CSIS Working Group on Authentication and Identity on the Internet

Issues Paper, July 2002

The CSIS Working Group on Identity and Authentication's first meeting explored policy and governance[1] issues for managing and authenticating online identities. 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 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 that new approaches are needed.

The goal of governance is to establish a "trust relationship" between any two end identity services, whatever their technology or mission. Federation is one way of agreeing on how to exchange the basis of trust between different systems. The central issue is how to define, establish, and govern trust, particularly systems that link a digital identity to a real person in the physical world.

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.

Left to their own devices, companies and governments will produce multiple, overlapping, and potentially contradictory identity systems. Changing this outcome is a political and policy problem more than a problem of technology. However, technology and policy issues are intertwined. Governance cannot be discussed as a technology-neutral subject because many problems relate in some way to what technology can and cannot do. However, there was general agreement that discussion should focus on policy and not specific technologies and that the group should be "technology-agnostic" (in the sense of not arguing for one specific technology over others).

The current digital environment provides neither a full measure of trust nor anonymity, but operates in a grey area where trust relies on a series of assumptions or on explicit understandings negotiated outside the digital environment. A solution that requires negotiation of contracts between each party is not scaleable. However, a strong identity is not necessary for every network activity. All digital identities will not need to correspond fully with legal identities, and different identities will have different attribute requirements. This means that multiple digital identities will be the norm, if only as a way to manage risk

[1] "Governance" describes the processes for the development, implementation, and enforcement of rules.

and liability.

How governments will interact with the private sector and how to govern that relationship will be a core issue for the group. Governments and the private sector could have different priorities for how identities are established, verified, or used. One participant said, “We are basically going to find the governments bumping into businesses.” Self-regulation can be only part of any solution. Better management of identities will require cooperative arrangements between governments, firms, and private entities.

Trust is a primary component in designing networks so that people will choose to use them in new ways, and some group members expressed an interest in ensuring that user interests are considered as part of governance. Are systems being deployed in a way that makes reasonable opportunities for anonymity or “pseudonymity?” Will they be highly centralized? Do they have fair information practices and what degree of control do users have over how their identity is used?

Traditional concepts of sovereignty will shape any new approach, but a successful solution will need to transcend borders, and thus is beyond the capability of any single state to create. Governments will differ over architectures, given the very different value judgments they will make regarding the nature of identity. Different political cultures will have different views about what attributes to link to a digital identity. One question was whether U.S. issues will be very different from those of other countries, and how attitudes might vary among regions or countries. Governance for a global system for transferring identification data will also make the various national privacy laws an issue. Governments will be central in finding ways “to cut through this Gordian knot of complexity.”

Many assumed that public key technologies, where a third party links an identity to a digital “certificate,” would be widely deployed to resolve trust issues. This has not occurred, in part because cryptography is in itself not sufficient to build a trustworthy environment. At the same time, many governments made strenuous efforts to create the legal framework for digital signatures. Digital signature laws give a “signed” digital document (which can be transmitted over the internet) the same legal weight as an ink signature by using strong encryption techniques. Despite the passage of digital signature laws, they have also not provided a sufficient structure to manage identity, in part because a robust signature in an otherwise untrustworthy environment is of little value. Remedying this requires addressing the broader issue of how to govern individual authentication systems and the federation of different identity and authentication systems.

There was general agreement that the political system is not ready for this problem, but would be interested to see the groups recommendations. Despite this, governments are going ahead and deploying digital certificate for “millions of users.” Other speakers noted that consumers and large parts of the private sector also lack a sophisticated understanding of the identity issue.

The goal of this working group is to develop principles that can guide a system of governance for digital identity management. The product of the group’s work should provide a framework for identity, authorization, and authentication in cyberspace. The primary audience will be policymakers, but some argued that focusing only on government policymakers may not be enough, and in particular, firms and consumers also need guidance and understanding of the governance implications.

Issues for Discussion

Three interrelated themes can shape future discussions of digital identity management: how digital identities are issued; how the trustworthiness of a digital identity is determined; and how to build scaleable cooperation on issuance, verification, and other aspects of digital identity management. Some related questions from these themes include:

Issuance of Digital Identities

- Who issues digital identities and under what common understandings and rules? How should these identities be linked to government-issued identity documents?

- What attributes do the identities provide to allow for verification? What common understandings and rules are needed on the range of attributes needed for verification of digital identities and how they will link to legal identities?

- What rules apply to issuance of digital identities to devices and how will they relate to "legal" identities? Should identities used by devices be differentiated from those used by persons?

- Confirmation and issuance of identity has been a state function of the last several centuries. The foundations of modern identities are the birth certificates, drivers' licenses, passports and social insurance numbers issues by the state to each of its citizens. What is the relationship between commercially-issued digital identities and government issued identities?

Trust

- Do digital identities need to be ranked for trustworthiness, perhaps using a scale ranging from binding legal identity at one end to anonymous at the other? Who would rank them?

- What are the policies for verification of identities? What liability does the issuer assume? Are better mechanisms needed to establish liability for actions taken in the name of a digital identity?

- What are the requirements for one network to verify and trust an identity issued by another?

- What are the governance issues in the relationship between identity/authentication systems and authorization systems?

- Where should verification of a digital identity occur? Are third parties essential for authentication, or can digital transactions be shaped to limit the role of third parties to the issuance process?

- How does an individual recognize as trustworthy the decision made by his public network to accept a digital identity as valid?

- What are the components for trust in an identity and how are they weighted? To what degree is trust a function of a strong issuance process, or verification of an identity by a recipient or a third party, or the firm assignment of liability for actions?

- What rules and procedures are necessary for an individual in one country to accept a digital identity issued in another? Are common, minimal standards necessary?

- To what extent is government involvement an essential component for trusting an identity? Is existing legislation governing identities sufficient for digital identity management?

- How do networks accommodate multiple identities of varying degrees of trustworthiness possessed by a single individual?

Cooperation

- What would Federation look like on the national and international levels? What are the essential elements of federated identity systems? Is federation the same for private-to-private and public-to-private?

- What are the national level vehicles for providing digital identities? What would a "public/private" partnership for digital identity look like in the U.S.?

- How would international cooperation for digital identities be achieved? Are formal international agreements (like the Vienna Convention that governs passports) necessary. Should a particular multilateral body (like the OECD or ITU) be responsible for developing common approaches?

- Are the rules that work in the U.S. the same as those that would work internationally? What are the national or regional differences that could affect governance of digital identity and authentication?

- How should the rules for identity management be constructed in the larger context of national data privacy rules?

- Will existing rules for cybercrime (like the Council of Europe Cybercrime Convention) need to be adjusted for greater use of digital identities?