DIGITAL SIGNATURES: A BUSINESS VIEW

William Kuechler and Fritz H. Grupe

The technology to create secure digital signatures is proven and workable on PC-level hardware, as well as on mainframes. The issues currently restraining widespread use of digital signatures are primarily legal. This tutorial survey first identifies the functions a digital signature should ideally perform by tracing an example Internet-based electronic business transaction. After an overview of the technology that provides the required functionality, this article presents the current legal status of digital signature use, including a number of unresolved liability issues, and summarizes some precautions for digital signature use.

Electronic commerce has been carried out successfully for years without the use of digital signatures (DSs). Hundreds of billions of dollars of commercial transactions are quite adequately handled each year using the 30+ year-old technologies of electronic data interchange (EDI), electronic funds transfer (EFT), and semiprivate communications links called value-added networks (VANs). Why, then, over the past few years have digital signatures been increasingly seen as necessary to digital commerce? And why have digital signatures had such a high profile in the trade press and even the popular press?

Digital signatures address a number of issues that have emerged as the e-commerce communications infrastructure has shifted rapidly from the private, semi-secure communications facilities of VANs to the very open, very insecure Internet. The transition from primarily one-on-one contractual transactions between known, trusted parties, and occurring repeatedly over time to many-to-many transactions between strangers that may occur once, never to be repeated, introduces still more issues that digital signatures have the promise to resolve.

Digital signatures currently have a high public profile for a “technology” issue because to work effectively they require not only technology but also an authoritative infrastructure that can only be enabled by legally binding agreements — laws at the state, federal, and international levels. Putting together the enabling legislation for this infrastructure is new ground for legislative bodies; some of the laws are definitely controversial and are evolving works in progress, and that makes news.

The following excerpt from the American Bar Association’s tutorial on digital signatures summarizes the situation:

As electronic commerce increasingly moves from a bilateral setting to the many-on-many architecture of the World Wide Web on the Internet, where significant transactions will occur among strangers who have no prior contractual relationship and will never deal with each other again, the problem of authentication/non-repudiation becomes not merely one of efficiency but also of reliability. An open system of communication such as the Internet needs a system of identity authentication to handle that scenario.

In the next section, the long list of terms and entities involved in technical and legal discussion of digital signatures emerges naturally by tracing an imaginary electronic business transaction between two fictitious companies.
Note that a digital "signature" as we describe it here and as it is commonly used is so distinct from digital formatting of a written signature that the term "signature" is sometimes felt to be misleading. Some authors have adopted the term "digital fingerprint" as a synonym. However, because virtually all state, federal, and international laws use the term "digital signature," we will continue to use it.

**AN INTERNET BUSINESS TRANSACTION EXAMPLE**

The business scenario below presumes the use of digital signatures and is described first with an actor-interaction diagram (Exhibit 1). This type of diagram was introduced by Jacobsen (1994) for capturing the system descriptions in object-oriented form, and its use has become extremely widespread. Next, a narrative elaboration on the diagram develops the legal and functional requirements for digital signatures. The main actors are two companies that have never done business before and know of each other only by what they have discovered on the World Wide Web. The example also introduces several legal entities that must exist for the transaction to take place.

The left-most column of Exhibit 1 describes the scenario in high-level business terms, from initiation to conclusion moving down the column. The columns of Exhibit 1 to the right of the scenario show the detailed activities and transfers of information and material between actors that are necessary to accomplish the actions described in the scenario.

"A" Company wishes to purchase office supplies over an Internet trading portal. The vendor with the best price for the mix of products "A" Company wants is "B" Supply Co., an organization "A" Company has never dealt with before. "A" Company wishes to send "B" Supply Co. an electronic purchase order and have it acknowledged electronically. Following receipt of goods, "A" Company would like to be invoiced electronically and pay via electronic transfer of funds to "B" Supply Co.'s account.

Exhibit 1 lists two actors that are required only in a trading scenario that uses digital signatures: certification authorities (CAs) for both "A" Company and "B" Supply Co. These entities...
are (ideally) trusted holders of electronically accessible information on the companies that subscribe to their services. The information they make available includes principally the keys required to code and decode digital signatures and the identities of the certificate holders; however, they may include other private information. Certification entities form part of the public key infrastructure (PKI) that is required for effective use of digital signatures. Their functions, legal status, and legal responsibilities will be discussed more fully in the section on legal aspects of digital signatures. By tracing through the scenario of Exhibit 1, the problems that arise in dealing with unknown entities and the solutions to these problems provided by digital signatures become apparent.

Having located a company it wishes to do business with based solely on the basis of cost and availability of goods (scenario activity 1), “A” Company wants to verify the identity of “B” Supply Co. before committing to do business with them. Part of the information “A” Company downloaded from “B” Supply Co.’s Web site is “B” Supply Co.’s certificate ID, a reference number on file with a certification authority. When “A” Company is able to locate the “B” Supply Co.’s certificate on file with the CA (scenario activity 2), it knows “B” Supply Co. is a real entity that will be legally bound by any valid business transaction they enter into. Accompanying the certificate is “B” Supply Co.’s public key, a code that allows “A” Company to send “B” Supply Co. information in a private (encrypted) manner.

In scenario activity 3, “A” Company orders supplies from “B” Supply Co. by sending “B” Supply Co. over the Internet an encrypted (private) purchase order and a second piece of information, “A” Company’s digital signature. Generation of a digital signature will be described in the section of this article on digital signature technical issues. “B” Supply Co. must be able to verify that “A” Company is a real company, will be legally bound by a valid trade commitment, and will accept responsibility (non-repudiation) for having sent the purchase order (PO). The means for accomplishing this are to take the certificate information given by “A” Company and download from the specified CA “A” Company’s public key (scenario activity 4). Simply being able to locate a current certificate for “A” Company on a trusted CA tells “B” Supply Co. that “A” Company is a valid entity able to enter into binding business agreements. Once “B” Supply Co. has downloaded “A” Company’s public key, it can decrypt the PO to determine the order information and also decrypt the digital signature. If this operation is successful, then “B” Supply Co. can be sure of three important facts:

1. “A” Company sent the PO.
2. The PO was transmitted without error or tampering.
3. “A” Company cannot deny having sent the PO.

Having verified the PO, “B” Supply Co. proceeds to fulfill the order, ship the merchandise, and transmit an invoice signed with their digital signature to “A” Company (scenario activity 5). Both pieces of information are encrypted using “B” Supply Co.’s private key. When “A” Company decrypts the message using “B” Supply Co.’s public key (retrieved from the CA in scenario activity 2), then “A” Company can be certain that the information did in fact originate at “B” Supply Co. and has not been damaged in transmission or tampered with.

In the final scenario activity, 6, “A” Company transmits funds to “B” Supply Co.’s bank, very possibly using traditional EFT, which does not require digital signatures, and simultaneously transmits an encrypted (for privacy and security) payment advisory to “B” Supply Co. “B” Supply Co. decrypts the message using “A” Company’s public key obtained during scenario activity 4.

THE TECHNOLOGY UNDERLYING DIGITAL SIGNATURES

Tracing a Web-based business transaction exposed three elements essential for trading over the Internet. The first is security — the guarantee that the document being transferred has not been altered in any way in transit. The second is attribution — that the source of the document can be identified without doubt. The third is non-repudiation — the sender cannot deny sending the document. The technological framework that enables digital signatures to provide these elements is encryption technology deployed in a distributed fashion identified earlier as the public key infrastructure.

Public Key Cryptosystems

Cryptography is the science of encoding messages — scrambling them so that the original contents of the message are indecipherable — and of decoding messages — unscrambling them so that the original message can be understood. In the past 25 years, several algorithms
for encrypting messages have been developed that have three highly desirable characteristics:

- They work well on many computers, including inexpensive computers such as PCs.
- The encoded message is, by mathematical proof, indecipherable by any known means in any reasonable amount of time.
- Separate keys can be created as a unique pair; messages encoded with the one key can only be decoded with the other key of the pair.

The use of digital signatures depends on such algorithms to create what is called a public key cryptosystem. In such a system, one key of a pair is made publicly available, and the other is held securely by a single party.

One other mathematical function, called a “hash,” is necessary to understand the creation of a digital signature. Hash functions have been known since before the dawn of digital computers and are valuable because they can take any document, treat it as a digital number, and create from it a unique, much shorter number. For every unique document, a unique hash results. In addition to being unique, a hash works only in one direction; that is, it is impossible to start with the hash of a document and recreate the original document.

Exhibit 2 and the discussion that follows it show at a detailed level how public key cryptography realizes the properties that were determined earlier to be necessary for unfamiliar parties to conduct secure E-commerce transactions: security, attribution, and non-repudiation.

1. To encrypt and digitally sign the message:
   - A mathematical operation (a hash function) is performed on the message to be sent, resulting in a 128-bit “message digest.”
   - The message digest is then encrypted with the signer’s private key, producing the digital signature.
   - The message and digital signature are sent.

2. To decrypt a digital signature, the receiver:
   - Decrypts the digital signature back to the message digest using the public key.
   - Performs the hash function on the message (creating a duplicate of the message digest).
The certification practice statement (CPS) defines the policies and procedures of the CA, such as how a subscriber may register, the various classes of certificates it offers, and the security of the CA’s operations.

The Public Key Infrastructure
To render a public key commercially useful, there must be some way to determine that it actually corresponds to the identity of the alleged owner. The PKI is a hierarchy of organizations that issue and validate public keys, facilitating the use of digital signatures. The structure and regulation of the PKI vary among countries and jurisdictions, but essentially the PKI consists of a means to distribute public key-pairs and mechanisms to verify the ownership of public keys and ensure that they are currently valid.

A certification authority (CA) is an organization that issues public key-pairs for its subscribers to use and issues digital certificates to the subscribers’ trading partners attesting to the ownership of their public keys. There are several commercial CAs (VeriSign, RSA, Entrust, etc.) as well as some authorized by governmental agencies (currently only Utah in the United States provides certification of CAs). The CA is a “trusted” third party that enables its subscribers to link their identities to the key-pairs they use to digitally sign electronic communications.

Digital certificates generally contain the name of the subscriber; information about the subscriber organization, such as name, address, credit rating, and authority to conduct certain transactions; the subscriber’s public key; the digital signature of the issuing CA; the issuing CA’s public key; and other relevant information. These certificates have a specified life (usually one year), and may be canceled or revoked if the private key is compromised or on request from the subscriber. There are different types of certificates available from the various CAs, depending on the use for which they are intended. For instance, a certificate used to authorize large financial transactions between banks requires a high level of trust and would probably involve extensive background investigation, whereas a certificate used only to protect personal e-mail might involve nothing more than a request to the CA.

To enable users to access information regarding the digital certificates with ease, they are collected in an online repository. In addition to currently active certificates, the repository will contain a certificate revocation list (CRL), which lists all canceled or revoked certificates, and may also contain a copy of the certification practice statement (CPS) of each CA that publishes certificates to it. The CPS defines the policies and procedures of the CA, such as how a subscriber can register, the various classes of certificates it offers, and the security of the operation of the CA.

The certificates themselves should contain reference to the location of the repository and the URL to enable checking of the status of the certificate, but many do not. In fact, no consistent standard exists for what a digital certificate should contain or how the information it contains is verified.

LEGAL REQUIREMENTS FOR DIGITAL SIGNATURES
Digital signatures used within a PKI have some intrinsic properties derived solely from the technology employed. These include privacy (the ability to conveniently and securely encrypt and decrypt messages from business partners) and proof of origin. However, to be fully meaningful in a business relationship, digital signatures must be legally binding on the entities that issue them, and this attribute is independent of technology. It derives instead from a set of judicial prescriptions, enforceable through the court system. Moreover, for the PKI to achieve the potential envisioned for it, CAs must be trusted. The most convincing way to enable trust is through judicial action establishing a governmental authority to authorize CAs. This is known as establishing the hierarchy of authority for the CAs and thus the PKI.

Digital Signatures Legislation at the State Level
The process of enacting the legislative framework for a fully functional PKI began at the state level in the United States. One of the first states to enact legislation was Utah, and few bills of recent times have inspired more commentary than the 1995 Utah Digital Signatures Act. Utah’s act has been modified from its original statement and has been superseded in some areas by more recent federal legislation. However, it is instructive to discuss that bill, as
Credit cards, by regulatory law, may only be issued by large financial institutions that are capable of absorbing significant financial risk.

most of the legal and judicial problems that have and will be encountered by any similar action were initially described in analyses of the legal and practical consequences of the Utah act.

Eager to further digital commerce through the use of digital signatures, several Utah legislative subcommittees consulted heavily with the American Bar Association during the writing of the Digital Signatures Act. The act specifies the legality of digital signatures in electronic business transactions and also provides for a state authority to certify CAs in Utah. The bill specifies in detail the requirements to become a Utah-certified CA and also specifies the liability incurred by CAs should private keys of subscribers be compromised. It does not, unfortunately, specify the liability of individuals and businesses using digital signatures, allowing that liability to default to a very intimidating interpretation. Legality and liability issues are important because they are generic to any digital signatures legislation. The liability issues merit further discussion.

Digital signature liability issues are most easily comprehended by analogy to the use of credit cards. By federal law, the maximum liability that can be incurred by the holder of a credit card for fraudulent use of the card is $50.00. That is, if a credit card or a credit card number is stolen and used by someone other than the original holder of the card, irrespective of the amount of fraudulent purchases, the cardholder’s liability is limited to a small value. This low liability fostered the use of credit cards when they were introduced. In the case of digital signatures, however, should a digital signature certificate holder’s private key be compromised and used for fraudulent transactions, there is no legal cap on liability. Further, the burden of proof of both adequate precaution to secure the private key and of fraudulent use of the key falls on the certificate holder. In effect, the liability of a digital signature certificate holder for fraudulent use of the signature is potentially unlimited. Moreover, although the Utah act specifies that the digital signature user must take “reasonable precautions” to secure the private key, it does not specify what constitutes “reasonable precautions,” potentially requiring a legal case for every instance of fraudulent use of a DS.

This liability issue has significantly slowed the acceptance of digital signatures. Given the analogy with credit cards, it is reasonable to ask: “Why not simply pass a law mandating a liability cap for fraudulent use of digital signatures as was done for credit cards?” The reason this has not been done in Utah or in any other jurisdiction to date is because no large risk-spreading agent is involved in a PKI, which is not the case for the use of credit cards. Credit cards, by regulatory law, may only be issued by large financial institutions that are capable of absorbing significant financial risk. These institutions, typically banks and large credit unions, distribute the cost of “insurance” for losses from fraud over cardholder and card-acceptor fees for hundreds of thousands or even millions of users.

The agents involved in a PKI (as it is currently envisioned) are the government (the top of the certification hierarchy), certificate authorities, and digital signature users. If the liability of the digital signature user for fraudulent use is to be capped, then who will accept the remainder of the liability? At present, no one. In fact, in the Utah bill, the liability of CAs was capped at a level that was criticized as too low by many legal commentators. Conversely, it was recognized that the low liability cap for CAs was a valid attempt to draw private entities into the role of CAs in order to more generally promote the use of digital signatures and electronic commerce overall. Note that in the interests of promoting electronic commerce, current legal and legislative thought tends away from the strict regulation found in the credit card industry for the CA market. Thus, under all bills legislated to date, CAs are not required to be government certified. In fact, at present, the largest CAs such as VeriSign™ are private and unregulated.

Insisting that CAs become certified and accept large liability risks is seen by both economists and legislators as an excellent way to stifle the market. At present, almost all of the states have initiated some form of digital signature legislation, but no one has found a solution to the liability issues inherent in a “free-market” PKI. Recent federal legislation also skirted the issue, concentrating primarily on enabling digital signatures, that is, on removing impediments to their use and standardizing definitions across the nation.

Federal Digital Signatures Legislation

According to the Electronic Signatures in Global and National Commerce Act enacted by Congress in June 2000 (more popularly known as the “E-sign” Act), a legally binding electronic signature is “an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed
State laws often take precedence over federal law, so it is important to check on the implications of these laws, as well as on the federal law.

The E-sign Act renders digital signatures legally binding as long as the consumer “has affirmatively consented to such use and has not withdrawn such consent” but does not require “any person to agree to use or accept electronic records or electronic signatures.” In addition, in order to perform electronic transactions, businesses are required to inform consumers (and presumably also any trading partners) as to:

- Their right to withdraw consent to accept electronic transactions and the procedures for withdrawal of consent
- Whether the consent is intended to be for a one-time transaction or ongoing
- How to obtain a paper copy of an electronic record
- The hardware and software requirements for access to and retention of electronic records

Consumers must also demonstrate that they are able to access information in the electronic form by consenting or confirming consent electronically.

The E-sign Act also states that the requirement for retention of contracts and records “is met by retaining an electronic record of the information.” It requires that the information remain available to all parties who are entitled to access for the period of time required by law and “in a form that is capable of being accurately reproduced for later reference, whether by transmission, printing, or otherwise.”

The E-sign Act allows state laws to specify alternative procedures or requirements for the use of electronic records or signatures on the condition that they “do not require, or accord greater legal status or effect” to any specific technology. State laws often take precedence over federal law, so it is important to check on the implications of these laws, as well as on the federal law.

State Laws
The E-sign Act encourages states to adopt the provisions of the Uniform Electronic Transactions Act (UETA), which was developed by the National Conference of Commissioners of Uniform State Laws in 1999. In addition to the issues covered by E-sign, the UETA addresses attribution, effect of other state laws, effect of private agreements, sending and receiving, effects of errors in electronic communication, and admissibility and transferability of digital signatures. At present, 22 states have adopted some form of the UETA, and it is being considered in several others.

Issues addressed by state laws that are not covered by E-sign or the UETA include creation of regulatory systems for licensing CAs and certificate repositories, definition of the responsibilities of CAs and users of digital certificates, and description of the liability and evidentiary burdens of the parties to transactions utilizing digital signatures.

At least seven states have digital signature laws that cover licensing of CAs (Utah, Washington, Oregon, North Carolina, California, and Nebraska) or approval of PKI service providers (Texas). Several of the laws that have been enacted, including the Utah and Illinois statutes, appear to violate the technology-neutral requirement of E-sign, and it must be assumed that the provisions that give preference to certain technologies will likely be contested in the future.

International Digital Signatures Law, and Jurisdictional Issues
In July of 2001, the United Nations Commission on International Trade Law approved a Model Law on Electronic Signatures. In the opinion of many analysts, the Model Law is similar to the U.S. Electronic Signatures in Global and National Commerce Act in that it is an enabling act, which specifies the legality of digital signatures for international E-business, seeks to remove some barriers to their usage, and promotes common terminology for dealing with digital signatures across nations. It leaves many low-level issues on the use of digital signatures unresolved. The European Union and many individual nations in Europe and the Far East have enacted digital signature legislation that closely resembles similarly intended legislation in the United States. The good news for digital signatures is that their legal status as replacements for paper signatures for binding business agreements is virtually assured globally.

However, transacting E-business with customers or suppliers outside the United States has become more uncertain over the past three to five years, driven by two significant differences...
in attitude between Europe and the United States, the first toward privacy of data and the second toward jurisdiction of disputes. These same differences — and uncertainties — apply to E-business conducted with digital signatures. The issues are far too complex for anyone to predict their resolution in detail; however, international legal analysts suggest two things:

- The strong European concern with privacy of individual data will make it problematic (risky) for U.S. certificate authorities to accept European clients, as European legal penalties for breaches of security will probably be more stringent. Likewise, the assurances and security practices required by European clients of certificate authorities will likely be perceived as onerous by U.S. companies. This prediction is simply an extension of the current situation in which U.S. financial institutions are grappling with European privacy laws.

- The very strong trend in Europe toward insisting that litigation of consumer issues take place in the customer’s country of origin increases the impediments to conducting consumer E-business with digital signatures beyond those currently being experienced. Specifically, the liability for fraudulent use of a digital signature will almost certainly be limited in most European nations relative to the United States. Thus, U.S. companies doing business with European-based customers and CAs face increased risk of fraud, as there will be limited legal recourse for recovering the costs of fraudulent purchases.

Consequently, an agreement between the United States and the European Union on these issues seems unlikely in the near future due to their origin in deeply rooted and widespread cultural differences.

**INEVITABILITY AND POTENTIAL DRAWBACKS OF DIGITAL SIGNATURES**

In the opinion of many analysts, the pressure for everyone, both individuals and businesses, to use digital signatures (DSs) will become irresistible over the next five to ten years. Suggested as the biggest instigators are governments, drowning in paper, that see completely electronic submissions of forms and documents, which digital signatures enable, as an integral part of the solution to that problem. Initially, government will pressure large businesses into DS use because they have the IT resources to implement DSs relatively quickly and they share many of the paper-overload problems with governments. Then, following the coercive model seen during the introduction of EDI (large companies insisting their suppliers comply with their electronic document specifications), the larger businesses and the governments will exert pressure on smaller businesses and individuals to begin using DSs. Adding to the pressure will be the fact that browsers and other Web-based software will increasingly come with all the features necessary for DS, lowering the investment required to use the technology to nearly zero. Further impetus is given by business-to-business Web sites that depend on this form of technology to connect buyers and sellers. Some observers indicate that, within a company, DSs can be used for intranet sign-offs, transfers, and other business transactions.

However, the many significant problems and shortcomings in the use of DSs that were first uncovered during a pragmatic analysis of the consequences of early DS legislation have yet to be solved. Some of the most important of these are:

- How reliable and secure is the CA that issued my public and private key set?
- How reliable and secure is the CA that issued the key sets of my trading partners?
- Does the CA gather enough information about keyholders to adequately identify them, and how is that information verified?
- What happens if a certificate becomes invalid?
- What happens if a CA goes out of business, has its certification revoked, or in some other way becomes “untrustworthy”?
- How will I securely store my private key?
- What are the laws governing the jurisdiction(s) in which I do business?
- What liability do I incur if my private key is compromised?
- How expensive is it to implement DS technologies?

We expand briefly on each of these points and provide a compilation of recommendations from legal and security concerns authors have for ameliorating the problems.

**How Reliable and Secure Is the CA?**

The information contained in a digital certificate is only as good as the security and stability of the issuing CA. Currently, the only governmentally authorized CAs in the United States are in
Even state-certified CAs require very little verification of anything other than identity.

Security over the Private Key
Protection of your private key is crucial in a digital signature setup. Several ways that keys can be protected are by encryption, storage in an offline media (diskette, smart card, token, etc.), or requiring a collaborative effort between two or more entities in order to use the key. If the key is to be stored on a networked computer, then network security is of paramount importance. If the key is on a hard drive or other storage medium, a technician, a fellow worker with physical access to your work area, or any passerby with malicious intent can compromise it. If a key is acquired or stolen, it can be very difficult to repudiate unauthorized transactions made by the thief. As discussed earlier, the burden of proof of an unauthorized DS transaction falls on the legitimate certificate holder. Examples of hackers gaining access to personal information underscore the potential for theft of DS information.

In quite another way, privacy becomes problematic. Because privacy is, for many communications, a key element in the use of DSs, access to private keys is of great concern. Governmental and law enforcement agencies, in particular, can require the divulging of the keys in use. Some experts express concern over the ability of one party to gain access to information about the second party to guarantee that the transaction is really with the person who it is purported to be. Anonymous transactions become impossible when the CA provides information about the real identity of the purchaser.

Invalid Certificates
In any electronic signatures law to date, it is the signature acceptor’s responsibility to ensure that a trading partner’s certificate is valid. Normally, this requires searching the certificate revocation list (CRL) of the CA that issued the certificate prior to the validation (decryption of the signature) of every transaction. Given the appropriate software, this is not as onerous a task as it might appear initially.

A situation that is hypothetical at this time, but becomes more likely as the number of CAs increases, is the business failure or revocation of authorization of a CA. In effect, the certificates of all subscribers to the CA become potentially invalid simultaneously. At present, no mechanisms are available for determining the ongoing “trustworthiness” of a CA and there is no legal precedent for adjudicating disputes in such a circumstance.

Another potential problem is created by the desire of one party to cancel the transaction. In many consumer and business transactions, there are legally permissible periods in which the buyer can reconsider the action and withdraw from the agreement. This flexibility is not guaranteed under DS laws. In the opposite direction, if a certificate is issued, there is a question as to how long it is valid. If a transaction takes too long to complete, a seller may discover that the buyer is no longer in business.

Jurisdiction
Major forces are at play concerning the issue of jurisdiction in the international arena. If you limit your transactions to U.S. citizens, then the rules of the game are those widely understood in the U.S. Uniform Commercial Code. If you do business internationally, however, especially at the consumer level where explicit contractual agreements are unlikely, then you expose yourself to significant risk of overseas litigation. This problem is not unique to DS-enabled transactions; however, the increasing use of DS will serve to further the current trend toward globalization of the marketplace.

State Legal Issues
Some state laws, notably Utah’s, limit the liability of CAs that are licensed in accordance with state law. It is important for the manager to know what the legal requirements are for security over private keys (such as whether they can be stored in a networked computer or must be maintained offline), how to report compromised private keys, how to contest a
forged digital signature, evidentiary burdens (i.e., who is responsible for proving that a digital signature is valid/invalid when there is a dispute), and any other rights and responsibilities they have under the law.

**Expense**
The expense of implementing DS technologies can be daunting. Reports of in-house implementations have been as high as $4 million. Most companies will chose to utilize outsourcing services such as VeriSign and other CAs. Some chief information officers are reluctant to use outsourcers because they believe that external links introduce a weak link that can be exploited by hackers. Even with the use of an outsourcer, the fees and charges must be considered.

**RECOMMENDATIONS**
- Determine first whether your company needs to implement DS technology, which is complex and expensive and has the potential for incurring significant damages if compromised or misused.
- Consider the use of multiple certificates and digital signatures, each with the authorization to perform only a limited set of functions.
- Several security experts propose this mechanism as the only way to limit liability for the use of DS in the near future.
- Check out current and pending legislation in your jurisdiction. State laws may impose additional requirements or regulations above and beyond the federal E-sign Act.
- Make sure any digital trading partners have agreed in writing to accept digital signatures as legally binding.
- Digital document archives are not always subject to the same level of organization as paper. Make sure a strong and well-enforced records retention policy is established for both.
- If you are planning to store contracts and records digitally, carefully assess your storage and backup requirements. The information must be stored in a form that remains easily accessible for the period required by law.
- Ensure that security over private keys is strong. Consider methods of offline storage such as smart cards or requiring participation of two parties to generate signatures for significant transactions.
- Research the security procedures of both your CA and the CAs of your trading partners.

**Notes**
5. This online issues page is kept reasonably current. Contains links to white papers and to legal commentary on most state and federal legislation concerning digital signatures.

**References**