ANONYMITY AND ENCRYPTION IN INTERNET COMMERCE

Daniel J. Greenwood

Introduction

This Chapter deals with information practices issues affecting Internet commerce. Privacy, the topic of the previous section, lies at the core of these issues. Encryption and anonymity, this section's topic, [1] are two topic areas that relate directly to privacy and also to broader information practices issues.

The technologies implementing encryption can provide important tools to safeguard privacy and to assure information practices policies are reliable. In a sense, privacy can be understood as the result of anonymity. That is, when one is anonymous, then one has privacy. Authenticating a person by means of a user name, smart card or other form of digital identification, will restrict or preclude anonymity. Of course, one can use multiple identities (known as pseudonyms) and can employ other methods to create privacy. Encryption is a technology that scrambles digital information according to a code that allows authorized users to unscramble the data later. Encryption can be used to prevent others from perceiving what one is saying, doing or keeping electronically. This is another way to create a veil of privacy.

Though one's identity may be known (i.e.: one is not anonymous), one may still hold electronic documents and speech beyond the perception of others by using encryption. Anonymity and encryption can be used for some digital information, but not for other information, and they can be used in many interesting combinations. Anonymity and encryption are powerful tools to sculpt creative and tailored information practices and policies.

PART 1. ANONYMITY AND PSEUDONYMITY

Anonymity is being unknown or unacknowledged. Pseudonymity is being identified by an assumed (often pen) name. The use of authentication technologies to establish the identity of a person is incompatible with anonymity because it prevents the person from being unknown. There are legal consequences to being anonymous and to being authenticated or identified.

Identifying every user on a network is not always necessary. Perhaps an anecdote will help to illustrate this point. When I used to work as a lawyer in the state government of Massachusetts, we implemented the first known public sector credit card payment applications online for citizens to use on the Internet. The application allowed users to renew a vehicle registration, order custom "vanity" license plates and pay tickets. An important part of the reason these transactions were chosen was precisely because they did not require authentication of the identity of the user. A driver's license or change of address transaction, on the other hand, would require such authentication.

There was, of course, a possibility that the "wrong" person might conduct one of these transactions. In other words, person "A" could log onto the site and, appearing to be person "B", might attempt to conduct one of the transactions. My legal analysis of this scenario, under Massachusetts's law, was that person "B" would be guilty of providing a "gift" to person "A." My personal analysis was that I hoped person "B" would quickly and routinely log on to pay my own tickets -- under any identity s/he cared to affect. As the section of this chapter on encryption will make clear, it is generally not wise as a business or technical matter to utilize more or different security than is needed for a given application (it depletes resources, creates complexity and invites problems). It was primarily for these reasons that the Commonwealth of Massachusetts chose "anonymous" electronic transactions as its first eBusiness application.

Context Determines Desirability of Authentication or Anonymity

The above story illustrates a relatively simple example of a business choice to support anonymity and assume no special authentication of a user for an e-commerce application. The legal, business, technical and policy aspects of authentication or anonymity are often far less simple than the decision to allow unauthenticated renewal of a car registration. For example, at their thorniest, the issues parallel the classic struggles between national or corporate security and individual liberty. The needs for security usually require authentication of individuals and their activities while civil liberties, especially but not exclusively including privacy, often favor anonymity or pseudonymity.

More frequently, the question of anonymity and authentication arise in more mundane circumstances, such as merchants with web sites who seek to generate a commercial advantage by authenticating the identities of users based upon resale of the user's preferences to marketers. An individual user might find such authentication annoying (due to the additional screens, time and trouble of user name/password management) and the ensuing marketing communications may well be deemed meddlesome.

A more benign example of the use of authentication would involve the provider of interactive media who seeks to authenticate an individual user for the purpose of generating highly customized and personally relevant information and resources to that user. Such a user might desire this level of individual tailoring and thus tolerate the authentication procedure in order to access the service.

At best, authentication regimes are desired and required by both the user and the provider, in the same way a bank account holder would probably not use an ATM machine unless adequate authentication (like a debit card and a PIN) was required to prevent unauthorized users for withdrawing funds. More typically, authentication is simply required as a standard business risk control measure (as with employee log-in to company computer networks). At worst, authentication measures are undesired and/or unknown by the users (as when browser cookies identify what sites an Internet surfer visits and when that users personal information is later sold).

When Anonymity is Bad: Anonymity as Accountability Avoidance

There are some who believe that anonymity is little more than a method of avoiding responsibility for one's actions. Any number of laws, regulations and corporate policies require identification of people as a necessary part of a transaction. U.S. Supreme Court Justice Scalia, in a dissenting opinion which struck down a law prohibiting anonymous political pamphleting, made perhaps the clearest and most succinct case against anonymity. Scalia wrote that anonymity:

> ". . . facilitates wrong by eliminating accountability, which is ordinarily the very purpose of the anonymity. . . to strike down the Ohio law in its general application--and similar laws of 49 other States and the Federal Government--on the ground that all anonymous communication is in our society traditionally sacrosanct, seems to me a distortion of the past that will lead to a coarsening of the future. I respectfully dissent.[2]"

There appears to be relevant research in the social sciences to confirm Justice Scalia's viewpoint. Evidently, anonymity and merging of one's self into a group has been correlated to an increase in course, and even brutal, behaviors. In an article presented at the Annual Conference of the European Institute for Computer Anti-Virus Research, Dr. Kabay of the International Computer Security Association put forth an impressive compilation of studies tending to show a link between anonymity and anti-social conduct.[3] Dr. Kabay overviews the potential harms associated with anonymity in this way:

> In general, the findings are not encouraging for the future of cyberspace unless we can somehow avoid the known association of antisocial behaviour and anonymity. Early work on people in groups focused on anonymity as a root of the perceived frequency of antisocial behaviour (Le Bon, 1896). The anonymous members of a crowd show reduced inhibition of anti-social and reckless, impulsive behaviour. They are subject to increased irritability and suggestibility. One wonders if the well-known incidence of *flaming* (rude and largely *ad hominem* communications through e-mail and postings on the Usenet and other public areas may be traceable to the same factors that influence crowd behaviour. Later social psychologists formulated a theory of deindividuation (Festinger et al., 1952) in which they proposed that one's personal sense of identity can be overwhelmed by the sense of belonging to a group. Zimbardo (1970) suggested that anonymity, diffusion of responsibility and arousal contributed to deindividuation and antisociality. He noted that deindividuated people display reduced inhibitions, reduced reliance on internal standards that normally qualify their behaviour, and little self-awareness. . . . Writers of computer viruses and others in the criminal computer underground may also focus so intensely on the challenge of defeating machines that they lose sight of their human victims. Criminal hackers have expressed themselves as attacking systems, not people. . .

Dr. Kabay also points to studies that show people who are anonymous tend to behave dishonestly, are more likely to be violent towards others, and suggests that the behavior of hackers acting as unidentified network users may in fact be "relatively normal people responding in predictable ways to the absence of stable identification and identity.[4]"

When Anonymity is Good: Anonymity as a Core Value, Like Privacy

Set against the view that anonymous communications and conduct in an electronic environment is presumptively negative, exists the widely held conviction that ensuring anonymous and pseudonymous transactions is among the most pressing needs of our time. For example, the Privacy Commission recently commissioned by the FTC reported that the United States is in urgent need of allowing anonymity for Internet transactions as a method of assuring privacy[5]. Roger Clarke, Visiting Fellow at the Department of Computer Science, Australian National University, put forward a crisp viewpoint in support of assuring protection of the right to anonymity. In his paper "Identified, Anonymous and Pseudonymous Transactions: The Spectrum of Choice", Clarke argued that there are two critically important policy imperatives of the next hundred years:[6]:

Policy Imperative No. 1

- maximise the use of **anonymous transactions**, and **resist and reverse conversion** of anonymous to identified transactions
- maximise the use of **pseudonymous transactions**, where anonymity is not an effective option
- preclude **identified transactions** except where it is functionally necessary, or where meaningful, informed consent exists

Policy Imperative No. 2

- enable **multiple identities** for multiple roles
- enable the **authentication of pseudonyms**
- provide **legal, organisational and technical protections** against access to the link between a pseudonym and the person behind it
- resist and reverse **multiple usage of identifiers**
- resist and reverse the **correlation of identifiers**

[emphasis in original text]

The first of these imperatives would deny the increasingly common assumption by governments and corporations that individuals should be authenticated as a matter of course. The point of view put forward in this policy imperative is that the default assumption should be that people need not be individually authenticated. Rather, authentication should occur only where necessary. The second policy imperative indicates the need to respect the use of multiple pseudonyms. In general, today, people are not legally restricted from using an alias or pseudonym, unless they do so for the purpose of defrauding or committing some other illegal act. Increasingly, however, organizations are requiring individuals to use a single legal name and a government issued or other valid identification. The policy imperatives, read together, strongly seek the reversal of this trend and demand a continuation of the current legal rule that use of multiple identities is valid.

Applying Legal Precedents on Anonymity to Interactive Media Environments

Federal and state statutes, regulations and case law recognize various situations in which anonymity or pseudonymity is either protected or prohibited. The legal precedents discussed below can provide some guidance, directly or indirectly, to counsel, businesspersons and technologists who seek to understand whether, how and how much anonymity may be desirable for any given electronic transaction or set of transactions.

The right to freedom of expression has also generated legal precedents protecting anonymity. For example, individuals may anonymously make political expressions relating to an election in the form of pamphlets[7]. Anonymous campaign literature is an important component to a free society because it assures all citizens the opportunity to add to the marketplace of ideas without fear of reprisal by employers or others. At election time in the future, will there be facilities or other technical functions that permit users of computer networks to express political ideas anonymously? On the other hand, it has also been held that requiring an identification badge is permissible for vendors selling periodicals on streets and in other public areas[8]. Such a bade or permit requirement makes sense as a matter of urban planning and assuring efficient traffic and pedestrian flows. This precedent also shows how a court may be less willing to grant anonymity for commercial sales and more likely for speech generally. However, the right of publishers, printers and distributors generally to maintain anonymity has been held to be an important part of press freedom[9]

Perhaps the strongest case in support of anonymous speech is Talley v. California [362 U.S. 60 [4 L.Ed.2d 559, 80 S.Ct. 536]. Talley explicitly establishes that the First Amendment right of freedom of speech includes the right to remain anonymous. In Talley, the U.S. Supreme Court reviewed a Los Angeles city ordinance prohibiting distribution of any handbill unless it had the name and address of the person who produced it and who caused it to be distributed were printed on the document. In the words of the court:

> Anonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind. Persecuted groups and sects from time to time throughout history have been able to criticize oppressive practices and laws either anonymously or not at all. . . . The old seditious libel cases in England show the lengths to which government had to go to find out who was responsible for books that were obnoxious to the rules. . . . Even the Federalist Papers, written in favor of the adoption of our Constitution, were published under fictitious names. It is plain that anonymity has sometimes been assumed for the most constructive purposes." (*Id.* at pp. 64-65 [4 L.Ed.2d at pp. 562-563].

This language reflects the importance given to anonymity be the judiciary. This point of view is not afforded only to verbal speech and ideas printed on paper. Rather, courts have been willing to apply protection of anonymity to encompass various media, including telephone answering machines[10].

In the business world, the transfer of money out of a checking, savings or investment account is the best example of a transaction that requires, for business and legal reasons, authentication. As suggested earlier in this section, account holders and financial institutions alike share a desire to prevent unauthorized usage of a customer account. In response to this, and to avoid money laundering that is associated with anonymous or insufficiently identified bank account holders, financial institutions have developed "Know Your Customer" programs[11]. More formal "know your customer" rules[12] for financial institutions were proposed[13] to reduce, identify and prosecute illegal financial acts[14]. These proposed rules spawned vigorous criticism and debate[15] and were finally withdrawn[16]. Though one may assume that financial transfers by their very nature require individual authentication in all cases to protect the sensitivity and value of the transaction, there are in fact many applications for anonymous money (like cash). Similarly, as with any other transaction, a simple cost/benefit and risk analysis is required to determine the levels at which authentication may be needed.

Another federal agency that has embarked upon a "know your customer" initiative is the Bureau of Export Administration (BEX) of the U.S. Department of Commerce[17]. Certain provisions in the Export Administration Regulations (EAR) require an exporter to submit an individual validated license application if the exporter "knows" that an export that is otherwise exempt from the validated licensing requirements is for end-uses involving nuclear, chemical, and biological weapons (CBW), or related missile delivery systems, in named destinations listed in the regulations. The details of encryption export are dealt with elsewhere in this book, but in this context, it is interesting to point out that authentication (and not anonymity) is required for end-users. Beyond knowing the named identity of a buyer of certain goods, exporters must also know a great deal about exactly what uses to which the goods will be put and where the goods will end up. The BEX "Know Your Customer Guidance" gives a variety of circumstances for exporters to monitor and which may indicate an

inappropriate end-use, end-user, or destination for their goods[18].

Outside of the mercantile worlds of export and banking, the controversy between anonymity and authentication has generated no shortage of litigation. For example, numerous medical conditions involving social stigma or religious doctrine have raised legal claims for anonymity[19]. Individuals making requests for public information under the Freedom of Information Act are not entitled to learn the identity of confidential informants to the government[20]. It is typical for the law to protect the right of individuals to be anonymous with respect to these types of issues. Another situation in which the need for anonymity is frequently invoked involves police informants. In this situation, the law must balance the rights to a fair trial and to confront an accuser with the competing public policy need to encourage citizens to cooperate with police[21]. A creative precedent for handling this tension can be for a judge to interview the informer directly, and make the resulting information available to all parties, without revealing the identity of the informant [22]. One can imagine various ways to use a judge or other magistrate for this type of purpose in the context of electronic communications.

In the context of public trials, there are a series of cases which weigh the need for open and transparent courts versus the need to protect the privacy and other constitutional rights of certain parties to litigation. In these situations, a litigant may seek to proceed as John or Jane Doe, rather than identify themselves on the pleadings or other court documents, including situations protecting the identity of children, religious and racial minorities seeking to uphold their rights, and persons with medical and psychological disabilities[23] . The mere claim of discrimination based upon gender, however, was not held to be sufficiently important to outweigh the broader interest in open trails[24]. Similarly, to preserve the right of financial privacy, certain proceeding before a federal Tax Court may be closed to the public[25].

Children's identities are protected under the law well beyond the context of public trials, including in the electronic arena. For example, the Children's Online Privacy Protection Act and accompanying rules[26] prohibit unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the Internet.

OSHA rules require particular responses by employers to reports of hazardous conditions in the workplace which require inspections (hence possible business disruption). Employers must permit employees to file these reports anonymously[27]. This is an example of the law finding that the general societal good of assuring safe workplaces requires protecting the anonymity of individuals. One can imagine analogous situation occurring on office networks and extra-nets, where employees file these or other societally important information anonymously. In these types of situations, it would not make sense to require full individual authentication of every employee on a business network at all times. Rather, under particular scenarios, there may even be a role for anonymous communication even within the intranet of a corporation.

In the legal area of reproductive issues, there are several examples of legal rules protecting anonymity of individuals involved with the adoption and the abortion processes. Under the U.S. Code, the Attorney General of the United States must pay for up to two anonymous test for sexually transmitted diseases for victims of rape[28]. Understandably, the protection of anonymity given to victims of sexual assault are forcefully taken from perpetrators. The judiciary has upheld statutes for registration and community notification of convicted sex offenders[29].

Georgia Anti-Mask statute was not held to violate the right to freedom of association in litigation by members of the Ku Klux Klan[30] . The court found that the interests of Klan members in remaining anonymous while engaged in intimidating or threatening mask wearing behavior was counterbalanced by the general public interest of general public interest in protecting citizens from violence and intimidation.

The Purpose of Legal Precedents on Anonymity

These examples of situations, in some cases, bear directly upon the set up of electronic transactions system. For example, the need to identify the citizenship and location of users who download certain encryption software applies directly to encryption companies. In other situations, the legal rules can be applied only by analogy. For example, it is possible that the legal precedent against the wearing of a mask for the purpose of intimidating another person could be interpreted to apply to the masking of an IP address with mal-intent. In general, the above listing is intended to point toward examples of circumstances where society has deemed identity or anonymity to be important. It is up to the bar and the rest of the information society to apply these principles to cyberspace over time.

PART II. ENCRYPTION AND AUTHENTICATION

This Part is intended for readers wishing a deeper understanding of what encryption is, how it works and business applications for its use. Encryption can be explained as:

> The translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text ; encrypted data is referred to as cipher text. There are two main types of encryption: asymmetric encryption (also called public-key encryption) and symmetric encryption.[31]

Encryption can be used to assure that data remains confidential or secret by making it impossible for parties without the proper codes necessary to utilize decryption mechanisms to access the data. Much of the work of information practices is concerned with implementing methods to control access to data according to authorization. Encryption is the most important tool for restricting digital information for such purposes.

Encryption for Authentication

Encryption can also be used to facilitate determination of the identity of a party for the purpose of establishing whether that party is authorized to access data. For example, if a particular web site requires a user name and password in order to access certain information or resources, then it is good practice to assure that the communications channel between the user and the system is encrypted when the password is transmitted. This is because the Internet is not a secure network and it is possible that unauthorized persons will intercept the password and will later impersonate the authorized user. This is, however, only one simple way that encryption can be used to facilitate the determination of identity. When combined with other technologies and appropriate business practices and models, it is also possible to use asymmetric encryption, also known as public key cryptography, to create a digital signature that can provide a high degree of certainty as to the identity of the signer. In this way, use of encryption can be tightly associated with the process of identification or with continued anonymity of an individual.

Electronic Signatures

An electronic signature is:

> an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record.[32]

There are many ways to create an electronic signature. These can range from simple methods, such as typing a name at the bottom of an e-mail message, to more complex and secure methods involving biometric technologies, such as fingerprint or retinal scans. Other types of authentication methods that are used to create electronic signatures include the use of magnetic stripe cards and PIN numbers, user names and passwords, public key cryptography, writing tablets with electronic pens, or even smart cards that generate a unique access code every few seconds. As technology advances, the list of viable alternatives is certain to grow.

Because there are so many ways to create an electronic signature, and because many of them do not resemble a holographic "autograph," some law reform efforts have adopted the term "authentication" rather than "signature." [33] However, it is currently best practice to use the word “sign” to indicate something a user does to identify himself or to manifest assent, and the word “authenticate” to indicate something the receiver of a signature would do to validate that the signature is genuine. It can be said that one authenticates a signature when

that signature is checked.

One of the most interesting and robust technologies being used and developed for authentication purposes is known as public key cryptography, which allows for a very high degree of reliability when implemented properly. A "digital signature" does not refer to the image of a signature in any way. Unlike an "electronic signature" which is simply any symbol or process intended to be a signature and a "digitized signature" which refers to an electronic image of a signature, a "digital signature" is actually a term of art that refers to the scrambling of data in order to provide security and authentication. The term “electronic signature” is the overarching concept, and does not indicate any particular technology. The term “digital signature” is a term of art which denotes use of public key cryptography (though these terms are not infrequently used interchangeably in the popular media).

While the technical details of public key cryptography are extremely complex and have limited utility to a broader audience, an understanding of the basic concepts is both accessible and useful. Due to the current interest in deploying large-scale public key systems, it is likely that this technology will touch many areas of the economy. In fact, the growth of public key systems in many sectors of the economy suggests that a rudimentary knowledge of these concepts will serve lawyers well when legal questions arise as a result of this technology[34].

The Basics of Public Key Cryptography

Codes and cryptography are thousands of years old. Although cryptography became much more sophisticated in modern times, its core still depended upon the sender and the receiver knowing the same "secret key" to encode and then decode messages. To be secure, a secret key coding system requires some method for distributing the secret key to intended users without it falling into the hands of other parties.

The basic nature of the Internet makes it poorly suited for a secret key system because it is an "open" network in which messages may make several "stops" before arriving at their final destination. This creates a serious risk that a third party could intercept a secret key at some point along its routing, which would allow him to read encoded messages or even send coded messages purporting to be from an authorized holder of the secret key. Physically delivering a secret key to every user by secure channels would be slow, expensive and unwieldy. Furthermore, physical distribution would effectively rule out serendipitous or one-time transactions between people and firms that have not previously exchanged secret keys. While this property of public key cryptography is intriguing, current business models, especially B2B models, already utilize secure channels which can be leveraged to swap authentication mechanisms (such as PINs and other secrets).

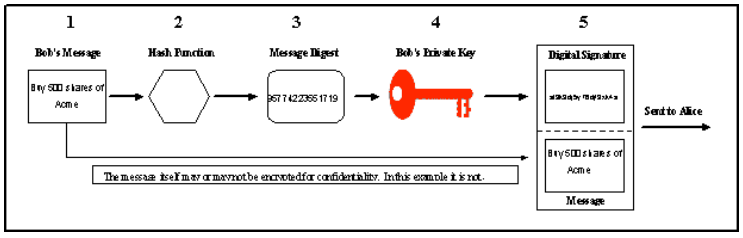
The cost of adopting a public key system may not be appropriate where other alternatives are suitable. More to the point, since most business channels do not rely upon or require serendipitous or one-time transactions, it is becoming obvious that this property of public key cryptography is a solution without a problem for most situations. In the future, as new business channels emerge, it is possible that this property of public key cryptography will be more important to more people and businesses. For the moment, the costs of creating the infrastructure necessary for strangers to trust one another based upon a technology appears beyond reach. Rather, it will be necessary for business relationships to develop over time whereby the risk is born by responsible parties who not only facilitate stranger to stranger transactions – but who also stand behind them. Alliances, insurance, bonding, membership organizations and many other models are emerging. One thing seems clear: no matter how interesting a property of technology may be, technology alone is not sufficient to create trust and to manage risk.

Where public key cryptography is used, it eliminates the need for users to share a secret key, which makes it ideally suited for communications over "open" networks such as the Internet. While the following illustration describes a complex process, the hardware and software that implements this technology will shield the end user from these details. Moreover, end users will find no need to concern themselves with the complicated background operations that make the system possible.

With a public key system, each user will have software that will generate two related keys known as the public key and the private key. The fundamental characteristic of these key pairs is that the public key, and only that public key, can decrypt a message encrypted with its corresponding private key. Similarly, the private key, and only that private key, can decrypt a message encrypted with its corresponding public key. As such, these key pairs are analogous to secret decoder rings from a box of cereal, where each ring fits into its companion ring and no other.[35]

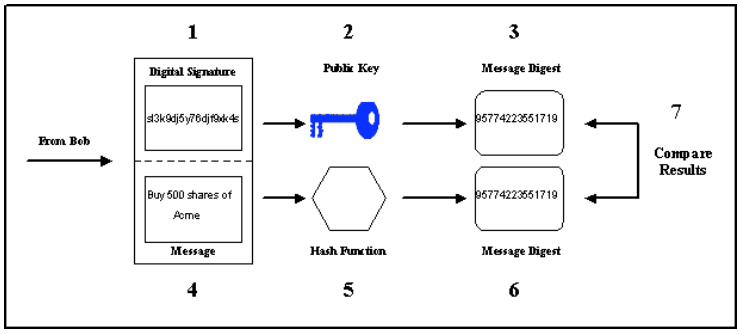
Once Bob, a user, has generated his public/private key pair with a computer, he keeps his private key very secure (protected by a password on his computer or, preferably, a smart card locked in a safe) but he makes his public key freely available by sending it to people or by posting it to a public key directory on the Internet. Then, if Alice, another user, wants to send Bob a private message she can obtain Bob’s public key and use it to encrypt the message. Since only Bob’s private key can decrypt a message that has been encrypted with his public key, both Alice and Bob can be sure that only Bob can read the message. Thus, public key cryptography allows two people to send secure messages without the need to exchange a secret key through a secure channel. Only Bob’s public key needs to be shared in order for Bob to receive completely secure messages.

This unique characteristic of public key cryptography also forms the basis for secure digital signatures. This process is illustrated in the diagram below. In order to generate a digital signature, Bob must first have a message (1) that he wants to sign and send to Alice. The message could be as simple as an e-mail message or as complicated as a lengthy contract. Bob would then run his communication to Alice through one of several standard algorithms known as hash functions (2) that performs a series of mathematical operations on the original message. The hash function produces a number called a message digest (3), which can be thought of as a fingerprint of the message, because any change in the message, no matter how slight, will cause the hash function to produce a completely different message digest. Bob then encrypts the message digest with his private key (4). The message digest encrypted with Bob’s private key forms the actual digital signature for the message.[36] Finally, Bob transmits both the digital signature and his original message to Alice (5). If Bob also wants to keep his message to Alice confidential, he could encrypt the message using Alice’s public key (not shown).



Upon receipt, Alice’s computer and software would perform two separate operations to verify Bob’s identity and to determine if the message had been altered in transit. As a practical matter it is not important which operation is performed first.[37] To verify Bob’s identity, Alice’s system would take Bob’s digital signature (1) and then use Bob’s public key (2) to decrypt the digital signature, which will produce the message digest (3). If this operation is successful, Alice knows for a fact that Bob, who alone has access to his private key, must have sent the message.

In order to ensure that Bob’s message had not been altered in transit, Alice would run Bob’s message (4) through the same hash function (5) that Bob used, which would yield a message digest of Bob’s message (6). Alice would then compare the two-message digests (7), and if they were the same she would know for a fact that the message had not been altered in transit.



Thus, public key cryptography allows people and businesses to exchange messages over open networks with a high degree of confidence that those messages are confidential (unable to be read by unauthorized persons), authentic (sender's identity can be verified), and of high data integrity (the message can not be altered without detection). This is a level of security far greater than that afforded by ink signatures.

However, nothing said thus far would rule out the possibility that an impostor could generate a public/private key pair and then post the public key on the Internet claiming it belongs to Bob. Unaware of the deception, Alice might then use this public key to send messages that the impostor, but not Bob, could read. The impostor could also use the falsely identified private key to digitally sign messages that Alice would assume Bob sent because they can be decoded using the public key which Alice does not yet realize is fraudulent. In order to prevent this, the parties relying on digital signatures must have confidence that the public key on the Internet that purports to belong to Bob is, in fact, owned by him.

One proposed approach to handle this practical problem was been to rely upon a trusted third party known as a certification authority (CA), which binds the identity of a particular party to a particular public key and, by implication, a particular private key. What follows is a typical explanation of how this trusted third party CA model is envisioned to operate.

CAs would bind the identity of a party to a public key by issuing a digital certificate. A digital certificate is a small electronic record that (i) identifies the CA issuing it, (ii) identifies the subscriber, (iii) contains the subscriber's public key, and (iv) is digitally signed with the CA's private key. The digital certificate can also contain additional information, including a reliance limit or a reference to the CA's "certification practice statement" that gives relying parties notice of the level of inquiry conducted by the CA before issuing the certificate.

To obtain a digital certificate, Bob would present the CA with a copy of his public key along with sufficient proof of his identity. For digital certificates that could be used for larger transactions, the CA might charge a higher fee and require greater proof of identity. Once satisfied as to the identity of the subscriber, the CA would issue the subscriber a digital certificate. When Bob wants to use his digital signature, he would also transmit a copy of his digital certificate to Alice. In addition to the steps described above, when Alice's computer receives Bob's message, it also confirms with the CA identified in the digital certificate that Bob is who he purports to be and that his certificate has not expired or been revoked. If Bob learns or fears that his private key has been compromised, he would notify his CA of this fact so that it could post that information to its "certificate revocation list" (CRL) or, perhaps, by reference to an online check of a database using a certificate checking protocol. All of this activity would take place in the background, unseen and unnoticed by Alice, and would happen in much the same way as it occurs with online credit card validation systems.

Different Models, Implementations and Approaches

There are many different models for the use of public key cryptography that do not assume or require a CA, including the implementations known as PGP (Pretty Good Privacy), which uses a "web of trust" wherein users vouch for each other (Abe know Betty and Cathy and introduced them to each other). Another non-CA system is know as AADS (Account Authority Digital Signature) which simply binds a public key with a user account number. Banks and other institutions that primarily refer to user identities by account might find this system efficient and useful. Neither PGP nor AADS require certificates.

The use of current certificate technologies (which rely upon the standard X.509 version 3 digital certificates) are difficult to set up, manage, use and upgrade. The Commonwealth of Massachusetts has published a detailed review of the experience of a five state e-commerce pilot in which certificates were used to identify individual buyers of supplies. Massachusetts, New York, Idaho, Texas and Utah participated in the pilot, known as the Multi-State Emall. Continued use of digital certificates and the trusted third party CA model was not recommended[38].

Beyond the business problems with current digital certificates, there are also privacy problems. In his book, Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy, Stefan A. Brands discusses the fact that a single digital certificate can be used to track the same user across many different transactions, and thereby link personally identifiable information to many different databases and other stores of information[39]. The book offers a detailed alternative approach that would allow individuals to use smaller "cryptographic building blocks" that give the certificate holder control over what information is disclosed and to whom.

One of the major unanswered questions about the use of public key cryptography for digital signatures, and a major point of contention between advocates of different types of electronic signature laws, relates to the business model for CA services that will ultimately prevail in the marketplace. A Public Key Infrastructure (PKI) would need to evolve to support use of this technology utilizing a trusted third party CA[40]. While advances in technology will certainly create new possibilities not presently contemplated, the two primary business models currently vying for support are known as the "open PKI" and "closed PKI" models.

An open PKI model assumes that subscribers will obtain a digital certificate from a CA that will securely link their identity to their public key for all, or at least many, purposes. Thus, in an open PKI environment a person could obtain a digital certificate and then use it to order goods online from various merchants, sign legally binding agreements, or even file documents with a government entity. Subscribers could use their certificate for any transaction requiring a digital signature. In the closed PKI model, users would obtain a different digital certificate for each community of interests with which they interact online. For example, a user could have one certificate for transactions with their bank, a different certificate for communications with their employer, and yet another certificate for dealings with their health care provider.

The difference between the two models is significant. Under an open PKI model, a person's certificate could potentially be used to sign any document, which makes the consequences extremely severe if the user's private key is compromised. In a closed PKI, on the other hand, the risks to the user and the CA from an improperly signed document are more limited due to the system's more narrowly defined scope. Furthermore, the members of a particular community within a closed PKI system may enter into agreements that define the rights and responsibilities of the members, which would further reduce the risks and uncertainty in such a system.

The above mentioned Multi-State Emall used a closed system in which all parties agreed by contract in advance to the same set of operating rules and conventions for the use of technology. The use of a set of operating rules, whereby multiple parties can opt into a secure and enforceable community of trade or other transactions is becoming the norm. Like trading partner agreements that supported Electronic Data Interchange, these newer sets of Operating Rules are becoming more standard methods of managing risk and trust for transactions over the Internet[41].

It is becoming clearer from a business perspective, that the most important question does not revolve around the public key infrastructure, but around the business, legal, policy and cultural infrastructures upon which use of technology must rest. That is, use of public key technologies are best applied in a tailored manner to suit the needs of the business and practical requirements of parties. It is unreasonable to expect parties to contort their business relationships to meet the unnecessary and costly structure of a public key infrastructure, rather than to simply purchase technologies that support and reflect their real business needs.

So called "digital signature laws", like the statutes in effect in the states of Utah and Washington, exist to support a public key infrastructure and a trusted third party CA.[42] In the mid 1990's, there was considerable interest in enacting this type of law for the purpose of facilitating electronic commerce. The policy consensus quickly swayed against these types of laws because they enshrined a particular technology and business model into law and distorted the otherwise competitive marketplace for different technologies and approaches. Most states have opted to enact "electronic signature" statutes, and a majority of states have further harmonized laws around the Uniform Electronic Transactions Act.[43] This approach assures that any technology parties choose to use can be sufficient to create a valid signature or record. The U.S. Congress has also reflected this policy in the Electronic Signatures in

Global and National Commerce Act, passed in the year 2000[44].

Non-PKI Technology: The Importance of Maintaining Options

Given that the acronym "PKI" assumes the use of a trusted third party business model, it should be mentioned that several implementations of public key technologies exist which do not assume the same model. AADS and PGP were already identified as non-certificate implementations. In addition, these implementations do not require a trusted third party. The SPKI (Simple Public Key Infrastructure)[45] standard can also be used without the need of a trusted third party. Finally, when all the parties who use a set of public key technologies sign contracts with one another or otherwise agree to a set of operating rules to define their rights and responsibilities vis each other, then no trusted third party is needed. Use of public key technologies within a single institution (as between employees) would also obviate the need for a trusted third party.

In addition to various implementations of public key technologies, there are also a number of non-public key technologies that exist in order to achieve electronic authentication. Mainstream authentication technologies include: Keberos, Passwords and PINs (including one-time PINs), Radius implementations, Virtual Private Networks (to create secure sessions), smart cards, cards with information on a magnetic strip, biometric technologies and challenges based on knowledge (such as the maiden name of the user's mother). It can be said that authentication technologies all fall into one or more of three categories: something you know (like a password); something you have (like an ATM card) and something you are (like a finger print or retinal scan).

One very interesting technology is known as Signature Dynamics. It is a mechanism for the secure capture, management and verification of handwritten signatures by electronic means. PenOp[46] has been the most well known company that implements Signature Dynamics. Signature Dynamics captures signatures simply and reliably, and enables them to be securely stored and safely transported between different systems. For evidentiary purposes, Signature Dynamics can verify the authenticity of the transaction on which signatures were executed. Signature Dynamics can also verify the authenticity of the signature on the document with an accuracy and speed unparalleled in the paper domain. In so doing, this technology provides evidence that is relevant to regulatory and legal requirements for handwritten signatures.

For the signatory, Signature Dynamic's major attraction is the familiarity of submitting their normal handwritten signature - using a pen (or, for devices like a Palm Pilot, using a stylus). For corporate users, the main benefit is that they can complete business processes electronically, achieving major cost savings by reducing the need for paper. It is also worth noting that Signature Dynamics removes the need for passwords and PINs, public/private key pairs or certificates. The state of California was the first to recognize the technology known as signature dynamics in law. The Californian regulations on use of digital signatures with government provide a helpful definition and contextualization of this technology.[47]

In addition to encryption and Signature Dynamics, biometric technologies can also be used. Biometric technology can be defined as:

> Generally, the study of measurable biological characteristics. In computer security, biometrics refers to authentication techniques that rely on measurable physical characteristics that can be automatically checked. Examples include computer analysis of fingerprints or speech.[48]

Biometrics can be used to establish the identity of a given party and encryption should be used to secure a communications channel over which the biometric data is flowing to prevent a so-called "man in the middle" attack. Such an attack would involve an unauthorized third party intercepting the data that reflect the biometric measure (e.g.: the voice print or retinal scan) and copying the data to be used for later impersonation. Using encryption between the biometric measurement device (e.g.: the finger print reader or facial recognition camera) and the end authentication database would help to defend against such an attack.

While use of such technologies as biometrics on the surface appear to directly defeat the cause of privacy and anonymity, there are situations in which authentication is necessary to assure confidentiality of information. For example, to assure that a person's medical records can only be accessed by authorized individuals, a strong system of authentication and authorization must be implemented. The same biometric technologies that pose the ultimate threat to a person's privacy can also be used in such a way as to assure privacy. This conundrum exists among all authentication technologies, but is most pronounced with biometric data, because such data literally and unambiguously links to a particular person.

There are many other objections to the use of biometric systems, but the most interesting critique is that once such an authentication device is compromised, it can be impossible to continue using the technology. This is because, unlike with a password which can be re—issued once compromised, a person will quickly and permanently run out of fingers and other biometric data sources. The DNA of a person (the ultimate biometric) can only be compromised once before irreparable harm has occurred. Nonetheless, since biometric authentication is possibly the best source of individual identification, it is a good bet that this technology will continue to evolve and be ever more useful in business transactions.

Determining Whether, Which and How Much Authentication is Needed

Much of the talk related to security and encryption revolves around creating "trust" or "trust management" systems[49]. The intellectual underpinnings of Public Key Infrastructure schemes are premised upon the concept of "trust management". This notion is wrong. The practical and technical requirement is to manage risk, not trust. Technologies must serve the goal of managing transactional and structural risk and should be judged by how well they achieve that goal. The single best paper on this topic comes from the indomitable Dan Geer, who presented this concept and a paper in 1998 to the Digital Commerce Society of Boston[50].

It is important for counsel to understand that various technologies and approaches exist to meet the authentication and confidentiality needs of an organization or other client. It is not an overstatement to say that legal requirements drive the perceived need for most security and authentication technology purchases. Whether there is a statutory requirement for a signature, fear of liability for lack of authentication or any of a wide variety of other legal needs, it is the law that stands as the source of most technical requirements in this area. Ascertaining the actual legal and business requirements for a given transaction or set of transactions is a necessary pre-requisite to providing counsel on the adequacy - or overkill - of any given proposed technology or application for authentication and encryption.

Before a counsel can assess whether or how much technical authentication or encryption is needed for a given web site or other multi-media resource, a more basic analysis of security and authentication needs for individual transaction must be undertaken. Basic judgments about security and authentication must be made by the counsel and communicated to the technical and business persons responsible for implementing encryption and authentication processes. In determining whether a given security need exists, counsel should consider questions like: how is this process implemented today in paper?; does it require a signature?; is there a statute or regulation that requires privacy or confidentiality or individual identification?; is this an area where there has been litigation or other disputes in the past – if so, what are the problems and how do they relate to the online system?; how much financial or other legal liability exposure is there for the parties if there is a problem with this transaction?.

The Security and Authentication Requirements Matrix below provides a general method for analyzing legal information security needs. This matrix is not intended as a complete solution, but rather an a general model for approaching analysis of these issues.

The left column lists categories of transactions that clearly implicate different legal arenas. Across the right columns are security requirements broken into three levels: Network, Document and Application. To make use of the matrix, a company would first determine which characteristics apply to its particular application. Then, reading across the right, companies would check off appropriate security requirements for each of the application characteristics that apply. It is important to note that application characteristics are broken out to assist counsel in targeting security solutions specifically to the part of the application where such solutions are required.

Security solutions can be costly, time-consuming and resource intensive and should therefore be matched closely to actual application needs. It is important to avoid requiring too little security, but it may be even more important to avoid heaping on too much security. Depending upon the costs, the liability, the benefits, and the total risk picture, a company that opts for security over-kills may actually harm its business interests. As noted earlier, in addition to the relatively high costs of information security technologies, end-user burdens and other harms to timely, responsive and flexible service can significantly disadvantage an online business channel.

For any given type of transaction, there is a checklist of information security requirements that might apply. These are in three levels: network, document and application. Some security only deals with the flow or control of data as it flows over a **Network** (including the Internet):

* *Confidentiality* means preventing interception and reading of the data as it flows over the network.

* *Authentication for access control* means only allowing certain users access to certain areas or resources on a network.

The next level, **Document Security**, deals with the transactional data itself - the data that actually constitutes the request for a purchase or the bid in an auction, for example. This data

may need to be kept over time, secured, authenticated and so on:

* *Data privacy* refers to data in which a person or entity has a continuing legal interest or right. Medical records, proprietary information and financial data would usually require this type of security (see the previous section in this Chapter on Information Practices).

* *Receipt or acknowledgment* refers to those instances where confirmation of transmission receipt is required for a given document or data set.

* *Authentication for binding intent* refers to data that form the basis of a contract or other document that is being assented to or "signed".

* *Data integrity* refers to the need to show that the data originally sent has not been tampered with during a given period of time. This may require secure digital time stamping services.

The last level, **Application**, involves functionality available within the application:

* *Authentication of Role or Authority for Specific Actions* refers to an individual user's ability to perform any given function within the application such as approving data or setting user rights.

These categories overlap to some extent, but they are presented as a basis to begin thinking about information security needs for a given application in a structured and solution-oriented manner.

Based on the boxes checked in the matrix, a counsel would then want to assist business and technical persons to match up the security requirements with an available menu of technical security offerings. Such a menu would include smart cards, biometrics, Public Key cryptography, signature dynamics and other technologies offered by vendors. Based on an analysis of costs, benefits and risks the choice of technical offerings can be more closely tailored to the actual application needs.

Transaction Type	**Security and Authentication Requirements**						
	Network Level		Document Level				Application Level
	Transmission Confidentiality	Authentication for Access Control	Data Privacy	Receipt or Acknowledgement	Authentication for binding Intent	Data Integrity And Digital Time Stamp	Authentication of Role or Authority for Specific Actions
Interstate Commercial Transaction							
Public Bids							
Newspaper							
Adult Entertainment							
Real Estate							
Securities Transfer							

If the transaction in question involves the interstate sale of goods, then the rules of the federal ESIGN legislation[51] would probably apply. If this transaction further involved a consumer who is entitled to receive a notice by law relating the sale (such a vehicle recall or repossession notice) then special rules apply before that consumer can legally elect to receive such notices electronically. Similarly, if the transaction involves adult entertainment, then it will be necessary to establish the age of the viewer. An assent, confirming age, may be part of the solution to this requirement. The list of transactions is purely to illustrate that the different issues raised depend upon the nature of the interaction, the parties and the applicable law.

A single matrix (at least on such a small piece of paper) is inadequate to convey the full, interconnected dynamics of a complex set of system security requirements. Depending upon the types of transactions to be facilitated, it may be desirable to modify a matrix to separate out the interface and also individual electronic records (at the sub-document level), in addition to the network, documents and application. Examples of sub-document electronic records include data that comes from more than one database to form a single screen of information. In addition, to assure a truly secure and reliable system, one must layer on other non-technical features, such as appropriate audits, internal business controls (separation of powers, etc.). Legal rules affecting records retention and filings with governmental entities of records related to transactions will constitute another source of technical requirements[52].

---

[1] This article was greatly enhanced by the assistance and input of Jessica Natale, a third year law student at Suffolk University Law School.

[2] McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 115 S.Ct. 1511, 131 L.Ed.2d 426.

[3] Anonymity and Pseudonymity in Cyberspace: Deindividuation, Incivility and Lawlessness Versus Freedom and Privacy Paper presented at the Annual Conference of the European Institute for Computer Anti-virus Research (EICAR), Munich, Germany 16-8 March 1998 by M. E. Kabay, PhD, CISSP Director of Education International Computer Security Association

[4] Id at 3.1.2.

[5] The Federal Trade Commission Advisory Committee on Online Access and Security, Draft Advisory Committee Report (as of April 26. 2000) "Maintaining the ability of individuals to be anonymous on the Internet is a critical component of privacy protection. Access systems should not require identification in all instances." http://www.ftc.gov/acoas/papers/draft_advisory_commttee_report_body.htm.

[6] Identified, Anonymous and Pseudonymous Transactions: The Spectrum of Choice, Roger Clarke, 1999, prepared for presentation at the User Identification & Privacy Protection Conference, Stockholm, 14-15 June 1999 [available at: http://www.anu.edu.au/people/Roger.Clarke/DV/UIPP99.html]

[7] McIntyre v. Ohio Elections Com'n, U.S.Ohio 1995, 115 S.Ct. 1511, 514 U.S. 334, 131 L.Ed.2d 426, on remand 650 N.E.2d 903, 72 Ohio St.3d 1544.

[8] City of Manchester v. Leiby, C.C.A.1 (N.H.) 1941, 117 F.2d 661, certiorari denied 61 S.Ct. 838, 313 U.S. 562, 85 L.Ed. 1522.

[9] Bursey v. U. S., C.A.9 (Cal.) 1972, 466 F.2d 1059.

[10] State v. Baker, Ohio App. 1 Dist.1993, 621 N.E.2d 1347, 87 Ohio App.3d 186.
USCA CONST Amend. VI-Jury Trials.

[11] More on these programs is available at: http://www.moneylaundering.com

[12] Proposed to have been codified as 12 C.F.R., Part 326.

[13] 63 Fed. Reg. 67524 (Dec. 7, 1998).

[14] On December 7, 1998, the Comptroller of the Currency, the Office of Thrift Supervision, the Federal Reserve Board and the Federal Deposit Insurance Corporation published proposed "Know Your Customer" regulations. Ostensibly, these regulations would have required banks and thrift institutions to:

1. identify their customers;
2. determine the sources of funds for each customer;
3. determine the "normal and expected" transactions of each customer;
4. monitor each customer's account activity and measure it against historical patterns; and
5. report to the U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN) any transactions that are "suspicious" because they do not conform to historical patterns.

[15] See, for example, the testimony of Solveig Singleton, Lawyer, The Cato Institute before the U.S. House of Representatives Committee on the Judiciary Subcommittee on Commercial and Administrative Law, at: http://www.cato.org/testimony/ct-ss030499.html. See also the open letter by Lowell H. Becraft, Jr. to the Federal Deposit Insurance Corporation at http://www.garynorth.com/y2k/detail_.cfm/3472

[16] A press release by Representative Ron Paul, a libertarian-leaning member of Congress, lauding the withdrawal illustrated the vigor with which these rules were resisted. The press release is available at: http://www.house.gov/paul/press/press99/pr032399-kyc.htm

[17] See http://www.bxa.doc.gov/Enforcement/knowcust.htm

[18] Id.

[19] W.G.A. v. Priority Pharmacy, Inc., E.D.Mo.1999; 184 F.R.D. 616, Protecting litigants from public knowledge of AIDS status; Eilers v. Palmer, D.C.Minn.1984, 575 F.Supp. 1259, Names of individuals supporting unorthodox religious views, need not be disclosed.

[20] New England Apple Council v. Donovan, C.A.1 (Mass.) 1984, 725 F.2d 139; Lame v. U.S. Dept. of Justice, C.A.3 (Pa.) 1981, 654 F.2d 917; Cofield v. City of LaGrange, Ga., D.D.C.1996, 913 F.Supp. 608; 5 USCA s 552.

[21] State v. Gamble, La.App. 3 Cir.1994; 631 So.2d 586; 93-809 (La.App. 3 Cir. 2/2/94, Roviaro v. U.S., U.S.Ill.1957; 77 S.Ct. 623, 353 U.S. 53, 1 L.Ed.2d 639; Westinghouse Elec. Corp. v. City of Burlington, Vt., C.A.D.C.1965, 351 F.2d 762, 122 U.S.App.D.C. 65, on remand 246 F.Supp. 839; People v. Woolnough, N.Y.A.D. 2 Dept.1992, 580 N.Y.S.2d 776,180 A.D.2d 837, appeal denied 596 N.E.2d 422, 584 N.Y.S.2d 1024, 79 N.Y.2d 1056, State v. Baker, Ohio App. 1 Dist.1993, 621 N.E.2d 1347, 87 Ohio App.3d 186.

[22] Rodriguez v. City of Springfield, D.Mass.1989, 127 F.R.D. 426.

[23] Heather K. by Anita K. v. City of Mallard, Iowa, N.D.Iowa 1995, 887 F.Supp. 1249.
42 USCA s 12133, Protecting child's need for anonymity to avoid harassment and permanency of lawsuit's record, concerning child's action the Americans with Disabilities Act; Doe v. Covington County School Bd., M.D.Ala.1995, 884 F.Supp. 462, Protecting anonymity of children suing school officials based upon alleged sexual abuse by public school teacher; Doe v. Stegall, C.A.5 (Miss.) 1981, 653 F.2d 180, rehearing denied 659 F.2d 1075, Protecting anonymity of litigants challenging prayer and bible reading in schools to avoid exposing litigants' personal beliefs and practices; Plaquemines Parish School Bd. v. U. S., C.A.5 (La.) 1969, 415 F.2d 817, 42 USCA s 2000c-6, Civil rights era African-American litigants entitled to proceed anonymously in segregation case; Doe v. Blue Cross & Blue Shield of Rhode Island, D.R.I.1992, 794 F.Supp. 72, In case against insurer to recoup medical expenses for a sex change operation, litigant was entitled to proceed under fictitious name to avoid threat of economic harm resulting from stigma, 30 Plaintiff entitled to proceed under pseudonym in suit against insurer for payment under disability insurance related to psychiatric disorders; Anonymous v. Legal Services Corp. of Puerto
Rico, D.Puerto Rico 1996, 932 F.Supp. 49, Americans with Disabilities Act suit against former employer involving mental illness of plaintiff entitled plaintiff to proceed anonymously.

[24] Luckett v. Beaudet, D.Minn.1998, 21 F.Supp.2d 1029.

[25] 26 USCA s 6110, 51 Rule 227.

[26] 5 U.S.C. 6501, et seq.; 16 C.F.R. Part 312.

[27] [EXECUTIVE ORDER NO. 12196 OCCUPATIONAL SAFETY AND HEALTH PROGRAMS FOR FEDERAL EMPLOYEES <Feb. 26, 1980, 45 F.R. 12769, as amended by Ex. Ord. No. 12223, June 30, 1980, 45 F.R. 45235; Ex. Ord. No. 12608, Sept. 9, 1987, 52 F.R. 34617>], 5 USCA s 7092, 1-201.

[28] 42 USCA s 10607

[29] Doe v. Poritz, N.J.1995, 662 A.2d 367, 142 N.J. 1, 36 A.L.R.5th 711; 42 USCA s 14071.

[30] State v. Miller, Ga.1990, 398 S.E.2d 547, 260 Ga. 669.

[31] While more technical definitions abound, this explanation is from the Webopedia, an online dictionary and search engine for computer and Internet technology, at [http://webopedia.internet.com/TERM/e /encryption.html]. This source defines "cryptography", a closely related concept, as: "The art of protecting information by transforming it (encrypting it) into an unreadable format, called cipher text. Only those who possess a secret key can decipher (or decrypt) the message into plain text. Encrypted messages can sometimes be broken by cryptanalysis, also called codebreaking, although modern cryptography techniques are virtually unbreakable . . ."

[32] This definition is from the state Uniform Electronic Transactions Act [http://www.law.upenn.edu/bll/ulc/uecicta/uetast84.htm] and has more recently been reflected in the federal law known as the Electronic Signatures in Global and National Commerce Act (ESIGN), enacting Senate Bill 761 in the 106th Congress, Public Law No. 106-229, 15 USCA 7001.

[33] The best example is the state Uniform Computer Information Transactions Act (UCITA) which provides that:
"Authenticate" means:
(A) to sign; or
(B) with the intent to sign a record, otherwise to execute or adopt an electronic symbol, sound, message, or process referring to, attached to, included in, or logically associated or linked with, that record.
[http://www.law.upenn.edu/bll/ulc/ulc_frame.htm] Note, however, that as of this writing the UCITA had only been adopted in 2 states and was viewed as highly controversial, while the UETA has been adopted over 20 states. The term "electronic signature", as reflected by UETA and under federal law, appears to be well established.

[34] The following section on public key cryptography is borrowed and updated from an earlier published article co-authored by Daniel Greenwood. The graphics were created by Ray Campbell. See: Electronic Commerce Legislation: “From Written on Paper and Signed in Ink to Electronic Records and Online Authentication”, By Daniel J. Greenwood and Ray A. Campbell, 53 The Business Lawyer 307-338 (1997).

[35] The math underlying public key cryptography is rather esoteric and is beyond the scope of this paper. In short, public key cryptography is based on the fact that the only way to factor a large prime product (a very large number derived by multiplying two large prime numbers) is by having a computer calculate every possible combination of numbers in order to find the two component numbers. If the component numbers are large enough, solving the equation becomes "computationally intractable." The current generation of public key cryptosystems uses numbers so large that it could take extremely powerful computers years, and millions of dollars (or more) to crack a single public/private key pair.

[36] The digital signature is created through two distinct steps: First, the message digest, created through the use of a hash function, ensures the integrity of the content of the intended communication. Second, the use of the private key to encrypt the message digest authenticates the identity of the person sending the message.

[37] The two operations are performed upon separate documents. One upon the digital signature, an encrypted message digest, and the other upon the message itself. Although the results of both operations are compared against each other to obtain a true verification, it is irrelevant which operation is performed first.

[38] For the full report, see sections 8 and 9 of the Emall Evaluation, at http://www.emall.isa.us/

[39] Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy, MIT Press, 2001, by Stefan A. Brands. http://mitpress.mit.edu/book-home.tcl?isbn=0262024918

[40] The acronym PKI stands for Public Key Infrastructure, reflecting the fact that the use of digital signatures based on public key cryptography requires an elaborate infrastructure (technical, business, policy, and legal) to support their use.

[41] The National Automated Clearinghouse Association published a set of guidelines to assist parties in setting up rules which parties would contractually agree upon before relying upon digital certificates. The Certification Authority Ratings and Trust Guidelines (CARAT) are available at: http://internetcouncil.nacha.org/Projects/CARAT_Final_011400.doc

[42] UTAH CODE ANN. Ch. 4 § 46.

[43] Uniform Electronic Transactions Act, available at <http://www.law.upenn.edu/bll/ulc/uecicta/uetast84.htm>.

[44] Electronic Signatures in Global and National Commerce Act, 15 USAC 7001. Also, for a good overview of the various laws enacted in this legal area, see www.mbc.com.

[45] See http://ietf.org/html.charters/spki-charter.html It should be noted that standards such as SPKI are not widely implemented and do not have robust tool sets to aid users. While PKI technologies are costly, it can be even more costly to tailor design tools. Non public key technologies often present the simplest and least expensive alternatives.

[46] Recently acquired Communication Intelligence Corporation.

[47] The California Digital Signature Regulations address Signature Dynamics as follows:
California Administrative Code Title 2. CHAPTER 10.
Section 22003(b) List of Acceptable Technologies
The technology known as "Signature Dynamics" is an acceptable technology for use by public entities in California, provided that the signature is created consistent with the provisions in Section 22003(b)(1)-(5).
1. Definitions – For the purposes of Section 22003(b), and unless the context expressly indicates otherwise:
A. "Handwriting Measurements" means the metrics of the shapes, speeds and/or other distinguishing features of a signature as the person writes it by hand with a pen or stylus on a flat surface.
B. "Signature Digest" is the resulting bit-string produced when a signature is tied to a document using Signature Dynamics.
C. "Expert" means a person with demonstrable skill and knowledge based on training and experience who would qualify as an expert pursuant to California Evidence Code §720.

D. "Signature Dynamics" means measuring the way a person writes his or her signature by hand on a flat surface and binding the measurements to a message through the use of cryptographic techniques.

2. California Government Code §16.5 requires that a digital signature be 'unique to the person using it.' A signature digest produced by Signature Dynamics technology may be considered unique to the person using it, if:
   A. The signature digest records the handwriting measurements of the person signing the document using signature dynamics technology, and
   B. the signature digest is cryptographically bound to the handwriting measurements, and
   C. after the signature digest has been bound to the handwriting measurements, it is computationally infeasible to separate the handwriting measurements and bind them to a different signature digest.
3. California Government Code §16.5 requires that a digital signature be capable of verification. A signature digest produced by signature dynamics technology is capable of verification if:
   A. the acceptor of the digitally signed message obtains the handwriting measurements for purposes of comparison, and
   B. if signature verification is a required component of a transaction with a public entity, the handwriting measurements can allow an expert handwriting and document examiner to assess the authenticity of a signature.
4. California Government Code §16.5 requires that a digital signature remain 'under the sole control of the person using it'. A signature digest is under the sole control of the person using it if:
   A. the signature digest captures the handwriting measurements and cryptographically binds them to the message directed by the signer and to no other message, and
   B. the signature digest makes it computationally infeasible for the handwriting measurements to be bound to any other message.
5. The signature digest produced by signature dynamics technology must be linked to the message in such a way that if the data in the message are changed, the signature digest is invalidated.

[48] [http://webopedia.internet.com/TERM/b/biometrics.html]

[49] See the article Trust Management on the World Wide Web, by Rohit Khare and Adam Rifkin at http://www.cs.caltech.edu/~adam/papers/www/trust-management.html. Foe an example technica at http://ietf.org/rfc/rfc2704.txt

[50] http://catless.ncl.ac.uk/Risks/20.06.html#subj1

[51] Infra, Footnote 4. (S. 761)

[52] The ESIGN law, infra Footnote 4, while allowing for the use of electronic records, assures that government records retention and filings authority remains. This law also enables government to set technical requirements for the "performance standards" affecting records retention, including accuracy and integrity of those records.