Authentication 2.0 - New Opportunities for Online Identification

James A. Lewis
Center for Strategic and International Studies

January 2008

Executive Summary: Authentication 2.0 - New Opportunities for Online Identification

Digital networks offer people new opportunities. Taking advantage of these opportunities, however, will depend on whether we can improve our ability to authenticate identity online. Weak authentication distorts social interactions, security, and business on the Net. Without better authentication, we will forgo many opportunities and the Net will remain a place that holds considerable risk.

Authentication technologies that can create digital credentials that are secure, but not necessarily trustworthy. This anomaly explains how we ended up where we are today – in a situation where we have very strong credentials that are not widely trusted and therefore not widely used. The problem – and the solution – to authentication do not lie with technology. Better authentication requires expanding trust, but trust is in short supply on the Internet. Changing this requires answers to three questions:

- How do we build trust and manage risk and uncertainty in authenticating digital identities?
- How do we increase interoperability among autonomous and heterogeneous authentication systems?
- How do we adapt paper identity processes to digital and networked applications?

Authentication online involves several steps. A person or device sends another person or device an electronic impulse over a network. This impulse represents ones and zeros – the basis of digital communications. Another computer receives the ones and zeros and translates them into an assertion about the sender's identity. What is being sent is not an identity, but digital information relating to identity, just as your driver's license is not your identity but a document that provides information about your identity. The recipient of the package of ones and zeros then has to decide whether and how much they trust this digital assertion. A small part of this decision lies with technology − whether the bits have been tampered with during transmission − but most of it relates to what lies behind them, the processes that link the digital assertion of identity (which we can call a credential) to a person.

People often assert that they have more than one identity, or that their identity has many different aspects. For authentication purposes, what they usually mean when they say they have multiple identities is that they use more than one name, they choose to use a collection of alternative names or pseudonyms, each of which can be associated with a different set of attributes or used for different transactions. But when it comes to important transactions – applying for a passport, getting a mortgage, or incorporating a company – transactions that involves large amounts of money or risk – these multiple identities fade away. Authentication in these cases must be based on the primary identity associated by governments to a person's physical body, and the trustworthiness of a credential is determined by the strength of its links to this primary identity.

In an ideal world, online authentication would be as seamless, invisible, and easy to use as the ability of one computer to connect with any other computer on the Internet. A world where each transaction needs its own credential would be unwieldy at best. The first days of credit cards are an example of this kind of world. Stores and restaurants each issued their own card. These cards were unusable at other stores or restaurants. Each issuing store or restaurant had to carry the

costs of managing the system. The single card system was inefficient for issuers, users, and receiving parties. Unfortunately, this is how online authentication now works.

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 shared operations are defined (as the Internet itself demonstrates). There is a time-tested way to get multiple, independent, and heterogeneous systems to work together to achieve a common purpose. This is to federate.

A federated approach to authentication means developing a common set of rules that allow identities issued by different processes and places to be recognized and treated equally. Rules for a federated approach to authentication will need to establish a baseline for enrollment, verification, and revocation for different classes of digital identifiers. While the procedures used by different authentication systems may differ, the outcomes will need to be the same. Rules also have architectural implications. Rules for how federated systems will share information for participation and for liability will shape the relationships among authentication systems. Some of these rules will be specific to authentication and controlled by the federation; other rules governing liability, civil liberties, or privacy will belong to both the federation and to the larger civil society.

Federation is moving to center stage because there are many authentication systems emerging in both the public and private sectors. National laws and culture shape these different initiatives, but the trend is to provide digital, networked credentials. No single system will work for all transactions, nor will consumers and citizens want such an identity system. Individuals, agencies, and companies will want to be able to use multiple credentials that provide different degrees of liability and trust. Participation will be mandatory in some systems and voluntary in others.

Identity and authentication do not happen in isolation. They require context and relationships, and a web of interactions among many participants. Technology alone cannot supply context and relationship. These must be assembled from a range of different interactions, each of which provides a piece of authenticated identity. The pieces needed for better authentication are present in a way that was not true a decade ago. Trial and error has helped to identify crucial obstacles and suggest the means in which they can be overcome, including the development of new technologies that offer greater control of information and enable approaches to authentication that no longer assume that the same solution is needed for every transaction. What we lack is the policy framework to join these pieces into trustworthy online identity systems that will win wide acceptance. These frameworks will appear eventually, but we can accelerate their appearance (and the benefits they will bring) by articulating a vision of what authentication and identity will look like, what needs to be done to achieve it, and who is best suited to do this. All of those who have a stake in authentication of online identity will need to play a part, or to be represented in the efforts to design effective policy frameworks.

Authentication 2.0 tells how new initiatives, new technologies, and new rules can provide these answers. It discusses authentication fundamentals and history and identifies key problems. It lays out the components of authentication: assertion of identity; verification of that assertion and interoperability of assertions and credentials – not just technical interoperability but an ability to

exchange trust over computer networks. It then T focuses on interoperability and 'federation' – what to do when there is no single overarching identity system or authentication technology and how to get the 'social contract' needed for trustworthy online identity. It describes the new technologies, initiatives, and regulations that give countries a better chance of fixing the online identity problem. Better government records and credentials are an essential element of this. Digital authentication will require governments to improve their processes for issuing birth certificates, social service numbers or driver's licenses. Governments and the private sector will need to decide how to use existing identity processes for digital identity and whether to seek legislation or other remedies to improve the issuance of core identity documents. Finally, the report discusses the challenges presented by issues like privacy and liability and offers next steps for taking advantage of the new technologies and initiatives.

Improving authentication is a daunting task. Progress will require coordinated action by multiple public and private sector actors. We should not underestimate the complexity of this task. But the opportunities are real. Improvements in government processes, new technologies and new private sector initiatives can combine to supply the authentication services needed to reap the full advantage of digital networks. What the report that follows has found is that government and the private sector have an opportunity now that they did not have a few years ago to fix one of the fundamental problems of the Internet.

Authentication 2.0 - New Opportunities for Online Identification
January 2008

We have entered a new era of online activity. Digital networks, using computers and mobile devices, offer new connections, new information, and new opportunities. The number and kinds of digital applications continues to grow and people interact digitally in ways we did not expect a decade ago. How people take advantage of these opportunities and applications, however, will depend on progress in authenticating identity online. Without better authentication of identity, we will forgo many opportunities and the Net will remain a place that holds considerable risk.

The ability to authenticate identity on digital networks shapes social interaction, security, and business on the Net. The first Internet era, the era of the dot.com, with its notions of the decline of the state, the emergence of self-regulating online communities, and a general view that old rules did not apply, gave rise to the idea that private actions would produce trustworthy public networks without government involvement. The legacies of that era include a misunderstanding of the role of government in providing the foundation for trust in identity, and an over-reliance on technological solutions to what were essentially problems of policy. Understanding why these dot.com ideas did not work and why this era of spontaneous online trust did not arrive is important for assessing how to move ahead in authentication.

The largest problem for authentication involves trust. Trust is in short supply on the Internet. In thinking about how to expand trust for Internet identities (and for Internet transactions using these identities), we have to confront a fundamental ambiguity. An accurate and secure digital identity will still be essentially untrustworthy if it is difficult or impossible for the receiving party to assess how much the assertion can be trusted.

Weak online authentication – which is what we have now – undercuts trust and limits the possibilities for greater security, more efficient government services, and a more productive economy. Strong authentication technologies can create digital credentials that are very secure, but not necessarily trustworthy. This anomaly in the security of digital credential explains how we ended up where we are today – a situation where there are strong and reliable credentials that are difficult to tamper with, but not widely trusted and therefore not widely used when it comes to authentication across different systems and technologies.

The weaknesses of online authentication are well known, and new initiatives, new technologies, and new laws are changing the landscape for online authentication of identity in ways that give us the possibility to seize the opportunities offered by digital networks. The five sections of this report tell how the authentication process combines identity, credentials, and trust. The underlying conclusion is that government and the private sector have an opportunity now that they did not have a few years ago to fix one of the fundamental problems of the Internet.

Section I: Fundamentals and History

Discussions of authentication issues often overcomplicate the issue. We are really talking about a simple act. One person or device sends another person or device an electronic impulse over a network. This impulse represents ones and zeros – the basis of digital communications. The

ones and zeros are received by a computer and translated into an assertion about the sender's identity. What is being sent is not an identity but a digital representation of information relating to identity, just as your driver's license is not your identity but a document that provides information about your identity. The recipient of the package of ones and zeros then has to decide whether and how much they agree with and trust this digital assertion.

A small part of this decision lies with technology - whether the bits and bytes have been tampered with during transmission - but most of it relates to what goes on behind the scenes, the processes that link the digital assertion of identity (which we can call a credential) to a person. We all have one body. Society and government assign that body a single, primary, legal identity. Body and assigned identity combine to make a "person," but that person can have many different credentials, each providing different and not necessarily consistent sets of information. It is in the processes for linking credentials to a person and their legal identity and body that authentication has often fallen short, usually because of two key problems – a lack of interoperability among different authentication systems and the lack of any solid means to judge the trustworthiness of a credential – a digital assertion of identity.

Some of the confusion over authentication arises from different meanings assigned to the word identity. It is not unusual to hear people say in discussions of authentication that they have more than one identity, or that there are many different and fungible aspects of their identity that they can use for authentication purposes. True multiple identities are a psychological disorder. Usually what people mean when they say they have multiple identities is that they use more than one name, that they choose to use a collection of alternative names or pseudonyms, each of which can be associated with a different set of transactions.

But, when it comes to important transactions – applying for a passport, getting a mortgage, incorporating a company, or appearing before a court – transactions that involve money, security, or liability – these multiple identities fade away. Authentication in these cases must be based on the primary identity associated by governments to a person's physical body, and the trustworthiness of a credential is determined by the strength of its links to this primary identity. Credentials can be weakly linked to the primary identity, but these will not be used for important transactions. Credentials can be anonymized, so that personal information is protected, but these anonymous credentials will be trusted only to the degree that the recipient of one believes it is firmly linked to a legal identity.

There is of course an intense terminological debate within the discussion of authentication. This debate revolves around definitions for identity and authentication components and processes. In some instances there are even competing terminological schemas, each with its own partisans, although there is often little substantive disagreement.

In part, the terminological debate reflects the unavoidable complexity found in the concept of identity. There is rich literature that dates back more than a century in the social sciences and in philosophy on identity and how it is created. Current discussions of authentication often reflect (albeit indirectly) this literature and its concepts.

These concepts describe identity as the set of characteristics by which a person or thing is known. Identity is an individual's understanding of himself or herself as a discrete entity, and his or her understanding of others as discrete entities. Identity develops through interaction with others, and it is dynamic – an identity can change over time as new attributes are added. Identity and naming can be linked – one term for describing an unidentified person is to say they are 'incognito,' Latin for an unknown individual. Individuals can choose to present some subset of the characteristics that describe them, and this subset can also be considered an identity. One dilemma for the provision of commercial or government services online is that it is currently difficult to determine, using only a digital credential or assertion, when this digital assertion of identity is based on a subset of characteristics and whether this subset sufficiently describes a participant in a transaction for purposes of payment or liability.

The terminological debate over authentication also reflects the absence of a viable business model - if there was a business model that made money, that model and its terms would dominate the discussion. In the absence of a compelling commercial application, competing terminologies can flourish. An effective process to create standards and interoperability in authentication will eventually reduce the competing terms to some mutually agreeable set. In the interim, it is important to make sure that terminological discussion does not slow progress toward better digital authentication.

A Brief History of Identity and Authentication

Authentication of identity is a relatively new problem, not only because digital technologies are new, but also because the whole concept of proving identity by using credentials is not that old. One hundred years ago, there were no identity cards. You were who you said you were or whom people knew you to be – your friends, your banker, your clergyman. With few exceptions, this is how people had identified themselves for all the centuries before the arrival of the Internet. Nevertheless, even a century ago, there were problems with this traditional approach. The possibilities for fraud were endless, aided by new technologies like the steamship and the railroad that let people move easily around the world, leaving behind old identities or creating new ones as needed.

In 1914, with the onset of World War I, this informal approach to identity created serious problems for security. Worried that German agents were slipping into the country, the United Kingdom created the first mass-produced identity document – a passport that contained a photograph and a physical description of the bearer. Other nations quickly followed suit. This was the birth of the modern, government-issued credential. A piece of paper with a photo, some personal information and an official seal remains the most common form of credential.

At first, the Internet did not change this. Authentication of an individual's identity was not a major issue for early computer networks that linked employees of a single firm or small communities of researchers and government agencies. This situation changed rapidly as the opportunities for transactions with strangers grew exponentially. Commercialization of the Internet resulted in a largely anonymous global network connecting millions of poorly identified users whose identity was established by assertion, through email or Internet addresses, using credentials derived from unknown or unknowable processes. Creating systems for better

management and authentication of digital credentials has been a goal of government, business, and the technology community for many years, and building secure public networks became an issue for public policy in the 1990s.

Governments and companies in many countries focused their efforts on two areas: developing and deploying specific, 'silver bullet' authentication technologies (often Public Key Infrastructures-PKI) [1] or on providing digitally signed documents the same legal status as paper. Most digital signature laws relied implicitly or explicitly on PKI technologies. PKI's are based on public key cryptography – a method for key management that allows strangers to exchange encryption keys for the coding and decoding of messages. PKI technologies were developed commercially in the mid 1970s, and they have been in search of a successful business model ever since. In the 1990s, it was assumed that this exchange process would be managed by 'trusted third parties' from the private sector who would provide digital credentials that could be used both to encrypt and decrypt messages and to confirm identity.

But neither PKI nor digital signatures found widespread acceptance. Privacy and liability concerns, cost, complexity, and a lack of related applications were major obstacles for the adoption of PKI. With digital signatures, few purchasers wanted the services being offered, in part because they offered little advantage over paper processes and carried unknown liability risks. PKI and digital signature failed to deliver trusted identities, as they did not adequately address the larger problem of how to create processes external to the network to ensure that a digital identity could be reliably authenticated. Additionally, the technology-specific approach used in many PKI and digital signature initiatives doomed these early efforts at authentication.

The Internet created demands for new kinds of authentication and credentials – digital credentials composed of bits and bytes, not paper, useable on digital networks. This credential would let Internet users "authenticate" – that is confirm - an identity claim made over computer networks. Authentication of identity allows us to assign privileges, responsibilities, and liability in cases of dispute. The goal was a digital document that, like a passport, would let you prove your identity as you traveled through cyberspace. The attacks of September 11, where weak credentials played a role, and now concerns over identity theft and online fraud, give added impetus to the search for better ways to authenticate identities.

Self-regulation has many advantages for distributed, nonhierarchical organizations, like the Internet. At the same time, self-regulation can decrease oversight and transparency in ways that damage trust. This is a particular problem for digital networks, where many of the rules that govern them are embedded in software and are not accessible to most participants. Our online behavior conforms to multiple sets of invisible rules, created by unknown parties, and the result of so many unknowns is mistrust. Transparency increases trust. Government rules and agencies can play a role in this, along the lines of the FTC's role in privacy protection, by ensuring that service providers are transparent about what they are doing with authentication information and that they comply with their commitments.

[1] Public key infrastructures are based on public key cryptography – a method of key management and exchange that allows strangers to exchange keys for the coding and decoding of encrypted messages. The key is a mathematical formula that encodes and decodes an encrypted message.

Opaque processes and weak identities have created a lack of trust that is perhaps the Internet's biggest problem. Cybercrime and identity theft are well known threats. More importantly, the lack of trust hampers the growth of new Internet applications that offer new services and new savings. Meanwhile, governments, corporations, and consumers are grappling with the challenges of online authentication. While better authentication of identity promises benefits for digital commerce and for security, there are risks and obstacles. These include the need to adopt identity policies and processes created for paper to a digital environment, reducing the lack of interoperability, deciding how to establish trust, allocating liability, and protecting privacy.

II: Elements of Authentication

In thinking about authentication, identity, and trust, it helps to start with the fundamentals. Identity has many meanings, but in this case, it means a set of distinguishing characteristics or attributes uniquely associated with one person. In most western countries, your family assigns you a name and your government records your name and the names of your parents. This is the start of identity. Over time, you are embedded in networks of transactions and associations. You accumulate records of activities (such as education, medical, financial, histories) and usually you acquire a government-issued credential (an identity card, a driver's license or passport) by the time you are twenty. This history and the associated records and credentials provide the basis for legal, primary identity.

Authentication begins with an assertion of that identity by someone who wants to engage in a transaction. Authentication is the process of determining the trustworthiness of that assertion of identity and of establishing the degree of confidence about the validity of an assertion of identity. Online authentication is the process in which an individual translates an assertion of identity into bits and sends it over a network to another party. There are many techniques that can be used for online authentication - passwords, biometrics, smart cards, or certificates - but online authentication of identity has three fundamental and interlinked functions: assertion, verification, and interoperability.

The act of authenticating an assertion of identity is based on relationships among three sets of actors: the person (or device) that asserts its identity; the receiving party of that assertion; and the system upon which these transaction occur. The most complex and challenging relationship is when a person in one system asserts identity to a receiving party in another system; how these systems interoperate in exchanging trustworthy assertions of identity (or their inability to do so) is the crux of the online authentication problem.

Assertion

The first set of actions in authentication involves the initiating party in a transaction asserting their identity. When you identify yourself, even in something as simple as providing your name, you are asserting something. You assert that the information you provide correctly identifies you – links you to a name, a history, or other attributes. The recipient of this information (known in some authentication lexicons as the 'receiving party') must decide if this assertion is true. This might be something as simple as an instinctive feeling about whether the person is telling the truth, whether a credential looks real or forged, or it might involve checking with a reference.

Identity assertions can be confirmed in several ways. In many settings, an assertion is simply accepted without question, but this depends greatly on context and the risk and value of the transaction – you may accept an oral assertion of identity at a party, but you would never accept it for a mortgage. Someone asserting an identity can supply documentary evidence to support and verify an 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 to which it is attached 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 receiving party.

Digital authentication can use shared secrets, biometric data, or software credentials, to make an assertion of identity where a user sends data in digital form over a network. Each method has strengths and weaknesses. Passwords, the most common form of shared secrets, are easy to guess or capture. Biometric data requires additional equipment and can be mimicked (one Japanese researcher fooled an early biometric authentication system by using Gummy Bears to copy imprints of a fingerprint), or captured in transmission. Digital credentials can be the most secure means of authentication, but face serious problems that technology alone cannot solve.

A credential translates an assertion of identity ("I am John Smith") into a physical or logical form. Credentialing links an identity document (digital or paper) to a physical person and their records. The issuer of the credential provides a document that can be used to confirm an identity for third parties, sparing them the effort of repeating the research needed for confirmation of identity. The credential issuer is basically saying I have done the work to determine that this person is who they say they are, so you can accept this document or token as a trustworthy confirmation of their identity. This means that whatever technology is used, a credential is only as good as the processes that lie behind its issuance and the ability of a receiving party to know and have confidence in those processes when they make a decision about an identity assertion's validity.

Most credentials are ultimately based on a government document or record. The life of a "stateless person' shows the importance of these government records for identity. In most cases, a stateless person is a refugee who has been obliged to flee his or her country of origin or residence. Often, the government of that country has collapsed. That leaves the stateless person with a passport or other document that is no longer confirmable – there is no government to stand behind its issuance. A person with no valid identification and no means of obtaining valid identification faces an array of troubles. The usual solution is for the UN High Commissioner for Refugees to issues some interim identity document, but these are often regarded with suspicion and scrutiny until the refugee is finally accepted as a resident by another government.

Enrollment is the process by which an individual person, corporation, or device is issued a credential. Enrollment has been the great weakness in digital authentication and is a problem not amenable to a technological solution. Part of the problem lies with weaknesses in the core documents upon which enrollment is based. In the U.S., enrollment begins with the birth certificate and the social security number (SSN). These documents are foundational and their

weaknesses and the weaknesses of associated processes have been a major impediment to better authentication. Until recently, the processes for issuing and managing these government identity documents were inadequate either for the digital economy or for homeland security.

U.S. birth certificates and the SSN are not credentials. They provide the foundation for issuance of other credentials, such as a driver's license or passport. The processes used for driver's licenses and passports are very different, however. Passport applications are rigorously screened; before the attacks of September 11, driver's license applications were not. This means that one of the central credentials used in the U.S. was inadequate. To a considerable degree, it remains inadequate, in large measure because the processes used for verification and issuance still reflect a world of paper files rather than networked digital records.

Other nations face similar problems in transforming paper documents to serve a digital environment. Meshing paper-based processes to a digital environment (and to digital credentials) has been difficult, since the process entails both new costs and requires new forms of cooperation between governments, the private sector, and citizens. It is also difficult because it requires coordinated change in both government policies and commercial processes.

The transition from paper is important because digital identities and credentials will be derived from government issued credentials and the transaction histories related to them. New technologies have created the possibility for strong credentials and a stronger credentialing process. Much of the progress in authentication technological in the last ten years has been to develop and refine the software behind credentials and the methods in which they are securely transferred from one computer to another. There are many different authentication technologies that provide strong and trustworthy digital credentials. The appearance of smart cards also creates new opportunities for better authentication. Smart cards can carry a larger amount of identifying information than the photo and few words on the laminated plastic card. More importantly, what makes the cards 'smart' is that the chip they carry can be "read" – and if the reader connects to a network, the information carried on the smart card can be checked and verified against a remote database. Homeland Security Presidential Directive 12 (HSPD-12), a requirement for federal agencies to improve their identity and credentialing processes, takes advantage of smart cards to secure both physical and logical access to federal facilities and networks.

However, there are several weak points in the credentialing phase that make people reluctant to trust online credentials. The first is the moment when a credential is associated with a person's identity. If you do not know the processes used to make the association between person and credential, and the data used in these issuance processes, you will not trust the credential. Did the issuer take a casual glance at a driver's license; did they run a credit check; or was there greater scrutiny of documents and histories? If these questions on how identity was established cannot be answered, trust in the credential is reduced. Getting digital credentials to work smoothly across different 'trust domains' (e.g. between different issuing entities, such as companies, universities, or government agencies) has been difficult, not only because of the technical issues involved interoperability, but also because of the lack of a common framework or rules by which one person could assess the trustworthiness of a credential issue by another.

Until recently, government efforts in the online identity process were usually counterproductive. Programs in Europe, the U.S., and Asia at times seemed to alternate between over-enthusiastic adoption of specific authentication technologies (like digital signatures) and timidity over networked credentials. The U.S. federal system, with its division of labor among counties, states and the Federal government, also hampers the introduction of strong credentials. Federal, State, and local governments in the United States were slow to move from paper to digital records for crucial identity documents, such as birth certificates, driver's licenses and social security numbers. They were even slower to network these records to allow for their verification and revocation. An identity system based on a melange of uncoordinated documents from all three levels of governments is not adequate for a digital economy.

Deciding if an assertion of identity is correct?

The next phase in authentication involves the individual presenting the credential to confirm identity and enable some kind of transaction – the assertion of identity, and the acceptance of that assertion as true by the receiving party. This is verification, acceptance of the credential as a valid assertion of identity. Verification is the process, at the initiation of a transaction, when the digital identifier is itself checked and authenticated – e.g. a receiving party accepts and trusts the credential. In an ideal authentication system, this happens automatically and transparently. Verification will be essential for online transactions as identification and authorization become inextricably linked.

Verification techniques used for physical credentials such as driver's licenses or passports, which in most cases involve an official holding the credential and staring at it to detect fraud, are of no use for digital authentication. We are all familiar with the process at the airline ticket counter. You hand your driver's license to the person at the airline counter to prove that you are who you say you are. The ticket agent looks at the picture on the license and 'validates' your identity (of course, what the driver's license actually validates is that the person carrying the license has the same face as the picture on the laminated plastic card). There is no tangible presence that can provide clues as to the validity of the assertion of identity. An experienced police officer or immigration official can often tell from behavioral clues whether a credential and its bearer deserves additional scrutiny. There are no such clues on your computer screen, however.

The essential questions for online verification revolve around trusted processes. How does the receiving party know that the credential was issued using trustworthy procedures, has not been tampered with, and accurately represent the claimed identity? The reputation of the issuer is important in this, which is one of the reasons government credentials are considered more trustworthy by most people (who assume that a government is more likely to ensure accuracy and enforcement). However, the most important question is what processes are used by the issuer to make sure that the identity represented by the credential is the same as the identity of the person (or device) applying for the credential. If the receiving party has no way to know what the processes are, or if they know the processes but do not know how faithfully they were followed, or if there is no remedy for accepting a credential that purports to be trustworthy but is not, many receiving parties will not use the credential for high value activities.

Another set of questions concerns the life of the credential after issuance. If the receiving party decides that the issuer and processes used to issue the credential are trustworthy, the remaining concern is whether the credential has been modified or tampered with since issuance. These questions about the reliability of the technology that is being used do not involve policy issues.

Digital credentials have an advantage over physical credential when it comes to verification. Not only can the software credential be more robust than the physical credential (in the sense that it can be harder to modify or counterfeit), it can also be checked against online resources. The ability to use strong encryption algorithms and to exchange data over high-speed networks with the issuer to confirm the credential makes it much more difficult (but not impossible) to spoof a digital credential. Digital credentials are at a disadvantage when it comes to the first set of questions. The processes used by the issuer are invisible to the receiving party, and there is no knowledge and little liability for the issuance process.

Basing identity on the foundation of government credentials is not the only way to establish identity. An alternative approach to authentication uses an individual's history of transactions to establish and confirm identity. The basis for this alternative is the increased ease of keeping and accessing digital records. A set of records, educational, medical, or other services, and in the last few years, consumption, is associated with each person. Each of us has left a largely unique trail of records that others can use to confirm our assertion of identity.

Credit card companies already make use of this approach. They have developed sophisticated algorithms to spot fraudulent charges. These algorithms compare a transaction to a pattern based on previous transactions to determine if it is legitimate or not. The appearance in the last decade of major information brokers, who have amassed collections of records on millions of individuals, simplify this transactional approach to authentication. High-speed digital networks allow for rapid checking against these databases.

EBay, the online auction service, also makes use of reputation to establish trust. In eBay's case, the record of previous transactions – how many and how many customers had a satisfactory experience – allows a stranger to assess whether or not to trust an online merchant. New social networks like Facebook, LinkedIn or MySpace use similar reputational techniques to provide users a means to evaluate trust.

Drawing from the experience of the financial industry, future systems might want to take advantage of network technologies to combine robust credentials with online verification based on records and transaction histories. By taking advantage of network capabilities to check multiple sources simultaneously, an authentication system is duplicating, in effect, an element of better enrollment processes. Authentication processes will be more trustworthy if they provide the option of going to databases or directories to verify the authenticity of a digital credential, but this ability to make credentials the link between an individual and their personal information creates serious privacy issues. Most transactions do not require presentation of a person's entire history to be validated and a credential should not be the passport to immense amounts of personal data. Rules and procedures to limit disclosure will be needed for both credential issuers and for receiving parties.

Authentication using digital technologies and databases will provide an opportunity to collect immense amounts of data. An ability to link identities to databases provides governments and companies a deep look into an individual's transactions and activities. Online authentication of an identity assertion provides a new and valuable data point and rules for authentication will need to address the question of what occurs when an assertion is received: what can be stored, what can be linked, and what can be accessed or shared. Existing privacy requirements in the EU and for various service sectors in the United States (health, financial, government) will shape the verification process. It is unclear as to whether current privacy protections are adequate for the emerging authentication landscape. A failure to resolve concerns that improved authentication would erode privacy and slow adoption.

The collection and use of census data provides a perspective on the privacy problem. While the U.S. government collects a vast amount of information about citizens and companies, and this data is available for research, by law this personal information is anonymized so that a statistic cannot be traced back to an individual or company. In contrast, there are a number of large data aggregators in the U.S. who also collect vast amounts of data on consumers. This data is not anonymized; it is offered for sale. The creation of strong credentials and expanded online authentication, without appropriate safeguard, could expand the collections of the data aggregators in ways that would further diminish individual privacy.

Section III: Interoperability - Creating the Social Contract for Authentication

Good processes for issuing and validating credentials are not enough to complete the picture for authentication. These two pieces require a third necessary element: interoperability. Interoperability is not an end in itself but the means to enable wide-scale digital authentication. Interoperability is crucial in a digital environment where there are many different credential issuers and many different authentication technologies. There are real costs to a lack of interoperability. Americans have experienced the cost of a lack of interoperability when they have arrived in Europe and found that their cell phones no longer worked.

Interoperability has two elements: (a) the technical standards and protocols that ensure that one authentication technology can exchange trust with another; and (b) the rules and policies that establish trust in the first place. However, you can have technical interoperability, where one authentication technology can work easily with another technology, and still not have interoperable authentication. Building interoperability requires both technical standards and a system of shared or common rules for processes (like confirming identity at the time a credential is issued) that all parties accept and use. Common rules make it easier for a recipient of a credential to assess whether or not it is trustworthy and a valid assertion of identity. Without these common rules on process, even having every company and person use the same authentication technology will not lead to a trustworthy environment

Interoperability 1.0 - PKI and Digital Signatures

Initial efforts to bring interoperability to authentication did not work. These initial efforts began in the mid-1990s, when government realized that the commercial Internet, a largely anonymous global network connecting millions of poorly identified users, was not optimal for commerce.

Repairing this becomes an issue for public policy. Governments and companies in many countries focused their efforts on two areas: creating public key infrastructures and building the legal framework for digital signatures. PKI and digital signature laws seemed to provide the technological and legal structure needed for interoperable authentication of identity. The UN, the European Union, the Organization for Economic Cooperation and Development (OECD), private groups, and nations like Germany and the United States developed models for digital signature laws. Many digital signature laws included standards for commercial authentication services, regulations for commercial providers, and requirements that digital signatures and digital documents would carry the same weight and standing as their paper counterparts.

In retrospect, these early approaches to authentication of online identity overestimated the value of authentication. Trust is expensive, and at that time, given the applications available on the Net and the costs associated with PKI, people were unwilling to pay for it. The chief contribution of these laws is that they ensure that digital documents receive the same treatment as paper documents when they are appropriately authenticated. In almost all cases, the use of digital signatures under these laws was voluntary. Consequently, relatively little use has been made of them, in part because of unresolved risk and liability issues and in part because of the lack of attractive applications. Few purchasers wanted the services being offered as they offered little advantage over paper processes and carried unknown liability risks. A 2002 survey of German Internet users found that only five percent availed themselves of digital signatures, despite strong support from various parts of the German government.

Privacy concerns, registration difficulties, cost, and a lack of related applications have been obstacles to the adoption of PKI. Closed authentication systems using PKI had greater acceptance since closed systems (such as internal company networks) are better able to control risk and limit the costs of key management. Some government PKI pilot programs in the U.S., Canada, Europe, and Asia have persevered and, in the context of a larger and more heterogeneous approach to trusted credentials, PKI could be one of the technologies used for authentication.

The PKI experience does offer two valuable lessons for online authentication, however. First, the policies and processes that accompany these technologies – including enrollment, treatment of personal data, and liability − must be addressed for any authentication system to be adopted. Second, no single technology or service provider will be able to meet the demands of the market – in fact, a homogenous approach to authentication may actually deter use.

A Second Life for Interoperability

The emerging authentication landscape will use different technologies, networks, and credentials – some governmental and some private. To be interoperable, one identity system must be able to accept and authenticate a credential issued by another identity system. Both technology and processes must combine to provide assurance that a credential is based on correct information, and that the credential and the information it carries has not been tampered with after issuance. Technology alone cannot provide interoperable solutions for trust.

Most people will not want or use a single, all-purpose credential for all of their online transactions. Multiple credentials preserve a degree of privacy that may protect an individual's core financial assets. Acceptance of these various credentials, however, is a problem. Absent some framework for interoperability, many companies will not want to rely on a credential issued by another company. This means that we will see multiple authentication systems distributed among government agencies, companies, and commercial service providers in many countries. The number of systems will expand and the technologies they use will continue to differ. All, however, will need to perform similar functions. This commonality of function provides a starting point for interoperability and widespread authentication of identity.

In an ideal world, online authentication would be as seamless, invisible, and easy to use as the ability of one computer to connect to any other computer on the Internet. A world where each transaction needs its own credential will be unwieldy at best. The first days of credit cards are an example of this kind of world. Stores and restaurants each issued their own card. These cards were unusable at other stores or restaurants. Additionally, each issuing store or restaurant had to carry the costs of managing the system. The single card system was inefficient for issuers, users, and receiving parties. Unfortunately, this is how online authentication now works, for the most part.

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 shared operations 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 these Internet protocols must perform are less complex than the tasks required for authentication, in good measure because the Internet was never designed to address issues of trust.

If each of the thousands of networks that make up the Internet had to go out and negotiate with all of the others as to how their networks would exchange information, growth would have been very slow, and the exchange of information and services over the Net would remain minimal. This interoperability problem was solved for networking by the development of the Internet protocols. Protocols and standards are agreed rules that enable heterogeneous systems to work together automatically. The use of agreed protocols and standards allows a network to communicate with thousands of other networks that are strangers to it and which may use different technologies. If authentication systems are to interoperate on a cohesive and large scale, they will similarly need agreed conventions and rules that enable different systems to work together.

Standards provide the basis for the collaboration – whether formal or informal. While there is general consensus that ‘open’ standards are best, as they expand the scope for collaboration and innovation, there is less consensus on what qualifies as open and how an ‘open standard’ should be used. The result is a complex mix of issues that challenge policies for authentication.

Governments can play a role in untangling this mix by setting clear goals. One approach to promoting interoperability is found in Section 256 of the 1996 Telecommunications Reform Act.

The Act has two key provisions relating to interoperability: "to promote nondiscriminatory accessibility by the broadest number of users and vendors of communications products and services to public telecommunications networks used to provide telecommunications service" and "to ensure the ability of users and information providers to seamlessly and transparently transmit and receive information between and across telecommunications networks." The Act further required (in Section 251) telecommunications companies not to install equipment that did not comply with the guidelines of Section 256.

The implementing agency, the Federal Communications Commission (FCC), chose to use private sector interactions, primarily standards-making bodies and business agreements among service providers, as the primary vehicles to achieve these goals, albeit with FCC involvement (to varying degrees) to ensure that the work of these bodies promoted the goals of Section 256. This approach, where governments provide goals and oversight while allowing the private sector to develop technologies and processes to achieve those goals, could also be applied to online authentication on both a national and international level (such as an agreement between the U.S. and the EU). There are risks in using a telecommunications precedent - incumbents tend to shape processes at the cost of innovation – and the Federal Trade Commission (FTC) might be the more appropriate agency for authentication, but articulation of the goal of interoperable online authentication in law or policy would provide the best framework for competition.

The spread of private and public sector authentication and identity systems has created a new opportunity to harmonize practices and promote interoperability. Grasping this opportunity will require a different approach to authentication that goes beyond engineering concepts and builds an underlying structure of rules and policies that would allow authentication systems to trust each other.

Federation and Interoperability

There is a time-tested way to get multiple, independent, and heterogeneous systems to work together to achieve a common purpose. This is to federate. Residents of the United States or the European Union are inherently familiar with federation and its benefits. Americans live in a federated republic composed of more than fifty different entities. The European federation is more limited in scope, but provides more than twenty sovereign, independent entities the platform, processes, and rules for cooperating. Federations work best when a basic document sets out how the entities will cooperate; defines their responsibilities and the responsibilities of the federation; and creates mechanism for dispute resolution and administration (this set of activities is sometime called ‘governance’). Some sort of federation, implicit or explicit, is needed for progress in authentication.

A federated approach to authentication means developing a common set of rules that allow identities issued by different processes and places to be recognized and treated equally. Rules for a federated approach to authentication will need to establish a baseline for enrollment, verification, and revocation for different classes of digital identifiers. While the procedures used by different authentication systems may differ, the outcomes will need to be the same. Rules also have architectural implications. Rules for how federated systems will share information for participation and for liability will shape the relationships among authentication systems. Some

of these rules will be specific to authentication and should be controlled by the federation; other rules, governing liability, civil liberties, or privacy, will belong to both the federation and to the larger civil society.

Federated authentication requires agreement between companies, between companies and governments and, possibly between different governments on how individual identity systems will interact. A federated system of authentication will not work without effective governance processes that provide an effective structure for cooperation. This class of political problems is sometimes called "collective action problems," where multiple actors need to cooperate to achieve the most efficient outcome. While federated authentication may seem to be a complex problem, there are numerous precedents for how to negotiate and achieve the cooperation needed.

There is one drawback, however, to the federal government as a model for federated authentication. The U.S. is a single system, with a single charter, one governing body, and subordinate elements. Trying to build a similar single organizing structure for authentication will deter participation. Authentication will more likely resemble a market, where there are many independent entities that both compete and cooperate within a framework of rules. The vision for federated authentication should be a loose collection of federations that share common understandings and protocols that can interoperate when business models and opportunities suggest there is value in doing so.

It is unlikely that a single overarching governance system for authentication will emerge full-blown from Brussels, Washington, or Silicon Valley. Progress is more likely to come about incrementally, as participants build on existing relationships to create smaller federations for specific purposes or specific areas. These federations will form the building blocks for cross-federation agreements that will lead to national or multi-national authentication systems.

IV: The New Authentication Landscape – Initiatives, Technologies, Rules

Federation is moving to center stage because many authentication systems are emerging in both the public and private sectors. No single system will work for all transactions, nor will consumers and citizens want a single identity system. Individuals, agencies, and companies will want to be able to use multiple credentials that provide different degrees of liability and trust. Participation will be mandatory in some systems and voluntary in others.

Many countries are making efforts to improve identity management, credentialing, and authentication. Machine-readable passports have become the norm. Countries are exploring many different technologies, including biometric identifiers and smart cards. National laws and culture shape these different initiatives, but the trend is to provide citizens with digital, networked credentials.

Better government records and credentials are essential. Weak processes at the start of the identity process distort and damage authentication. Digital authentication will require governments to improve their processes for issuing birth certificates, social security numbers, or driver's licenses. Governments and the private sector will need to consider how to use existing

identity processes for digital identity and whether to seek legislation or other remedies to improve the issuance of core identity documents.

Almost one hundred countries have some kind of compulsory national identity card programs. About half of these now use digital technologies. Other countries, with different legal traditions, including the United States, Canada, New Zealand, Australia, Ireland, and the Nordic countries, do not have national identity cards, but provide special-purpose credentials for accessing government services or networks. The use of special-purpose cards for the provision of social services is common and most industrial countries that do not use a national identity card issue their residents' health or social security cards. Sweden, for example, does not issue cards but provides each citizen with a national number.

Norway's banks and its primary telecommunications service provider Telenor have developed an alternative authentication system that does not rely on a national ID or on smart cards. The initiative, called "BankID," provides a strong digital authentication system based on mobile phones. The banks, which already have rigorous systems for verifying a customer's identity, enroll users and issue them a digital credential. The credential is stored on the customer's mobile phone and can be used for online banking, Internet bill payments, and for obtaining online services from companies or government agencies. There is no direct government involvement, although regulatory requirements for banks to know their customers remove uncertainty from the enrollment process.

Japan has similar commercial initiatives using the cell-phone as a platform for online commerce, based in part on government policies to create a ubiquitous network environment in Japan, where you can access the Internet from any location. As part of this effort, Japan's National Institute of Information and Communications Technology (NICT), the mobile IT Forum (mITF), KDDI R&D Laboratories, Hitachi, NTT DoCoMo, and NEC are developing authentication systems for mobile phones. Japan also issues a Resident Registration smart card (a card with a built-in microprocessor that stores digital data that, when used with a card reader, can be sent over a network) that allows citizens to authenticate themselves in order to access government services online. Use of the card is voluntary. An earlier effort to create a mandatory national ID smart card that would have given each citizen an eleven digit identity number failed because of public concerns over privacy and security− the Japanese government had promised to put in place a new privacy law before introducing the card, but was unable to do so.

Some countries with national ID cards are using them as the basis for online authentication. Although the primary uses of these ID cards is for security, law enforcement, and receiving government benefits, the increasing use of smart cards allows the modern ID card to become a credential for online authentication. These national smart cards are appearing in Austria, Belgium, and Germany. Belgium allows the private sector to use its national smart ID card private sector for commercial services and requires it for some Internet chat rooms (to make it harder for an adult to pose as a child). Austria authenticates online identity by using both a national smart card and identity information stored on a mobile phone's Subscriber Identify Module (SIM).

Finland is considering a similar system using cellphone SIM cards. This would build on the advanced identity system Finland already has in place. Finland has a national identity card, issued by the police. The card uses a chip that contains a "Citizen Certificate," issued by the Government's "Population Register Centre," the Finnish government agency that records and stores (on computerized databases) vital statistics on Finns and resident aliens. The government-issued credential uses PKI to identify cardholders in online transactions (when the card is swiped against a card reader). However, the certificate holds little personal information, as it stores only the person's name and a unique electronic identification number. The Finns do not use their equivalent of a social security number for the credential, which increases privacy protection. They also believe that having the card issued by the police increases its trustworthiness. Finland has also issued its government employees a smart card that can be used for secure online transactions.

In many ways, Finland is an ideal location for public authentication systems. Its small population is well-to-do and technologically sophisticated. It has an existing national ID and registry system administered by the government that provides a solid foundation for credentials. Privacy is not an issue, given the protections the Finns have built into the Certificate process.

Finland highlights some of the problems faced by efforts to create large-scale public authentication systems. Even with these advantages, however, uptake of the Citizen's Certificate has been slow. Although the Certificates became available in November 2006, only three percent of the population (as of August 2007) had obtained one. A lack of interoperability may explain some of this (and the Finns are spearheading an effort to create European-wide interoperability with an effort called the "Porvoo Group" − Porvoo is the town in Finland where the Group first met). The absence of commercial applications for the Certificate may also slow adoption. If the U.S. underestimated the need for government involvement in authentication, Finland may have underestimated the need for attractive commercial uses.

Authentication in the U.S.

The range of identity initiatives in the U.S. launched since 2001 is daunting. They include the e-Passport, the Western Hemisphere Travel Initiative (WHTI), the Transportation Worker Identity Card (TWIC), the Registered Traveler Program, Homeland Security Presidential Directive-12 (HSPD-12) which mandated new logical and physical credential for all federal employees and contractors, and the REAL ID Act, which requires states to improve the processes used to issue drivers licenses and to make licenses harder to counterfeit.

These initiatives touch all adult Americans. Soon, many Americans may find themselves carrying two or even three of the new Federal credentials. Only some of these initiative offer digital credentials, but they all provide the firm and trustworthy basis for enrolment and credentialing whose lack has hampered authentication's growth. In the private sector, initiatives including OpenID, Higgins, Cardspace, Shibboleth and the Liberty Alliance offer the possibility of broad-based, interoperable authentication systems for business and consumer use. The combination of more trustworthy government identity documents and a rich landscape of commercial authentication services will, with the right rules and structure, provide the possibility for rapid improvement in online authentication.

The impetus created by homeland security requirements for better credentials has led the United States to take two important first steps to improve identify processes – Homeland Security Policy Directive-12 (HSPD-12) and the Real ID Act. These offer improvements to initial credentialing that provide the foundation for better authentication.

HSPD-12

HSPD-12 mandates strong identity procedures and credential for the Federal government and its contractors. HSPD-12 authorizes the Commerce Department's National Institutes of Standards and Technology (NIST), in consultation with a host of agencies, to establish a common identification standard for federal employees and contractors. "Secure and reliable forms of identification" means credentials that are issued using sound criteria for verifying an employee's identity; is strongly resistant to fraud, tampering, counterfeiting, and terrorist exploitation; can be rapidly authenticated electronically; and issued only by officially accredited providers (e.g. contractors must be certified by the government before their ID cards can be used in government programs).

The new federal identity cards will provide for both physical and logical (i.e. network) access. HSPD-12 calls for the use of graduated security criteria (initial planning envisions four different levels) ranging from low security to highly secure. HSPD-12 builds on the success of the Department of Defense (DOD) in moving to smart cards for physical and logical access to its facilities and networks. DOD has issued over five million smart cards (called Common Access Cards) to service personnel, retirees and contractors. The DOD model cannot simply be expanded for use by other agencies or the private sector (if nothing else, its use of a single data base for enrollment would be politically unacceptable), but it is precedential in demonstrating successful deployment of a robust authentication system based on smart cards.

Digital credentials are a new public service. Governments create identity documents for one purpose, but they are rapidly adopted by the private sector for other uses. Driver's licenses and social security numbers have become all-purpose identifiers. New government-issued digital credentials will be used in a similar fashion, probably as part of the process for obtaining a credential from a commercial authentication service provider.

Real ID

Requiring the verification and networking of government identity records (such as birth certificates or social security numbers) is essential for authentication. The Real ID Act, although deeply unpopular, addresses fundamental problems for authentication of identity in the United States. The Act requires the verification of documents presented to obtain a driver's license – many states had previously relied on what appeared to be a faith-based approach - and it accelerates the move by State and Federal agencies from paper to digital identity records.

Real ID was not the first (or perhaps the best) effort to solve these problems. The September 11 attacks revealed major flaws in the processes used to issue driver's licenses. The Intelligence Reform and Terrorism prevention Act (IRTPA) of 2004 implemented recommendations of the

9/11 Commission. Section 7212 required the Department of Transportation, in consultation with the Department of Homeland Security, to establish minimum standards for driver's licenses and personal ID cards issued by states that would be used to board domestic commercial aircraft and gain access to federal facilities. The standards required by IRTPA would have established what kind of documentation is needed to prove an applicant's identity; how those documents would be verified; and what safeguards would be used to prevent fraud. It specified the use of security features to ensure that driver's licenses and personal identification cards are resistant to tampering or counterfeiting. IRTPA's approach was preferred by state governments, but the Real ID Act repealed Section 7212.

The Real ID Act also sets certain minimum standards for the issuance of driver's licenses.[2] It creates standards for the establishment of identity (a photo ID, birth document, social security number, and proof of address and citizenship). More importantly, it requires the state to verify these documents before accepting them, including verification with the Social Security Administration that the SSN is valid and has not been used to issue another driver's license. This expansion of the enrollment process to include document verification is the most expensive element of the Real ID Act (Congress provided a tiny subsidy to the states to implement the Act), but is it also the most important. The ability to verify the documents used to assert identity is essential for creating trustworthy credentials. Even if the only effect of the Real ID Act is to reduce the use of fraudulent SSNs, it will be a major improvement.

For states to comply with the Real ID Act, they will also need to create and store digital images of the documents used to establish an identity and provide electronic access to these records for other states. This, combined with the requirement to use a common, machine-readable format for data, creates a network for national authentication. This requirement creates concerns among privacy advocates that there will be a single national database holding all citizens' 'personal' information. A more likely outcome is that there will be many government and commercial databases holding personal data, as there are now. What has changed is that searches of these databases will, in the future, be networked, not based on paper, and allow for digital searches.

New Technologies and Architectures

HSPD-12 and Real ID offer a foundation that technologies can use to create new authentication services for the new kind of Internet that is emerging. The phrase "Web 2.0" describes new Internet applications that are seeing growing use by companies and consumers around the world. In these web services, a user goes to a website and runs an application that is remotely hosted on the web services site's server computers rather than loaded onto the user's own desktop or laptop computer. The service uses data that is stored at the web service site. The bulk of the work in a transaction takes place over the Internet, offering large savings and greater security. Web 2.0 offers a new model for providing services over the Internet, but it requires strong authentication if it is to succeed.

One benefit of the limited success of PKI and digital signature laws was that it created incentives for new approaches to authentication that are more in tune with changes in how the Internet is

[2] The license is required to show name, date of birth, gender, address, and signature, incorporate tamper proof features, and use common, machine-readable technology using common data elements.

being reshaped. Developers realized that they would need to improve interoperability, security, and privacy in loosely coupled systems. This led to work that produced a number of identity management systems and protocols. These approaches include:

- **Shibboleth** is an initiative of Internet 2 – a consortium of universities that is developing new internet technologies. Shibboleth uses SAML (Security Assertion Markup Language) as set of rules on how information about identity should be exchanged and authenticated. Shibboleth provides for federated authentication (a certificate issued by one university can be accepted by another university) and has built-in privacy controls that allow users to decide how much information to share.

- **Kerberos** is another authentication protocol and was one of the first network authentication technologies to be developed. It is widely used. Kerberos uses a "key distribution center" – KDC – as a trusted third party who issues encrypted identifying "tickets" to users. The users can then use the tickets to authentications each other's assertion of identity. One of the attractions of Kerberos is that it allows for "single sign-on," which means that once a ticket has been issued by the KDC it can be used more than once and on different networks. Kerberos pre-dates Web 2.0 but it has been adopted for use by many of the new web services.

- **OpenID** also provides for single sign-on. OpenID piggybacks on the architecture of the Internet. An OpenID user registers with an "Identity Provider." Once they are registered, the user makes an assertion of identity to a site using OpenID by providing an Internet address to links back to the Open ID provider. This secure link confirms the identity assertion. Once an OpenID account is created with one identity provider, it can be used with any other website using OpenID.

- **Yadis** is a related protocol that also uses special web site addresses to obtain and confirm identity information (Yadis originally was an acronym for "Yet Another Decentralized Identity Interoperability System"). Yadis is a component of the OpenID initiative.

- **Higgins** is an open source project that began in 2003 that is supported by IBM and Novell. Higgins is intended to allow users to decide what information to share in different contexts (e.g. people share health information with a doctor, but not with a job search site) and uses. Higgins uses a framework that allows information from multiple sources to be shared in carefully controlled ways based on the underlying relationships. Higgins does not itself authenticate identity, but lets programmers write "plug-in" applications that can work with multiple, different authentication technologies.

- **CardSpace** is a Microsoft identity management system similar in process to Higgins. CardSpace allows a user to create digital identity cards, each of which contains a different amount of information about themselves. The user can then decide which card to use when they authenticate themselves with a website. CardSpace allows users to create an identity document for themselves and decide what information it should contain, or, for more valuable transactions, get an identity document issued by a trusted identity provider, such as a bank or other commercial service or governmental agency.

- **Liberty Alliance** is a standards-setting body for authentication technologies. Liberty has developed technical standards that allow different authentication technologies to interoperate. Liberty's Identity Assurance Framework (IAF) outlines policies and business rules against which identity services can be assessed for trust. Liberty has begun work on an Identity Governance Framework (IGF) that will use "trust frameworks" - rules on how a credential should be issued, verified and managed - to determine how much a credential can be trusted.

There are substantial differences among these technologies and architectures and they are in some ways competitors. None has universal acceptance. The common pattern with these technologies is that they offer greater precision and control in the use of personal data and greater acceptance of heterogeneity and the need for interoperability. Authentication protocols, like Higgins, OpenID and CardSpace, also extend the ability of users to control the release of their personal information as part of the authentication process. These new approaches to authentication provide the technological basis for progress, but they face the same set of policy-related problems that hampered PKI and the earlier generations of authentication technologies.

V: Next Steps for Better Online Authentication

There is powerful demand for better authentication, from both commercial enterprises and government agencies. At the same time, consumers want to be able to use a range of credentials, from those that provide little information to those that are tightly linked to other records. This demand, if the necessary policies can be put in place, should lead to a decisive expansion of online authentication services. The basis for this expansion will lie in the combination of improved technologies, greater commonality among commercial systems, and strengthened identity management by government. But the pace and scope of the expansion will be determined by how forthright both the government and the private sector are in approaching and resolving key issues discussed in this report: trust, interoperability, privacy, and liability.

The popular culture of the Internet has been based on pseudonyms and weak linkages between an online identity and the actual person. Weak Internet identification is one of the explanations for some of the Internet's most troubling aspects, such as cybercrime and feckless, ad hominem debate. However, anonymity is one tool people can use to try to protect their privacy. A lack of anonymity may have a chilling effect on discussion. The best digital identity system would preserve anonymity for some transactions and provide strong authentication of identity for others. A rigid approach to online authentication that does not provide a range of options to control personal information used for online activities will see consumers and citizens opt out, by limiting their participation or by choosing not to participate at all.

There will be legitimate instances when users will want their digital identities to be weakly linked, or not linked at all, to their legal identities. Whether this is good or bad is a separate discussion, but anonymity has always been prized for some transactions (as an essential guard for privacy, if nothing else) and this is unlikely to change. On the other hand, a system that provides anonymity and digital identifiers that are weakly linked to legal identities can have only a limited set of applications. No one will want to engage in valuable transactions on the basis of these identities, but until there is a way for relying parties (those who are on the receiving end of

a transaction) to distinguish between strongly linked credentials and weak credentials, a kind of Gresham's law for authentication will apply – the level of trust for all credentials will be no higher than the trust given to the weakest credential, since there is no way to tell them apart.

This makes for a very complex policy landscape. We want approaches to identity that can accommodate different technologies; that protect a user's personally identifiable information and privacy; and provides the option for strong linkages between digital identity and legal identity without the necessity of a new contract for each transaction. Essentially, we will want an authentication system that allows strangers to securely exchange trust when they choose to do so.

This will not be, however, a "Big Bang" event, where a single, large system appears in a very short time. Instead, the spread of strong authentication will be incremental and iterative, as the availability of trustworthy credentials leads to offerings of new services and applications, and as the appearance of desirable new services and applications increases demand for trustworthy credentials.

Nor will the growth of authentication process be centrally directed. Many different groups will need to finds ways to cooperate for authentication to work. The focus of this cooperation will be the development of uniform standards and protocols, both technical and policy, that can accommodate diversity. It is relatively easy for a recipient to know how much to trust a credential issued by his or her own system, but truly useful authentication will enable a recipient to know how much to trust a credential issued by an issuer who it may not know. There will be technological requirements for the exchange of trust among unknown systems, but the more important set of requirements involve the aspects of linking the digital assertion to the legal identity.

These requirements include the accuracy and verifiability of the government records upon with legal identity is based; transparency in how these documents are used to link the legal and digital identities; control by the user of how much of their legal identity is shared with a receiving party; and measure to mitigate risk for participants in any authentication system.

A Firm Basis for Assertion

No single process will be capable of addressing all the issues that currently slow an expansion of online authentication. However, there is a division of labor in the steps needed to accelerate authentication that could let several different processes simultaneously address issues. Some problems – core credentials – are best addressed by government. Other problems – liability – are best left to the market and the legal system. Cooperative processes with the private sector (but not necessarily excluding government participants) best address a third set of problems – policy standards for authentication. A final set of problems – those revolving around privacy protection – require input from consumers, lobbying groups, and the privacy community. Coordination of these disparate efforts will be difficult, but not impossible.

The first element, accuracy and verification of government records, requires action by governments. Turning paper into digital records is not enough. One way to accelerate authentication would be to make government records a web service. These records must be

searchable and verifiable over the Web. In this, government databases will need to mimic some of the techniques used by the large credit aggregators, who can provide access and searches to their databases over the Internet. The purposes of this search of government record can be constrained, to protect privacy, to a few simple queries: is this record accurate and still valid, and has it been used to confirm another identity.

To use the social security number as an example, when someone applies for a credential and provides their social security number, an online query could determine if the SSN was valid, if the person to whom it had been assigned was deceased, or it had been used for another credential. These validation queries need to be automatic. Requiring a human to manually search and confirm the validity of the SSN adds cost and the possibility of error. Although existing law makes it illegal to use the SSN as a credential, the number is often required because of its use as a unique identifier for financial services and taxation records. For the U.S., this makes the SSN one of the most important records for authentication. Other countries that, like the U.S., do not have national ID cards, use similar systems where citizens are issued a number for verifying assertions of identity that can be used to access social services and health care.

The ability to validate is not enough, however. A receiving party must know that the validation occurred, and be able to estimate the security of the validation process. The normal commercial solution to such problems is to use standards. A standard is a set of best practices that, if followed, will produce a uniform result. We use standards to assure the trustworthiness of many products, from simple fasteners to large, complex systems like aircraft. A standard for credentialing could be used to let a receiving party assess how strongly a digital identity was linked to a legal identity.

Neutral Standards

Standards generate positive network effects, in that the more people who use the standards, the greater the benefits for all users new and old. Standards improve efficiency. There are concerns that standards can reduce innovation. However, innovation often occurs around and on top of standards, such as the millions of innovative offerings on the Web that leverage HTML standards.

The best standards for authentication purposes would be “technology-neutral.” Technology neutral means that rules and processes accommodate many different technologies as long as they produce the same outcome. The experience with PKI and digital signatures shows the drawbacks of a prescriptive approach that requires the use of specific technologies.

A technology neutral, standards-based approach is attractive for several reasons. Standards can provide interoperability across applications and systems. They are scaleable to new authentication technologies (that meet the standards) as they appear. They can accommodate new approaches to identity management. A standards-bases approach is better suited to federation, as it provides a framework for many different authentication systems to cooperate.

Several existing groups could create these standards. Industry consortia and fora such as OASIS, Liberty, and W3C have joined traditional standard-setting organizations like the International Standards Organization (ISO) or, in the case of the U.S. government, the National Institute for

Standards and Technology (NIST) in the standards-making business. No single entity will dominate the authentications standards process, and the best approach might be to find ways to expand cooperation among different groups. Some problems that have major implications for the adoption of authentication systems, like privacy and liability, might even be best addressed by solutions already developed by other groups.

Privacy and Personal Data Protection

Better 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 the personal information used for enrollment and verification, the tracking of online activities, and the correlation of online credentials with other information. The rate of progress on privacy is one of the factors that will determine the rate at which stronger online authentication is adopted and used.

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.

Data is now much easier to acquire, store, and use than in the past. There has been a significant increase in the ability of commercial data aggregators – such as ChoicePoint, Lexis/Nexis, and Axciom – to compile massive databases of public records and other publicly available data on individuals. One such data aggregator reports $1 billion in sales each year to major corporate customers. It spends $50 million a year to collect data on consumer transactions; its records cover more than eighty percent of the U.S. population and its proprietary analytical software and powerful computers allow customers to mine this data for useful linkages and patterns.

Some new technologies, like OpenID, Higgins, or CardSpace, manage privacy concerns by allowing users to choose what they will share with a receiving party. These technologies allow the user to create a digital credential and decide how much personal information it should include. In other cases, the user may need to obtain a credential from a third party – their employer, a bank or identity service provider, or a government agency − in order to engage in a transaction.

There will also be instances in which the receiving party will demand extensive information in order for a transaction to occur. The intent might be to provide additional information to confirm an assertion of identity (and the need for this additional information should decrease as more trustworthy credentials become available). The real issue is what the receiving party does with the assertion of identity and its associated information; is it stored, is it linked to other data, and

it is sold to or shared with third parties without the consent of the person making the assertion? A relatively simple way to address this concern would be to link an authentication policy's standards to existing privacy safeguards. Existing privacy guidelines (like those produced by the Center for Democracy and Technology) and existing law (in the European Union or elsewhere) can form the basis of privacy protections that will mitigate risk.

Liability

Liability is a corollary of trust. Liability rules will determine the shape of both individual authentication systems and any federated approach to authentication. An assertion of identity or a credential is more trustworthy if I know that someone bears liability for an error, if a credential or assertion appears to be accurate and it turn out to be false. The attribution of liability reduces the risk of accepting a credential. Few companies are willing accept liability, however, and governments usually assume no liability for the credentials they issue. Uncertainty about liability is a major impediment to greater use of authentication. Liability can be assigned, of course, by written contracts between the parties to a transaction, but relying on a paper contract to engage in online authentication greatly restricts the scope and size of the opportunity for new kinds of transactions.

One way to assign liability in authentication is through precedent. Over time, as court cases are decided, a pattern of responsibility and limits on damages will emerge. This process is incremental and lengthy, however, decisions can vary from court to court, and the result of waiting for precedential decisions will be to slow the adoption of online authentication.

Legislation is the alternative to court decisions. Instead of letting case law solve the liability problem, legislative bodies could allocate liability and set limits on compensation. If the legislation gets it right, the market is accelerated. If it gets it wrong, the result will be to limit the size and scope of the market for authentication services in ways that harm innovation and economic growth.

A relevant example of legislation affecting liability is the Electronic Funds Transfer act of 1978, which limited consumer liability for unauthorized use of a credit card to $50.00. By setting the terms and requirements for liability, the Act had two effects: it encouraged consumers to make greater use of credit cards and (other forms of electronic payments), and it incentivized credit card companies to make major efforts to reduce the risk of unauthorized transactions. The companies pay for the losses above $50.00 by adding a small percentage to the interest fees that consumers pay.

Liability could be assigned by law for both consumers and service providers. Legislation to allocate liability for both users and issuers could blend existing practices, such as provisions similar to those that apply to credit cards. If liability is limited only for consumers, service providers will be unwilling to offer authentication, as the bulk of the risks would have been shifted to them. Legislation that limits liability for service providers, similar to statutes that limit the liability of airlines for loss or accidents, will be necessary. For transactions that are valued above the liability ceiling, the participants would need to acquire additional insurance or decide not to engage in an online transaction.

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

A third approach to liability is for participants in a transaction to buy insurance against error. Many mortgages in the United States come with title insurance. This insures the buyer against the risk that the title to the property being acquired is in some way flawed. This situation has many parallels to authentication, but insurance (like case law) requires a body of precedents that allow an insurer to estimate the risk of loss. This data is not available for authentication, and better estimates and data on authentication risks could help guide policies and rules that would expand the use of digital authentication.

As with authentication itself, there is not a one-size-fits-all solution to liability. High-value transactions will require different liability procedures than low-value transactions. Transactions involving credit cards may not need any additional effort to address liability at all. Reputational risk is minimal, and will diminish as better authentication increases the risk of detection for anonymous slander – why debate someone who will not give their name?

Similarly, authentication policy standards would need to acknowledge the liability issue. Liability is complex and shaped by legal precedent and commercial law. Credit card companies hold most of the liability found in current online transaction. If online services move beyond a reliance on credit cards as the primary vehicle for commercial transactions (and it is not clear that this will occur), other measures for handling liability may emerge. Some authentication service providers already offer warranties or other protections. Insurance products could be expanded to cover liability. These sorts of solutions to liability issues are probably best left to individuals and firms, and the best contribution of a policy standard might be a requirement for transparency to users and receiving parties regarding the liability protections offered as part of an authentication service.

Expanding Opportunity

Two words – luxuriant variety – describe the current status of authentication of identity. There are multiple credentials, technologies, agencies, companies, and rules involved in authentication. This is not going to change, but it can be made more orderly and dependable. Advances will come in incremental steps, as businesses and governments find viable ways to use better authentication for new or improved services.

Identity and authentication do not happen in isolation. They require context and relationships and a web of interactions among many participants. Technology alone cannot supply context and relationship. These must be assembled from a range of different interactions, each of which provides a piece of authenticated identity. The pieces needed for better authentication are present in a way that was not true a decade ago. Trial and error have helped to identify crucial

obstacles and suggest the means in which they can be overcome – including the development of new technologies that offer greater control of information and enable approaches to authentication that no longer assume that the same solution is needed for every transaction.

What is still lacking are the policy frameworks to join these pieces into trustworthy online identity systems that can win wide acceptance. These frameworks will eventually appear – but we can accelerate their appearance (and the benefits they will bring) by articulating a vision of what authentication and identity will look like, what needs to be done to achieve it, and who is best suited to do this. All of those who have a stake in authentication of online identity will need to play a part, or to be represented in the efforts to design effective policy frameworks.

In some ways, the steps outlined above for improving authentication are daunting. Progress will require coordinated action by multiple actors in the public and private sectors. We should not underestimate the complexity of this task. Policies that reduce the burden of building cooperation (such as opt-in approaches, where the unwilling are not required to participate, or open systems and standards, that accommodate different technologies) will speed improvement. The opportunities are real – improvements in government processes, new technologies and new private sector initiatives could be combined to create the range of authentication services needed to further exploit digital networks.

The amount of trust people will place in an authentication systems (and therefore the extent to which they will use it) depends first on the use of a secure technology. The degree of trust people place in an authentication system using a secure technology, however, will be determined by the transparency and robustness of the enrolment and credentialing process; the protections afforded to privacy; and the assignment of liability. The basis of this trust lies with government rules and services that provide a framework for commercial opportunity. Better rules and services from governments mean more economic opportunity and greater security for their citizens. In this case, the rules and services are those that let businesses, using new digital technologies, create a trustworthy online environment.

The knowledge that authentication of identity can fail creates an invisible ceiling for business and government. The risk of failure limits our ability to take full advantage of digital networks and the emerging web services that are based on them. "Closed" authentication systems – where the participants are bound to each other by some form of contract – are already widespread. "Open' authentication systems, where a token, credential or other identifier issued by one system can be used by another even if there is no contract or other prior agreement or knowledge between the two systems, are few and far between. The lack of open authentication systems creates significant opportunity costs – the lost or forgone chance to do better. The nations that can reduce these opportunity costs without damaging civil liberties will perform better in an increasingly competitive international economy.

The problems we began with were how to adapt paper identity and credentialing processes to digital and networked applications; how to increase interoperability among autonomous and heterogeneous authentication systems; and how to build trust in authentication and digital identity processes. The countries that can solve these problems, individually or jointly, will be better able to seize the opportunities of the digital age.