Governance and Authentication: Ambiguous Bits and Federated Identity
May 2003

How does a machine know you are who you say you are and what you are allowed to do? A car 'knows' you are authorized to drive it when you insert a metal key. An automatic teller knows who you are and how much is in your account when you insert a magnetic card and enter a Personal Identification Number. The machine isn't actually confirming your identity; it is accepting a token issued to you by someone else, who may have taken steps to confirm at the time of issuance that you are who you say you are.

Identity management and authentication are growing 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.

Identity is a central problem for cyberspace. Digital technologies have introduced new ambiguities into the process of identification by removing an assertion of identity from any context in which we could judge its validity. There are no external clues and no opportunity for the subconscious process of judgment that often accompanies the acceptance 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 public Internet[1] began its dramatic expansion. Now, with numerous large scale, government or transnational commercial identity authentication systems being put in place, the two central issues for public policy are how to manage authentication and digital identification 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, but there is growing interest in coordination. An increase in valuable network applications and the risk of online identity theft is creating consumer demand for better digital identity systems. Governments will issue digital identifiers to their citizens in order to reduce costs and improve the delivery of social services. Banks and large corporations will seek to leverage the 'closed' authentication systems they have created for high value transactions. Individuals will want to manage liability and privacy risks by using a range of digital identities that mirror the options available to them offline. These forces will drive the deployment of three classes of authentication systems:

- High-end, closed systems, based on paper contracts that allocate liability and

[1] For the sake of simplicity, this paper will use the term Internet for both the business, government, and education computer networks that comprise the Internet as well as smaller internets that are not connected to the Internet.

which, given their cost, will be used for high value transactions.

- "Open" Consumer-level systems where parties to a transaction may not be previous known to each other and must rely on digital credentials.

- Government-issued digital identifiers used for authentication in the delivery of social services and for the identification of vendors and agency personnel and, possibly, for commercial services.

Each class has unique features, but they also have many common elements. This commonality provides a basis for interoperability, but without cooperative effort between governments and companies, authentication systems will be largely incompatible. Avoiding this does not require central control or extensive regulation. What it does require are processes and rules that let the private and public sectors work together on authentication.

Background

The expansion and commercialization of the Internet, an open, geographically dispersed system, changed the nature of computer networks and created new problems for governance. Security, privacy, and trust were an assumed part of the smaller, government-run network populated by universities, government agencies and research networks. Infrastructure and rules were designed to maximize information sharing among networks and users. The nature of much of the activity on this early Internet– essentially the open exchange of information, subject to peer review among a community of researchers with no commercial transactions and few automated services - also required a lesser degree of trust and security. Misrepresentation offered little benefit and held inherent risks and penalties. Privatization and commercialization changed this by adding millions of anonymous users and by introducing a broad range of commercial services to the Internet. The change to a quasi-anonymous commercial network created a new set of problems revolving around trust and security.

Early assumptions that a secure public network for communications and business would emerge naturally as a result of market forces were optimistic. The Internet is a collection of networks whose technical standards aim at compatibility among diverse systems. Data integrity, security and authentication were initially secondary issues. The Internet environment remains one of rapid growth and diverse, evolving technologies. The result is a network of unsecured systems that do not uniformly or predictably provide integrity and nonrepudiation, confidentiality, and authentication for transactions. The effect is to seriously impede the further development of the Internet as a new way to organize economic activities. A recent study estimated that $15 billion worth of business-to-consumer and business-to-business e-commerce transactions are unrealized because of concerns over trust.

This problem will only grow more complex as ubiquitous computing and expanded Internet activity become normal elements of business and private life, and as nations take

different approaches to regulating internet activities. The drivers of this new digital environment for consumers and firms will be embedded network, wireless connectivity and autonomous software agents. Processing power and memory will be abundant resources in the near future. Computer and Internet access will, in a few years, be like the electrical grid: cheap, readily accessible, and integral to daily life. Wireless connections to this computing grid will make Internet-enabled devices sophisticated, interconnected and ubiquitous.

With the right framework of rules, new software applications will take advantage of these ubiquitous computing resources and automate many routine activities (allowing machine to talk to machine without human interaction). These applications could allow for computer control of devices and appliances or authorization of commercial transactions through the Internet, using mobile, wireless devices (like laptops and PDAs) and through anonymous public access points that will allow use of the Internet much the way that public phones allow access to the telephone networks. Autonomous software agents could automate a new range of routine activities, to control inventory, negotiate contracts and prices between suppliers and customers for purchases, and arrange for shipping and delivery without human intervention.

Trust (in this case, authentication of identity) has become a function of exchanges between persons and machines or exchanges between machines (without human involvement). Interactions are rapid and automatic, executed according to a series of pre-programmed rules whose composition and nature may not be accessible to the user. We have examples of this available now – gas pumps and fast food outlets automatically accept passkeys for payment and bill specified accounts, implicitly accepting that the person holding the key is authorized to make the transaction.

The need for automatic authentication of identity and authorization will increase as wireless applications proliferate and as people become increasingly sophisticated in using network enabled services. Standards like 802.11 and Bluetooth already allow devices to link wirelessly to computer networks. New applications will take advantage of this wireless connectivity to let people use the Internet to remotely or automatically authorize actions. Using the Internet for authorization instead of special purpose devices simplifies applications and lets a greater number of appliances and applications authorize more activities at greater speed and range. Wireless connectivity and cellular networks will offer new applications and services that are cheaper and more convenient and will let individuals remotely authorize new sets of transactions – such as remote management of houses and other property, mobile authorizations for purchases, or delivery of specialized services and data. Price advantages and market forces will drive applications and networks in this direction.

Ubiquitous computing and wireless connectivity to the Internet will place an increasing burden on mechanisms for authenticating identity and the authorities associated with that identity. Currently, digital identity can involve a profusion of telephone numbers, PINs, accounts, Internet connections with multiple user-names and passwords; legal identities associated with government issued documents and. The result is multiple, incompatible

sets of rules that govern issuance and the use of identities.

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.

In one scenario, a single smart card with strong biometric identifiers could serve as a driver's license, passport, credit card and Internet access enabler. The University of Pennsylvania already issues its students a 'smart' ID that authorizes network and building access and which can be used in local stores and restaurants. Alternatively, a single, firmly linked legal identity could be established and shared by a number of devices – smart cards, cell-phones, PDAs, for authentication and authorization. Alternatively, individuals could use a matrix of identities, some robustly linked and binding and others offering more anonymity or a reduced authority that they could draw upon for differing kinds of transactions.

The implication of a lack of trust is that Internet use and the provision of services will be slowed and made more complicated, imposing real economic and social costs. The events of September 11 give the issue added importance for security. "Trusted" networks are an essential element of cyber security and critical infrastructure protection. The ability to reject traffic from "untrusted" sources (i.e., those without certificates or not otherwise properly authenticated) would improve cyber security and critical infrastructure protection. Information technologies, combined with biometrics, could be used to create a national or even international identity system for use both on the Internet and in daily activities. Increasing the level of trust is not technologically infeasible, but the technologies required to increase it can create serious political and policy problems. A lack of compatible rules for how identities would be established and authenticated and how they would interact and enable would create confusion and increase the potential for balkanization of the Internet.

Managing Identity on the Internet

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.

A failure to improve identity management would reduce the benefits of a global computer network for commerce and public activity. These benefits are so great that it was once thought that market forces would result in improvement, but we can no longer assume that the market alone will rapidly or smoothly resolve authentication problems. Better systems for identity authentication and authorization may not emerge if governance is not adjusted to allow their use or if demand for them remains low. A number of factors could depress demand for authentication below the point necessary for widespread adoption, in particular risk (especially risks associated with third parties) and pricing (in light of viable, albeit limited, alternatives for managing identity).

Despite progress in digital signatures and the provision of certificate services, many larger network users still rely on signed, written contracts as the basis for trust. Contracts, which spell out the responsibilities of each party, create a private basis for trust in business, but this solution is not scaleable, is overly expensive for many transactions and reduces the benefits of autonomous agents and public networks.

Authentication mechanisms are necessary for a thriving networked economy, but their development and implementation raise important concerns for individual privacy and system security. The core issue is that the third party will not adequately protect identifier information from misuse, or that the third party service provider will itself misuse information – not authentication information per se, but information provided as part of the identification process or generated by the client's activities on the internet. To strengthen trust, multiple parties will have to act in a coordinated way. Third parties can overcome some of these concerns if there are strong procedures for their activities. This can be accomplished through regulation and oversight, either by government agencies or through some self-regulatory process. Both public and private solutions have strengths and weaknesses in managing authentication and identity. Improving identity and authentication on the Internet, and ultimately security, requires addressing these problems.

Governance, the ability to determine policies and set rules, has not been one of the Internet's strong points as it has developed. Governance issues, like the management of identity, have become an obstacle to growth, and a source of risk for public safety. Providing the architecture and rules for persistent, unambiguous authentication of identity is one of the challenges that must be addressed for further progress.

Public Key Infrastructure and Digital Signature

In the 1990s, many governments focused their efforts on creating public key infrastructures and building the legal framework for digital signatures. Neither digital signatures nor PKI have been as widely adopted as was expected. Unresolved risk and liability issues, privacy concerns, cost and a lack of related applications have limited their use. Digital signatures offered little advantage over paper processes. A recent survey of German internet users found that only five percent availed themselves of digital signatures even though Germany's digital signature laws is one of the most complete and has been energetically pushed by the Federal Government.

PKI systems for closed systems have had greater success. Closed systems (such as internal company networks) are better able to manage the risks associated with enrollment or revocation of credentials. In addition, government PKI pilot programs in the U.S, Canada, Europe and Asia persevered. These programs form the basis for a renaissance of sorts for PKI. Wide-scale deployment of PKI systems for authentication has begun and many governments are adopting PKI systems for the online delivery of social services or for government purchases. The United States, Canada, Singapore and Hong Kong have or are developing programs using PKI for e-government activities.

The result is that within a few years millions of individuals in OECD countries will have government-issued digital identifiers. Many individuals will have multiple digital identifiers issued by different organizations, each with their own trail of transaction histories. These will include digital identifiers issued by governments as well as identifiers issued by service providers, employers or financial institutions.

Authentication and Government-Issued Digital Credentials

Government issued documents are the starting point for verifiable identities. In economically advanced countries, you are born, your parents name you, and the State records your birth and enrolls you in its social services. Over time, your attendance at school is recorded, you purchase services and engage in financial transactions and, in many countries, and you are issued a photo identity document. When you assert your identity, you need to use these government-issued credentials and, for high value or high-risk transactions, the government identifiers will be checked against records of your transactions. The result is either credentials or transaction histories can confirm identity.

Other credentials (passports, drivers licenses, credit cards, incorporation for business entities) rely on birth certificates and social service identification numbers. Over time,

these credentials are reinforced by the history of transactions associated with them (school records, records of purchases from public utilities networks, addresses, bank accounts). They will also be the starting point to generate credentials or tokens of various kinds (smart cards, certificates, etc) that will provide digital identity. Digital identities and credentials will be derived from government issued identifiers and transaction histories.

These government-issued documents grow from processes not originally designed to confirm identity. The birth certificate grows out of the practice of registering births. Governments have collected vital statistics since the 16th century, to gain an idea of the size of their populations (and therefore of national strength). Governments did not issue driver's licenses to prove identity but to show that the holder had passed a government test of his or her driving ability. The U.S. never intended the Social Security Number to serve as an identifier. Providing identity is a secondary purpose, but despite their drawbacks, government-issued identity documents command a higher degree of trust than any commercially issued identity document.

Passports are an important example of this greater trust. Passports were the first of the widely issued government-issued identity documents. They came into widespread use at the end of the First World War to allow governments to identify non-citizens who could pose a security risk. Some governments, like the UK, are now considering how to duplicate the passport issuance process as the best way to issue digital credentials. Others countries, like Italy or Finland, have made digital credentials an integral part of national identity documents that are replacing passports in Europe. The passport issuance process may be the useful model for future government-issued credentials.

Almost one hundred countries, including Germany, France, Belgium, Greece, Portugal and Spain have compulsory national identity cards. Other developed countries with different legal traditions, including the United States, Canada, New Zealand, Australia, Ireland, and the Nordic countries, do not have national identity cards. Sweden does not issue cards but provides each citizen with a national number. Most industrial countries that do not have a national identity card have issued their residents health or social security card and the use of special- purpose cards for the provision of social services is common.

Translating existing governmental credential issuance processes into digital form and creating a structure of rules that will allow an identity issued by one government or commercial authentication system to be accepted by others will require a cooperative effort between countries. Governments and the private sector will need to consider how to use existing identity processes for digital identity.

Governments around the world are attracted to the online delivery of services because of the lower cost and potential for improved performance. Authentication of identity is the key to online delivery of services. This makes authentication a central element of e-government. Government-issued digital credentials will join other identity documents, like driver's licenses or social security numbers, which have become essential for private

activities. A new class of digital credentials created by government face challenges that are common to all authentication systems but also challenges that are unique to government systems, particularly on the issue of whether a government credential will be used for private purposes.

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

Deciding if and how to accommodate private use is a central issue that will shape government issued credentials. An official use only system could be easier to manage, but a decision to allow private use would increase cyber security and promote e-commerce and better authentication. It is easy to imaging, for example, software that would not accept e-mail which was unaccompanied by a verifiable digital credential or which would flag uncredentialed emails for special treatment. This would immediately reshape the spam problem and would reduce the incidence of certain kinds of worms, viruses and other cyber attacks. Providing robust digital credentials could create social value far beyond the benefits of e-government.

There is a real opportunity cost to societies if they choose to limit the use of government credentials, but at the same time, a number of difficult corollary issues flow from a positive decision. These include deciding how private parties will access public systems for credential verification and to obtain revocation information, how the service will be funded (there are ongoing charges present with digital credentials not found with paper credentials) and how what will inevitably be a joint public/private enterprise will be managed.

Government credentials are accorded a higher level of trust, whether they deserve it or not. A poll in 1999 found that two thirds of Americans would be willing to appear in person, as they do for driver's licenses, to obtain a government-issued digital identifier. Even though the processes for issuing them are often flawed and easily subverted, most users assign a high degree of trust to government credentials. The percentage of false credentials out of the total population of Social Security Numbers and driver's licenses is very small, leading to a perception that they and the processes used to issue them are trustworthy. Users do not assign the same level of trust to credentials issued by private vendors.

The precedent in identification developed over several decades is for businesses to

piggyback on a government-issued identifier and use it for commercial purposes. In the U.S., social security numbers and drivers' licenses have become general-purpose identifiers while national identity cards serve a similar purpose in other nations. Despite weaknesses in the issuance process, the drivers license remains more widely accepted and is accorded a greater degree of trust than any commercially issued identifier

Government-issued digital identifiers will probably be adopted in a similar fashion for commercial and private purposes. This would continue the precedent found with social security numbers and driver's licenses in the U.S. It is also possibly that commercial identity services could link their credentials to the government issued digital identity (i.e. a separate identity token or credential that can be verified by reference to the government-issued identifier). The government issued digital identifier could become a kind of root identifier upon which to base other authentication systems. Governments could accede to the use of their identifiers for commercial purposes but not participate in any online verification system.

Some governments have acceded (or planned) for this and intend or expect that their digital credentials will be used for commercial purposes. Often, these are governments that already issue national identity cards or other national identifiers to their citizens. In some cases, such as Italy, the government credential has met with mixed success. In other countries, such as Korea, government credentials for the Internet are widely used.

Digital credentials are essentially a new kind of public service. The value of this new service will depend on how broadly governments acceded to private and commercial use. The process of verification and revocation means that governments will face a new set of expenses in creating and maintaining the databases that support authentication activities. Private use of the government credentials will increase the load and the resource requirements for a system by expanding the number of requests that government computer systems will need to service.

Governments could provide this service without charge, as agencies will need to operate and maintain authentication systems for their own purposes. Another option would be to offer citizens the option of paying a single fee at the time they receive their digital credential if they want it enabled for private use. A third approach would be to charge a small fee each time there is a transaction using the digital credential that accesses government systems. Presumably, if the system is not mandatory for accessing services, there will be no charge for using the digital credential to access government services (at least for consumers) since many people would choose not to use them.

Credit cards offer a model of a transaction based fee structure. Each time the card is used, a fee is charged by the system operators to fund operations and to provide a profit. If governments chose to adopt a similar approach, they would need to consider whether they would d need legislative authority to charge a new fee. Whether to allow the use of government-issued digital credential for private purposes on a no-fee basis or as a paid service is a major policy issue that will grow in time as the use of credentials in e-government expands.

Outsourcing some government authentication activities could solve some of the resource and management problems. Almost all governments are unwilling to allow private parties to issue identity credentials. Agencies may be uncomfortable with the increased risk of fraud such outsourcing may entail. However, other activities, such as managing the verification/revocation process, could potentially be outsourced. Governments could pay firms to provide these authentication services, or they could allow companies to bid on providing authentication service and charge fee for private transactions, making the private use of government credential serve to partially subsidize public authentication needs. Governments could also allow commercial authentication systems to add management of government credentials to the commercial 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.

Allowing the private use of government credentials would require a decision as to how the mixed public/private system would be managed. Management could be provided by governments alone (through law or regulation), or it could be done cooperatively with private partners. Management could be limited to a single country or it could involve cooperation with other countries. No single approach will work for all activities. For some issues, government or national processes alone will be sufficient, but for others, a larger framework will be required. Developing this framework for governance is one of the principle challenges for the widespread and effective use of authentication systems.

Government-issued digital identifiers may face an extra burden in that if they become the digital identifier upon which others are based, their issuance process will need to be particularly robust. The current processes used in the U.S. for issuing drivers licenses or social security numbers is not be sufficient for digital purposes, given the higher potential scope for fraud using a false digital credential. One element for consideration by government systems will be whether to seek legislation or other remedies to improve the issuance of core identity documents (birth certificates, social security numbers) or the extend to which transaction histories will also be required for the issuance of credentials.

The United Kingdom considered adapting the same process used to issue passports as a means to issue digital credential for access social services. The UK, like the United States, does not have a national identity card (although it has proposed issuing an entitlement card that could provide digital authentication). Other nations that already issue their citizens a national identity document have been able to piggyback the issuance of digital credentials on this process. The issuance process will not be problem for digital credential issued to government employees, but credentials issued to citizens will require greater scrutiny. The passport issuance process could provide a model for enrollment and issuance of digital identifiers.

The passport process raises another question for government-issued digital credentials. Over time, nations have developed a process wherein a country can accept as a legitimate credential (for some purposes, including identification), and with a reasonable

understanding of risk and trustworthiness, passports issued by other nations. Passports do not provide a useful model for dealing with fraud or revocation, but they do raise the question of how one nation will treat a digital credential issued by another.

This problem is small and manageable for digital credentials used for official purposes (say to identify a defense contractor). In those cases, a government agency could reasonably choose to issue its own credential rather than rely on one issued by a foreign government. Other activities pose problems that are more complex. We do not have the experience, processes and framework in place that could allow an entity in one country to trust a digital credential issued in another. This has trade and commercial implications that are very important for online activities. Resolving this issue would have to be on the agenda for discussion in any cooperative management arrangement. As with the decision on whether to allow private and commercial use of digital credentials, governments will need to consider what systems will be to public access, what information they will provide and under what conditions.

Governments will also needed to consider how they will deal with liability issues. A failure to resolve liability issues has been a major obstacle to the widespread use of open, commercial authentication systems. This is a larger problem for authentication that probably requires legislative solutions. Governments traditionally do not assume liability for identity documents they issue, and a system that provides a passive credential could continue this precedent. Liability arises if a credential's assertion of identity is sent back (in some form) to the issuer for verification. Unlike paper credentials, digital credentials, particularly with PKI systems, can require information that is verified by the issuing authority or some other third party.

If use of the credential was limited to official purposes, governments can self-insure against liability risks. However, if government-issued digital credentials are used for private purposes and these credentials require some sort of verification from government sources, liability issues are raised. Revocation also raised liability issues. There could be a presumption of liability if the government revokes a digital credential but does not make this information public and the credential is used for fraudulent purposes.

In the physical world, official assent or action is not required to use a government-issued paper credential -- governments are usually not involved in transactions where a driver's license is used to authenticate an assertion about identity. This is the approach taken for other forms of government issued identification – the government role is only to issue the identifier. It is not clear if this precedent, where governments passively allow a credential they have issued to be used for commercial purposes, can continue in the digital age. One of the causes of identity theft (along with poor enrollment practices) is the failure to manage credentials after issuance. Governments need better processes to ensure that core credentials are not misused. Consumer and government systems may find fraud endemic without some improvement in what governments do after they issue an identifier.

Data protection issues pose special problems for government-issued credentials. This will also require a series of decisions regarding how much and what kind of information to share. Agencies will need to adjust and expand their privacy policies to accommodate authentication. Privacy decision will affect the acceptance of authentication systems. Many users will avoid systems that do not protect personal data. At the same time, personal data provides context for a decision on whether to accept an assertion of identity. Authentication systems that provide no personal data will face hurdles to acceptance. The dilemma with a simple confirmation of a credential is that this does not inspire trust. Third party verification also does not inspire trust unless that third party accepts liability. Trusted 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. Governments will need to balance the amount of information provided in the verification process against the amount of liability they wish to accept.

In theory, little or no personal data is required for authentication using a certificate or token. However, the use of transaction histories, a very robust method for authentication, requires the use of personal data. Authentication by using transaction histories may be necessary to decrease the risk of identity theft. Stronger authentication system might use a combination of databases or directories. A commercial digital credential could be reinforced by being based upon and linked to a government-issued digital credential and by being confirmed through checks against transaction histories. This might be essential for higher value transactions, and mimics the process used by credit card companies.

Cross-referencing of data bases might also be necessary as part of authentication for social services or high value transactions. In the U.S., state drivers license authorities already do this when they check new applicants against other States driver's license databases. Agencies will need to decide if the ability to check vital statistics as part of the confirmation/revocation process. Governments may also need to balance the trade-off between the degree of fraud that can be tolerated and how much authentication processes reduce privacy through the use of personal data.

Elements for Federated Authentication Systems

Multiple authentication systems will be distributed among government agencies, company networks and commercial service providers in many countries. The number of systems will expand and the technologies they use will continue to differ. This heterogeneity masks a high degree of commonality in the tasks that must be performed for authentication to occur. How each system performs these functions will determine in large part the degree of trust that can be assigned to it. For authentication, the processes for enrollment, verification and revocation, privacy and assignment of liability are the elements that will determine trustworthiness and allow for cooperation.

Enrollment

Reducing uncertainty and risk in digital identities will require broadly applicable rules that cover the central elements of authentication: enrollment, verification, revocation,

liability and data privacy. The goal is to provide a means for one authentication system to decide how much to trust another and for users of these systems to trust how these decisions were made. Establishing transparent performance thresholds for these elements against which an identity service's trustworthiness can be measured and communicated is essential for reducing risk and uncertainty and for federation to work.

Enrollment is the process by which an individual person, corporation or device is issued a digital identifier for use on networks. Strong enrollment processes are essential for an effective authentication system, and transparency and commonality in enrollment processes are essential ingredients for interoperability and a federated authentication.

Identity is created in the context of a larger social network. Families name their children and governments record the birth of citizens and issue them with an identifier for social services. These government-issued identities are starting point for credentials and, with their associated transaction histories, will be used for enrollment and issuance of digital identifiers. Four processes used in the United States that 'authenticate' an identity offer perspectives on digital authentication. These are the obtaining a driver's license, passport of credit card and getting a U.S. security clearance for access to national security information. Each of these processes has many areas of commonality and relies in varying degrees on two different processes: the presentation of credentials and a review of the history of transactions associated with those credentials.

Driver's licenses are credentials issued by multiple sources and used for both official and commercial purposes. As States added a photo to the driver's license, it became the de facto response to requests for a photo ID. The driver's license requires a social security number, proof of residence (often through documents showing active accounts with a local utility). These identity documetns are checked at the time of initial issuance of thelicense, usually in a cursory fashion. Some states also check for traffic or parking offenses. The initial issuance requires the applicant to appear in person, although subsequent renewals do not always requires a face-to- face transaction.

Despite requiring renewal at regular intervals, the rate of fraud and error in the issuance of driver's licenses is high. Applicants are issued a token (a plastic card) with their photo (a basic biometric identifier) and other identifying data. Some states are moving to the use of cards with more sophisticated biometric data. Fraud and revocation problems are driving issuers to adopt common standards for enrollment and for credential format.

The credit card issuance process is more robust because, unlike the driver's license, it also authorizes access to a resource: somebody else's money. Opening a credit account requires, minimally, name address and social security number. These data are usually enough for the large commercial credit reference bureaus to perform a review of the creditworthiness of the applicant and, in the process of reviewing the applicant's transaction history, provide some confirmation of identity. Financial institutions are perhaps the only place in the private sector where trust matches that given to government credentials, given their emphasis on building and preserving trust and their acceptance of financial liability.

The credit card process has several facets of interest to digital authenticating. First, the industry has created a system for checking transaction histories as part of the enrollment process. After applicants are approved, they are issued a token (the credit card) that allows them to access the system. The credit card is often used in combination with the photo ID drivers license, providing a rough-and-ready combination that authenticates identity and authorizes access to financial networks and resources. Third, the industry has put in place a revocation process that relies on several different processes to determine whether to revoke access authorization, including sophisticated software that identify suspicious anomalies in use. The system for authorization and revocation is networked and works in real-time, funded by a fee collected on each transaction. There is no renewal process, but active use entails a constant low-level scrutiny for the issuer.

Adopting the audit trail used by credit card could also make authentication more acceptable. If users were notified every month on the use of a credential assigned to them, they could check this against the transactions they had authorized to detect fraud or misuse. This checking function could probably be performed by a software agent, and would reduce uncertainty in the use of credentials.

Passports are widely issued government-issued identity documents used by governments to identify nationality. In most countries, passport issuance requires a personal appearance for initial issuance and the submission of multiple identity documents (birth certificate, photo identification). At one time, British passports contained not only photos and signatures, but also written personal descriptions of the holder, describing the shape of face, features (i.e. size of nose, forehead and eyes) and their complexion. The United States checks the applicant's name against law enforcement databases – not to verify identity or information, but to determine if there is any negative information that would prevent issuance of a passport. At the end of the process, the applicant is issued a document with a long renewal period. Other core identity documents may, despite the expense, need to move to issuance processes similar to those used for passports.

The Federal security clearance process is complex, expensive and time consuming. It confirms identity and uses a hierarchical system of clearance to authorize access. It relies on face-to-face interviews, submission by the applicant of an extensive transaction and activity history, verification of an applicant's history by investigators, and the review of an applicant against Federal databases, including the collection of fingerprints for review against criminal databases. Renewal requires resubmission of transaction histories and further checking. The process takes months to complete, costs thousands of dollars and uses real investigators but it has very low rate of fraud. No credential is issued at the end of the clearance process. After being cleared, an applicant supplies name, social security number and date of birth to obtain access to classified material. This information is referred to the issuing agency for verification before access is allowed. The lack of a token and the verification process reduces the chances of fraud.

The common elements in these enrollment schema are that they are based on government issued identity documents and use historical data to verify the link between the individual

asserting an identity and those documents. The more sources of verification used, the more reliable the verification. The best of these systems also use in-person applications, where context and behavior can provide additional information to determine the veracity of an identity assertion. Devices[2] and companies will also depend on these government-issued identity documents, as they will be issued digital identifiers on behalf of a person.

Given the dependence of digital credential on government-issued identity documents that form the 'root' of digital identity, the strength of the processes for issuing these government identifiers is an element of risk for digital authentication. Weak processes at the start create the opportunity for fraud and misuse in cyberspace. Canada, for example, found that although only 25 million Canadians qualify for a Social Insurance Number, it issued 28 million of them. For closed authentication systems developed for high value financial or commercial transactions that rely on contractual arrangements and existing financial relationship, this will not be a problem. Since government issued credentials will provide the foundation for commercial consumer authentication systems (and possibly government systems) countries will not be able to tolerate the current error rate in issuance for social security numbers and driver's licenses.

Enrollment processes will also have to be transparent to other users and meet common standards or criteria to build trust. Ignorance of the basis for issuing a credential devalues the credential itself. Knowing that a credential has been issued only after a known set of requirements had been met would reduce uncertainty. A trustworthy system might use XML to embed in a credential the record of the identity documents used in the enrollment process. This would provide additional information and context for recipients (or perhaps software agents acting in their behalf) to assess trustworthiness. For example, inspection of a credential provider's website might show that a driver's license and credit card are required for enrollment, but a user could better assess trustworthiness if detailed information about the specific documents used for enrollment are embedded in the credential. Use of XML software could help restore context to digital identifiers.

One immediate requirement for enrollment created by the needs of digital authentication is that there will be increasing pressure for governments to improve the processes they use to issue core identity documents, such as birth certificates, social service numbers or identity cards. These government-issued identifiers form the basis for establishing identity. Many governments did not intend for birth certificates, social service numbers or driver's licenses to act as credentials, but as the number of transactions among strangers has increased, these documents have been pressed into service as credentials. Improving the issuance and revocation processes for these paper credentials is essential for avoiding large-scale errors and fraud as digital authentication proceeds.

Verification and Revocation

[2] Devices are embedded microprocessors or software agents that are capable of engaging in network 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 devices legal identity or on a legal identity derived from a person or firm.

Verification is the process, at the initiation of a transaction, when the digital identifier is itself checked and authenticated. In an ideal system, this would happen automatically and transparently according to pre-designated criteria selected by the recipient. Verification techniques used for physical credentials, such as driver's licenses or passports, are of little use for digital authentication. Despite efforts to create tamper-proof documents that cannot be forged, fraudulent credentials are relatively common. The most effective response has been for issuers to develop networks of cooperation that allow them to evaluate and verify a credential issued by another.

Verification will be essential for online transactions as identification and authorization are inextricably linked. Passports or drivers licenses can be visually inspected, can be examined in the context of a set of visual and aural cues. Digital credentials offer none of this. While encryption technologies may allow us to feel confident that there has been no tampering with a digital credential, authentication among different systems will require an external verification process in lieu of physical inspection. Networks offer the ability for a party or data that is independent of the transaction to verify digital credentials.

An external reference could take several forms. A recipient of a digital identifier could go to the issuer to verify it. Alternatively, the recipient could maintain a list of trustworthy issuers (based on the understanding of the adequacy of their issuance process and the ability of the digital identifier to resist tampering or fraud), whose credential would always be accepted if it appears to be in good order. A third party could provide external verification using data provided by an accepted list of issuers.

Several techniques can verify assertions of identity. Simple assertion is one and its acceptance depends greatly on context. Someone asserting an identity can supply documentary evidence to verify the assertion. A third-party can corroborate an identity or a person can cite existing relationships. Biometric data can establish identity when that data has been previously collected and assigned to an existing identity (although a biometric identifier is only as good as the network it is attached to and the enrollment process that generated it). Finally, identity can be established if there is a shared secret, a piece of data known only to the asserter and the recipient.

Verification of a credential or token[3] places great stress on the issuance and enrollment process and on the security of the credential or token after issuance. Authentication systems need some visible means to manage these risks if credentials are to be widely accepted. High value systems manage risk through contractual assignment of liability. Contracts spell out the responsibilities of each party and create a private basis for trust, but contracts are not a scaleable solution, are too expensive for many transactions and limit the use of autonomous agents or public networks. Drawing from the experience of the credit card industry, future systems might want to take advantage of network technologies to use other techniques. These techniques are to use network capabilities to check multiple sources and histories.

[3] A token is a physical representation that stores the credentials used to provide digital identity. These can include smart cards, biometrics or stored software (certificates).

Verification should reflect the strength and speed of information technology in using networks, in processing capabilities and in searching databases. As with other processes, the goal should be to digitize and automate routine processes, deepen them and move human intervention to the high end. The goal of verification should be to put a digital identifier into context. The lack of context – the visual and aural cues used to identify people in face-to-face encounters or the history of previous transactions that can document an assertion about identity, is a large problem for authentication (as it is for much of the information on the Internet). Networks, databases and processing power can supply context for digital identities.

The credit card industry has developed techniques that use sophisticated algorithms to automatically compare a proposed transaction to the history of transactions associated with an account. If there is an anomaly, the transaction may be halted and the account given greater scrutiny. The process is expensive, but some elements (use of networks to connect to algorithms and databases to detect anomalies in use) could be adapted for authentication. At a minimum, it could flag for a recipient if there is an unusual use of the digital identifier or the number of times the digital identifier has been used successfully n the past. E-bay does this now in a basic form when it shows how many successful transactions are associated with a seller or purchaser's account.

Authentication processes can also take greater advantage of network capabilities to check multiple sources simultaneously, duplicating, in effect, an element of the better enrollment processes. Authentication processes will be more trustworthy if systems provide the option of going to multiple databases or directories to verify the authenticity of a digital identifier they are being presented.

For government systems, one key issue will be the question of access to databases and directories for verification purposes. Nations will need to decide if they will allow commercial identity service providers to access the directories that support government-issued digital identifiers. This could be especially sensitive for the question of whether to allow foreign entities access. Privacy will pose special challenges since national attitudes and protections vary widely. Open authentication systems that can operate across border will require explicit understandings on how to treat private data.

It is not clear whether government issued digital identifiers will become the online equivalent of the national identity card or driver's license – de facto lynch pins for identity – but there will be pressure to do this. Governments never intended the driver's license to be an identity credential, but demand from consumers and merchants moved it into that role. A similar process could occur for digital identifiers, and efforts to resist or limit this might actually discourage adoption of government authentication systems. Commercial digital identifiers could, for example contain a reference that would link back the digital identifier issued by government agencies for social services. They would not use the government identifier but would be able to check an assertion against it, much as the driver's license is used to check assertions about identity off-line.

Revocation

Even without fraud, there will be many instances when issuers will need to revoke a digital identifier. Companies may go out of business, devices may be sold to a new owner, persons may retire to a monastery or die, and in all cases the owner of a digital identifier may change accounts with a service provider. For these reasons alone, a federated authentication system will need to manage digital identities to be able to revoke them when they are no longer valid. The potential for fraud also requires that revocation processes operate simultaneously with online verification as a transaction is initiated. Verification and revocation are linked, and will be able to use the same resources and processes. The chief difference between the two is that data used for revocation will need to be updated more frequently than verification data. When an entity is issued a digital certificate, it is good for a specified period and no further updating of the information is required. In contrast, revocation data will need to be updated continuously.

DNS router tables and credit card systems offer two automated and on-line precedents for revocation of digital identifiers. DNS tables operate in a hierarchical environment and verify each level of an Internet address according to established protocols. Routers maintain lists of valid Internet addresses needed to forward messages on to their final destination. These lists are updated daily when the router requests information from the next level in the hierarchy, culminating in the thirteen root servers that provide the basis of the Internet addressing system. Each router asks the one above it if the DNS data it is using is still correct. Changes in the address databases are made by a large number of organizations for the addresses for which they are responsible. Frequently used addresses are stored to speed processing. The system is transparent to users and transactions fail when the naming information is no longer valid (the DNS system, managed by the international organization ICANN, also has implications for the management and governance of a federated authentication system that will be discussed below).

Credit cards, unsurprisingly, have a very effective system for revocation. It is networked, so that thousands of individual recipients (in this case, merchants) in card system have access to it. It operates in real time, not to verify the identity of the person presenting the card but to verify that they are authorized to carry out the transaction. It is automatic and can be triggered by preset limits, algorithms for identifying suspicious transactions or by inputs from system managers. No personal data is shared with the merchant other than that the presenting account is authorized to carry out the transaction. Transaction fees charged to the users cover the expenses of the system (the credit card system also has implications for the management and governance of a federated authentication system that will be discussed below).

One implication of these systems for authentication is that governments will need to develop processes for revocation of the digital identifiers they create and, that they will need some way to share revocation data with the private sector in a timely and accurate fashion. This is not something governments have done before.

Privacy

Authentication raises critical privacy issues. Privacy is a major concern for Internet users and authentication and digital identity cannot be separated from the larger debate over online privacy. The fundamental issues are control of personal information used for enrollment and verification and the tracking of online activities. Enrollment and verification will use large databases controlled by third parties containing important personal information. This data will be used to issue credentials and to confirm identity. Unauthorized access to these databases would pose a real threat to privacy and could allow for identity theft on a gargantuan scale. Erroneous entries could damage reputations or deny opportunities. Similarly, misappropriation of a digital credential could allow an imposter to engage in transactions with another's identity. Some authentication techniques, such as those that rely on a shared secret or a token will not pose the same kind of risk for personal information but still face the problem of tracking online activities.

Authentication technologies provide a link between persons and their online activities. Current protocols assign computers and other devices on the Internet with a unique address (some are permanent and some last only for the duration of the connection). Every transaction on the Internet leaves a record of the requesting computer's Internet address -- for example, when a Web page is requested, the recipient site can log the address of the requesting computer and the nature of its request. However, this address identifies the computer, not the person using it. Widely deployed authentication systems could change this. If sites refused access to those who did not authenticate their identity, the visitors' actions could be logged against their real identities.

Each level of authentication will have different privacy concerns. For the high-value commercial system, personal details are less likely to be a part of a transaction. Protection of intellectual property and financial data will be more important. To preserve the confidentiality of this data, high value systems will develop safeguards and assign liability for loss. The concerns for consumer level systems are (a) absent privacy safeguards perceived to be effective, people may make less use of a system; (b) the databases containing the information used to enroll or verify a digital identifier will hold personal information susceptible to misuse; and (c) weak enrollment or verification processes could greatly increase the possibility of identity theft using the new digital identifiers.

Government authentication systems face a much more serious challenge. Since governments will use digital identifiers to authenticate transactions for the secure delivery of services or for taxation, these transactions will necessarily involve a very high level of personal information on health, finances, employment or education. Fraudulent transactions, where one person posed as another, could be very damaging.

Assignment of identities to devices creates another set of privacy problems. Authentication of a device will link back to a personal or corporate identity and will likely involve authorizations (i.e. what transactions the device is authorized to undertake).

The device will essentially be a representative of the person who authorized it to act. Devices will have two sets of privacy issue: first, that the record of transactions the device has undertaken is also protected and second, that the personal data of the entity they link back to is protected. Devices will need a strong link to their owner for purposes of liability but at the same time minimize release of that owner's sensitive personal data.

A federated system would also need to comply with the various privacy regulations of the countries or regions in which it would operate. Differing preferences for regulation among nations probably also means that the degree of government involvement in authentication systems will differ.

One protection for privacy that will need to be a fundamental part of open, interoperable authentication systems is the need to continue to allow for anonymous or pseudonymous transactions. Creating strong online identification will change the behavior of people on the Internet, and absent a continued capability for anonymous or pseudonymous action, users will either find ways to evade authentication requirements or opt out of transactions. There is some evidence that suggests that a significant percentage of Internet users will opt out of online applications if they are required to positively identify themselves. A requirement for positive identification in all circumstances would reduce the scope for freedom of expression on the Internet, and would create a new set of privacy problems. Consumers and smaller commercial entities will opt out of an authentication system if they think a side effect is to damage the privacy of their personal data – both the identifying data used for verification and data that could be collected when they conduct online transactions in an authenticated mode.

A federated model could consider a mix of policies and technologies to limit risks to privacy. 'Blind issuance' or 'selective revelation' technologies can minimize the amount of personal data required to confirm a transaction. Privacy risks would be reduced if verification processes do not use personal data, but instead only confirm that a credential was issued through a trustworthy process. Data labeling techniques could enable a system where privacy rules were articulated and applied to authentication and verification processes. Finally, auditing technologies that track both verification requests and the use of digital credentials may need to be an essential element of federated authentication. Automatically reporting back to issuers and holders of a credential on its use and on compliance with privacy requirements would reduce the risks of digital identities –online banking systems that tell you how many log-on attempts there have been since you last used the system are a basic example of this.

Open, interoperable authentication will not work if privacy safeguards are not a central part. Governments will need to meet legal requirements to safeguard information provided by their citizens and, in some cases, by citizens of other governments if they access foreign databases. The problem is compounded by differences between the U.S., where privacy standards are very low for commercial activities, and Europe, where privacy requirements for commercial activities are at least nominally more robust.

Liability

Assignment of liability will be a crucial determinant for both the success of individual authentication systems and for any federated approach to authentication. Deciding who is liable for the damage caused by for fraud and misuse is one of the largest components of risk and uncertainty for digital identity systems. Liability for digital identifiers is much greater than that of paper identifiers because the scope for fraud or misuse is immensely expanded. This includes not only fraudulent representation in a transaction (similar to the risks with analog credentials), but the risk that a digital identifier will be captured and used in other transactions that are unknown to the legitimate owner. Use of digital identifiers will be greatly reduced in circumstance where people are unclear about the amount of liability they are taking on in a transaction. Absent measures addressing liability, demand for online authentication will be significantly reduced.

There are a number of ways to reduce liability risks. Paper contracts between the parties using the authentication system reduce risk. Most firms using authentication systems today rely on contracts – an anomaly in that the digital system can only be enabled by a paper process. Before any digital transactions take place, the parties have accepted a binding legal commitment (usually a document) that allocates liability. These systems are closed in the sense that only those who have accepted such documents can participate. The binding legal commitment can be between the two parties involved in the transaction or can involve a third party, such as a financial institution.

A second approach would be to use the development of case law to assign liability and risk. In the event of fraud or misuse, the victims would take their case to the courts and over time, a body of legal decisions would establish the parameters of liability. A reliance on court decisions has serious drawbacks. Waiting for the courts to assign liability through case law will greatly delay and limit the adoption of any authentication system. Cases will be few because few people will use such systems until liability risks are reduced.

A third approach is for legislation to allocate liability and risk. Previous legislation did not adequately allocate liability and risk, which greatly reduced demand for authentication services. Resolving the liability problem for authentication may require a blend of practices already in commercial use. Liability will need to be assigned (and limited) for both consumers and service providers. For consumer-level systems, provisions similar to those that apply to credit cards (in the U.S. Federal legislation limits consumers liability to $50 dollars) will be necessary to manage risk and uncertainty 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, will be necessary.

These two practices will establish the ceiling for financial risk and liability in authentication. The likely result will be that people will be unwilling to use the open system for transactions whose value is greater than the legally established liability thresholds. Higher value transactions will be ‘bumped up’ to the closed system. Creating

a floor and a ceiling for liability will limit the kinds transactions that use open authentication systems, but is will also enable 'open' authentication systems where there is no previous binding legal commitment among parties to a transaction.

Government-issued digital identifiers could pose a more complicated problem. Although some agencies (at least in the US) may limit the use of these identifiers to transaction with the government (and to the specific agency), it is also likely that once government issued digital identifiers become common, their use will spill over into commercial transactions. Some governments, like Korea, go so far as to require use of a government-issued digital identifier for some online transactions (such as stock trading) and others may follow suit as more systems are deployed.

Governments do not assume liability for misuse of the identity documents they issue (although misuse is usually a crime). Damages from fraudulent use of an SSN or drivers license cannot be recovered from the issuing agency. The same will likely occur with government issued digital identifiers. One possible outcome, given the higher degree of trust likely to be placed in government-issued digital identifiers, is that some transactions will require use of both a government identifier and a commercial identifier. A dual credential process would add an additional source for verification to the liability protections associated with the consumer identifier.

Increasing the scope for interoperability and cooperation

These common elements - enrollment, verification and revocation, privacy and liability - provide a starting point for building cooperation among authentication systems. Cooperation will become increasingly important as the number of authentication systems increase. A lack of cooperation and interoperability increases risks to users and reduces the efficiency of digital networks.

The lack of interoperability is not the result of technological problems. It results from the lack of structure and rules. Heterogeneous technologies can work together when the rules for this are defined (as the Internet itself demonstrates). The Internet allows thousands of different computer systems to interact seamlessly in transferring data and code among themselves. The key to this is the use of a common set of protocols that lie between a computer system and the rest of the network. However, the tasks of these protocols and the management of this communications system are less complex than the tasks for authentication. The issues of trust involved in authentication cannot be resolved by technology or protocols alone.

While there are technologies that can form a unified authentication system, there is no underlying structure of rules and policies that would allow authentication systems to work together. Concerns about risk, liability and privacy and the plethora of credential issuers work against this. Single logons will be attractive for some sets of applications, but users are likely to want multiple logons as a way to manage risk. Global identity or

credential directories using protocols such as LDAP[4] may emerge as commercial or public services, but these would also face requirements for comparable and transparent processes in enrollment, verification, privacy and liability. To build this structure of rules and policies, parties will need to agree on minimal requirements for trustworthy digital identities. The task is to identify the processes, participants and vehicles needed to build a cooperative framework for authentication.

The spread of private and public sector authentication and identity systems has created a new opportunity to harmonize practices and promote interoperability. However, cooperation in authentication faces several problems that are unique to networks. Market forces alone will not generate a solution. Effective governance for authentication will require some combination of private and governmental approaches.

Taking advantage of this opportunity will require a new approach to governing the Internet. Early thinking about Internet policy gave considerable weight to the idea that market forces would lead naturally to the deployment of trustworthy public networks, just as market forces had created the exponential growth of the Internet. Understanding why this did not occur is important for thinking how to shape future efforts. The most important of these include a mis-understanding of the role of government in building trust and for establishing identity, underestimating the limits of contract law, and an over-reliance on digital technologies in place of the multiple credentials and transaction histories normally used to establish identity.

Self-regulation has many advantages for distributed, nonhierarchical networks. At the same time, it can imply lack of oversight, transparency and consensus. This is a particular problem for the Internet, where many of the rules that govern it are embedded in software and are not accessible to most participants. To be widely accepted as trustworthy, authentication systems will need to be transparent and accountable and be seen as 'legitimate.' When governance structures are not seen as legitimate, they face debilitating political problems even if they provide effective solutions to policy issues. Accountability in authentication would mean that the costs of negligence or fraud would not always be borne by recipients. Accountability might also make it necessary to create some sort of ongoing management entity for authentication governance. Cooperative systems also need to specify the rights of participants. For individuals, the primary concern is the right to correct errors. For systems, the concern is how they participate in the process of decision-making and their right to make changes in the rules.

A cooperative structure for authentication would need to make transparent what systems and individuals must do to participate. This requires common understandings about what is required to enroll an individual and issue them a digital credential; how one authentication system will let others know when a credential is valid and when it has been revoked. Other systems will need to understand the degree of liability assumed by the issuing system for error or fraud. The degree of privacy protection afforded will need

[4] Lightweight Directory Access Protocol allows users to locate organizations, individuals, or other resources on a network.

to be explicit.

Digital outcomes are not innately trustworthy, given the lack of context, ease of counterfeiting, et cetera. Systems must know what other systems are doing, in order to judge risk and trust. The emphasis is on transparency in processes (how an outcome is achieved rather than on the outcome itself). Use of a common technology, such as PKI, provides a degree of transparency, but in itself, a common technology is not enough as common technologies do not to provide the same answers to those questions usually ascribed to "policy." Assertions that an outcome is good must be accompanied by transparency about how that outcome was achieved, so that other systems can make independent judgments.

The delinking of physical jurisdiction and governance also makes building cooperation more complicated. A cooperative framework for authentication will shaped by the larger policy debate on sovereignty and cyber space. Sovereignty is the largest obstacle to cooperation in cyberspace. Traditional concepts of sovereignty will shape any approach to cooperation, but the best solutions will need to transcend borders. Market forces continue to make networks and infrastructure in different countries more interdependent and more linked. Financial and banking networks, telecommunications, and international aviation communications and traffic control are leading examples of larger, international networks on which the international economy depends but which no single country controls. For many new problems, multilateral cooperation is necessary for successful national policies, but governments lack effective mechanisms for coordination.

One specific challenge is the divergence of U.S. practices (in law and regulation) from the rest of the world. As the Internet grows and diversifies, the nature of the online population is evolving to include groups with different expectations. There is a higher preference for regulation and government involvement in many other countries.

Policies also need to adjust to a more complex and equal interaction with private sector actors than was the case in the past. The deregulation and privatization pursued by many countries in the last two decades has resulted in a new kind of public policy, where governments share responsibility for some functions with the private sector and seeks to manages this responsibility through public/private partnerships. In addition, national policies will be affected by the decisions of producers or consumers in other countries will affect the success of national policies. This is particularly true of Internet issues, where most of the infrastructure and architecture is now in private hands. These private actors will often act in response to market forces that lie outside of the control of individual nations or of any government will shape the policy environment. Governance activities will need to be carried out in a commercial context.

Creating Cooperative Authentication Systems

Getting a large and expanding number of independent systems to cooperate effectively in authenticating digital network identities requires an agreed set of common elements; transparency in processes; and a framework for creating, implementing and enforcing

rules. A framework for cooperation lays out how people agree on rules and how they change them. These rules must be mutually advantageous and provide the conditions for effective authentication.

Rules can formalize this cooperative process by creating thresholds and standards for processes that correlate with degrees of trust and risk. This requires parties to agree on minimal requirements for trustworthy digital identities. The mechanisms available for providing rules are through contracts, through regulation or through private cooperative agreements. The closed authentication systems that depend upon contracts are not a central concern, because they do not pose the same problems for cooperation as do open systems. The transaction costs imposed by the need for a contract limits their applicability to a relatively small number of high value transactions. Authentication will require a blend of regulation and cooperative agreement for sets of relationships that work on a national level and can interoperate on a multinational level.

Governments and companies will need to jointly develop a common set of rules that allow identities issued by different processes and places to be recognized and treated equally. These include rules governing:

- The relationship between persons or devices and the identity issuer. These entail the grounds for issuing an identity. Identity issuance is usually part of birth or naturalization, 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 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 standards on how identities are issued and safeguarded 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 credential and the recipient of that credential. These will be primarily commercial practices, governed by commercial law, but very strong safeguard and penalties for misuse of digital identify credentials will need to put into place.

The best approach to rules will not be to set a single standard and expect all systems to meet it, but instead to identify several different levels or grades for authentication that correlate to the minimum standards for the rigorousness of internal processes and then let individual systems decide where they want to come out. These should cover enrollment, verification and revocation, liability and protection of personal data.

Given the complex and varied nature of transactions in which digital identities could involved, and given the tendency of individuals to control risk by limiting the amount of information they reveal in certain transactions, the result will be different classes of

digital identifiers. A cooperative system will have to accept different classes of users and different levels of trust for digital credentials. There will be cases where trust will not be reciprocal. A low level system can trust a credential issued by a higher level system, but the high level system will not trust a credential from the low system, or will only trust it for limited purposes.

Mechanisms and Venues for Cooperation and Federated Authentication

There are several models for cooperation, but given that the systems involved in authentication will be heterogeneous and autonomous, a federated approach is preferable. A federated approach works best when the participants are autonomous but need to cooperate to solve common problems. Federation implies cooperation among independent systems distributed across the Internet. Participants in a federated structure have defined specified obligations and agreed to meet them.

Building a federated approach will require negotiations at several levels. On a national level, the private sector and the government will need to determine what national laws and regulations will be necessary and how their authentication systems will interoperate. This could include establishing requirements for digital identifiers, a means to assess credentials and systems against these requirements and to convey that assessment to relying parties, and rules for third party credential use. On a multilateral level, countries will need to create rules for how national systems will interoperate. Multilateral delegations will need to blend both private sector and government representatives, as is the practice at the OECD or the ITU. Finally, private sector groups will need to develop the standards necessary for interoperable authentication systems. While this is a complex task, there are precedents for how to negotiate and achieve the cooperation needed. One issue for consideration is whether to use an existing organization or to create a new group specifically for this purpose.

Surprisingly, an improved ICANN-style approach might be worth considering. ICANN has many flaws, including a lack of transparency, accountability and representation. An improved ICANN that was composed of both public and private sector members with representatives' from a range of countries, that used transparent processes and included mechanisms for accountability, could offer a coordinating body for authentication issues. This could work as a pilot group of a few leading or like minded participants that could do precedential work in a transparent fashion for later review and use by some larger multilateral body. Governments will have immense 'leverage' in this process as they are likely to issue millions of digital credentials as part of their social service activities, a figure likely to be unmatched by commercial authentication services.

Some authentication architectures could require the creation of a managing entity (as ICANN has responsibility for the DNS). There are many disincentives for creating yet another body, including how to fund it. However, the process of reaching agreement on a federated approach will require one or more groups to serve as the vehicle for discussion. The central requirement for such groups is that participants in a federated authentication system perceive them as legitimate. This means that rule-making needs to be

representative, transparent and follow equitable decision-making practices. Rules promulgated by a group not seen as legitimate would likely not be followed.

ICANN itself is not the right model for establishing the process for creating a federated authentication system. The U.S. government was able to unilaterally award management of the Domain Name System, which it controlled, to ICANN. There is no similar ownership or dominance of the many existing authentication systems, so a unilateral solution for governance is not feasible. An improved ICANN might blend public and private entities that provide authentication services into a pilot group that could establish early and precedential arrangements for cooperation and interoperability.

Non-cooperative solutions for authentication are not impossible and international cooperation is not necessary for federated systems to work on a national level. If the U.S adopts one approach and the European Union another, they could perform independently, albeit not maximally. However, a collection of unilateral approaches is unlikely, given the degree of international cooperation that already exists for high level authentication services (such as Identrus[5]), the multinational nature of many service providers (seven of the ten largest Internet Service Providers in Europe are American companies) and the level of comity among the PKI programs of different nations. There is an opportunity for a group of like-minded nations to develop the framework needed for federation of authentication. Regional bodies like APEC, which is already reviewing PKI cooperation, could play a role. Ensuring compatibility among digital identity systems may require the development of model legislation. The UN Committee on International Trade Law, which drafted a model law for digital signatures, could serve as a vehicle for discussion, but its large and varied membership does not make it a good starting point for cooperation.

The OECD might be a good choice for a negotiating venue, given its experience with network security, e-commercial and other issues. The OECD has frequently provided a vehicle for developing collaborative solutions to multinational problems. Its members are among the more economically developed states and have a degree of like-mindedness in their approach to problems (the G-7 is a similar body but the OECD's larger membership makes it more attractive). The OECD has experience with Internet issues, having developed common guidelines for taxation, privacy and security, and its negotiations, while government led, have a strong private sector component. OECD Guidelines are voluntary, not binding. The U.S. has brought issues similar to digital authentication to the OECD in the past in order and it could suggest that the OECD undertake to develop common approaches to enrollment, verification and revocation, privacy and governance for authentication systems.

Conclusion

The problem of authentication will only grow more complex as ubiquitous computing and expanded Internet activity become normal elements of business and private life,

[5] Identrus is a closed, contractual system created by a group of financial institutions for high value-financial transactions.

With the right framework of rules, new applications will take advantage of these ubiquitous computing resources and automate many routine activities. Providing the architecture and rules for persistent, unambiguous authentication of identity is one of the challenges that must be addressed for further progress.

Neither governments nor the private sector can alone solve the problems of authentication and identity. Building trust in anonymous global collection of computer networks will require countries to cooperate. The shape and nature of this cooperation is only now beginning to emerge. However, finding ways for countries to cooperate at both the governmental and private levels is not a new problem. Countries have been able to work together in many other areas by developing cooperative arrangements that specify how systems will interact and under what conditions the laws of one sovereign state apply to another. The Internet does not yet have the web of cooperation that has built up for other problems. This is in part because it is new, in part because we are not sure what is needed, and in part, because it infringes on so many sensitive economic and political issues. Creating this cooperation is the essential step for digital authentication to work.