities and information is a central issue for Internet governance and the digital economy. Identity management and authentication will only grow in importance as Internet and wireless applications and services become further integrated into business and consumer activities. Progress in resolving issues related to identity and authentication is essential to reach the full economic potential of the Internet and for its expanded use in providing new services. Identity and authentication also have deep implications for commerce, public safety, civil liberties, and privacy.

With numerous large-scale government or transnational commercial identity authentication systems being put in place, the broad problem for the Working Group to consider is how to create governance structures that allow these heterogeneous systems to federate. Existing models for Internet governance have espoused an ideal of self-regulation or self-governance, but the experience of ICANN suggests that this will not work for authentication and identity and new approaches are needed.

A "trusted" network goes beyond engineering concepts and requires a marriage of technology and procedures that allow users to feel confident that important data and messages are confidential, unmodified, and linked to an unambiguous identity. Building secure and trusted public networks requires developing the policies and legal and regulatory structures needed for trust; coordinating theses structures among nations; and determining how they relate to the architecture, technology, and commercial viability of Internet services.

Managing authentication and digital identities includes the problem of assigning and validating trust over networks. Efforts to manage authentication and identity have either had difficulties in providing a sufficient level of trust to be accepted by network users, or in transferring "trust" from one network to another. The problems for digital identity management are to find ways to create "trustworthy" digital identities, to identify the degree of trust each digital identity carries, and to determine how to transfer these identities among networks without degrading their trustworthiness. The users of digital networks will need to find ways to create and implement rules and policies that enable trustworthy identities, and then build the software and systems to carry them out.

The source for trusted identities begins with governments. Metaphysical concerns aside, identity is provided by governments. Governments are the fundamental source of identity, and government-issued identities form the starting point for any trustworthy digital identity system. The birth certificate and the social security number are the starting point for all other means (passport, driver's license, credit card) used to provide identity. They will also be the starting point to generate "tokens" of various kinds (smart cards, certificates, etc.) that will provide digital identity.

Digital interactions will require a recognizable and common hierarchy of trust as to the identity of the parties engaged in the transaction. This does not exist now. Trust is either undifferentiated, network-specific, or limited to unevenly distributed commercial

services. Hierarchies allow individuals to hold more than one digital identity and allow decisions about what kind of transaction to engage in based on the level of trust assigned to a digital identity.

The basis for hierarchy is that trust and anonymity are at opposite ends of the spectrum. Anonymous transactions are inherently low-trust. A refusal to provide a digital identity that can be linked to a physical identity provides the least-trustworthy digital identity. A digital identity strongly and accurately linked to a physical identity is the most trustworthy.

Translating existing governmental identity issuance processes into digital form and creating the structure of rules that will allow an identity issued by one government to be accepted by another will require a cooperative effort between countries and between government and the private sector. Currently the government issues a paper identity token. Governments will need to consider how to use their existing confirmation and issuance process for digital identity. This should not take the form of a smartcard or chip provided to a person, which could be lost or stolen, but a database accessible for confirmation of identities in private or commercial transactions.

In this sense, DNS and the root can be a model for new ways to identify and provide identity documents to individuals. Government would provide and manage the "root" identity upon which commercial services would be based. Networking allows a large number of authenticators to depend on a small number of identity issuers.

The government-issued identity provides the basis for individuals to create multiple classes of digital identities. These classes are differentiated by the degree of liability associated with them for the holder and the degree of trust placed in them by the recipient.

New technologies have introduced ambiguity into the meaning of identity. We will need to consider not only the identity and authentication of persons, but also entities other than people, including software, institutions, and devices operating on a range of networks beyond the Internet. Digital identity systems will need to work for devices as well as persons, and will involve transactions between persons, between persons and devices, and between autonomous devices. The group will also need to consider the linkage between authorization and authentication. Authorization issues will also shape authentication of digital identities and are central to questions of liability.

A completely anonymous world would be neither safe nor productive. Identity allows us to assign privileges and responsibilities, and liability in cases of dispute. At the same time, a world where identity was unbreakably linked to every action would be stifling. The Internet offers the possibility of both worlds. Individuals will want a range of identities, from anonymous or near-anonymous, weakly-linked identities or pseudonyms, to robust, legally binding identities that mirror the options available to them offline.

Traditional methods of identification, developed over decades of practice and evolving in

the face of new technologies, are inadequate for Internet purposes. Visual or voice recognition and even some digital signature technology are vulnerable to capture and manipulation during transmission over the open, distributed networks that make up the Internet. Advances in digital signature technology promise some relief, as do biometric technologies, but existing digital identification techniques are not yet widely used.

This reflects several factors. Individuals prefer to "manage" their identity (or identities) through a variety of mechanisms. The degree to which they are identified and the amount of information imparted through that identity process will vary depending on their assessment of the benefits and the risks. As with cars or ATMs, identification depends on a third party placed between user and machine, whose "assertion" or "token" can be trusted. Risk appears in the structure of authenticating identity, in the effectiveness of third party authentication and, more importantly, in issues regarding how information generated by identity systems is safeguarded and used.

These multiple levels of digital identities fall into four classes: legal, government-issued identities; derivative identities; persistent pseudonyms; and temporary pseudonyms. The degree of trust that can be assigned to each class depends on the strength of its linkage to the government-issued identity. Close linkages imply high responsibility (or liability) for actins taken with the digital token in the name of that identity.

- Legal, government-issued identities. For all practical purposes, a person is "stateless" and without identity until they receive valid, government issued documents. Use of these identities in a transaction makes them legally binding.

- Derivative identities. Most of the identity tokens people use are derived from government-issued tokens, but these derivative identities can carry high degrees of trustworthiness. Their trustworthiness comes from the strength of the linkage to the legally binding identity and to the degree of liability associated with them for actions taken. Use of these identities can, in certain circumstances, also be legally binding.

- Persistent pseudonyms. Pseudonym means "false name." These are identities created by an individual and used repeatedly for a particular set of transactions. These are not binding, and any trustworthiness associated with them is intuited from their pattern of behavior.

- Temporary pseudonyms are identities generated for a single transaction or event and are not re-used. Digital networks restrict the ability to be completely anonymous (there will always be a network address during the event), but a decision not to provide an permanent identity (logging in as "guest" or "anonymous" or creating a temporary pseudonym) is possible.

There are also four classes of participants in digital identity systems: devices, persons, firms, and governments.

- Devices: Machines or software agents capable of engaging in transactions with others on their own, without direct human guidance. Devices will increasingly populate the Internet. Digital tokens for devices will be based either on the device's legal identity or on a legal identity derived from a person or firm.

- Persons: human beings with government-issued identities.

- Firms: groups of persons who have been issued a legal identity (incorporate means "to be given a body") by a government.

- Governments: The formal political and administrative structure of societies which have, for more than a century, been the source of binding identities.

The rules for interactions are determined by the level of trust required, not by who purports to be carrying them out. Network applications will not need to distinguish among the class of participant to an event or transaction, but they will need to distinguish among classes of identity, because each class carries a different level of trust. If the user has the authority to make a legally binding commitment, it does not matter if this is a firm, a person, or a device (such as a software agent). This will require rules for assigning trust levels to digital tokens.

Devices will be issued identities. These identities can be derivative, created from government-issued identities held by a person or firm, or devices will be able to become a legal person in their own right through incorporation. The rules of incorporation will require, however, that the legal identity of the device be linked backed to persons holding government-issued identities. Devices will ultimately depend on a legal person for their identity. Governments will need to devise rules for assigning identities to devices.

The identity issuance process can be separated from the identity authentication process for high-trust identity tokens. A system for authenticating an identity issued somewhere else does not need to hold personal data. It only needs to know where to go to confirm that the token is linked the personal data and with what degree of trust. It is easier to trust someone to check an identity than to hold personal data to create an identity.

Assigning governments the role of issuing the basic digital identity would limit the number of issuers to a few, well-known parties; take advantage of existing identity issuance systems which are already accorded a high degree of trust; and make multilateral coordination easier to obtain.

This is a different role for governments. Currently, they issue identities and then do very little to confirm them as they are used. This is sufficient for identity issuance linked to an event (birth, naturalization) for which there are many witnesses, but it is insufficient for re-issuance requests – state governments do nothing to verify that requests for reissuance of a birth certificate come from the original recipient. Governments will need to undertake a new function and provide a new service that will be built on existing identity issuance functions.

To date, governments have been unwilling to outsource the provision of identity documents. Control of identity issuance has been a core government function as it is tied to both state security and access to benefits. This accounts for the high level of trust accorded, a level of trust that might be difficult for private institutions to match. However, the functions of issuing and answering authentication requests could be contracted out to private firms successfully if governments put in place rules and safeguards that preserved the high level of public trust.

Ensuring multilateral compatibility of national systems for issuing digital identity will probably require the development of model legislation that can be implemented nationally. In addition, some mechanism for ensuring compliance will need to be developed (as is currently done for financial institutions) and a private sector rating system could emerge.

The rules will for the most part be developed privately, but they lack a common framework of principle, law, and practice to guide them. Existing legal structures for identity and authentication are, for digital applications, sufficiently amorphous (or insufficiently developed) and allow a wide range of variation. Digital signature laws do not always address how identity is assigned or managed. Public scrutiny and oversight and compatibility among systems (nationally and internationally) pose real challenges. Market forces alone will not generate a solution. Improved governance means replacing a series of unrelated, ad hoc efforts with a transparent and accountable system using cooperative efforts among private entities, legislative and regulatory processes, or some combination of private and governmental approaches.

Firms will offer identity services, but the more robust of these identities will be based (as they are now) on a government-issued identity. A credit card and a driver's license or passport identifies you to a car rental company, but you needed a social security number and a birth certificate to get them. For commercially-issued identity tokens to be trusted, there will have to be a common, robust process for linking them to government-issued identities and assignment of liability for mis-issuance. The less robust the linkage and the less liability the commercial issuer is willing to accept, the less networks and persons should trust the identity.

Federated identity systems enable users to engage with service providers through identity providers. Identity providers may be online merchants, local banks, government licensing authorities, financial brokerages, or any number of existing businesses. In this model, identity data and abstracted user profiles are normally kept separate because the enterprise — acting as the identity provider — is financially rewarded to maintain control over its customer identity data. The loss of hard-won customer data — the gravest threat to the enterprise posed by Internet identity service channels — can be defended against by retaining control and ownership of the enterprise's customer data and is achieved with federated identity systems.

Managing digital identities will require governments and firms to jointly develop rules

for sets of relationships that work on a national level and can interoperate on a multinational level. Federation means developing a common set or rules that allow identities issued by different processes and places to be recognized and treated equally. These include rules governing:

- The relationship between persons and devices and the identity issuer. These entail the grounds for issuing an identity. Identity issuance is usually part of birth or naturalization, both of which entail confirmation of the event and the linkage by a trusted third party (the hospital staff or the Immigration and Naturalization service). Rules are needed for how digital identities will be made available to persons and how they will be stored and made accessible for use

- The relationship between issuers. This includes both government-to-government and government/company rules. Countries will need to develop agreed-upon standards on how identities are issued and safeguards that issuers must demonstrate that they have met for one issuer to trust a digital identity token issued by another.

- The relationship between the holder of the digital identity token and the recipient of that token. These will be primarily commercial practices, governed by commercial law, but very strong safeguards and penalties for misuse of digital identify tokens will need to be put into place.