Understanding Digital Signature
And
Public Key Infrastructure

Overview

The use of networked personnel computers (PC's) in enterprise environments and on the Internet is rapidly approaching the point where they will be considered mass media and as a means to conduct a variety of online transactions. As with many predecessor technologies, this medium will advance the flexibility and velocity by which many transactions will be made.

While the use of PC's and the software used on them has proliferated, an environment has evolved in which documents can be created, distributed, used and retained completely in digital form. When they are intended to support a business or legal transaction, some of these documents may require a signature as an endorsement, or authentication to be considered "official" or "authorized."

Until now, when a signature was either desired or required, such documents had to be converted to a paper in order to carry it. This simple act thus creates a variety of problems that frustrate both the flexibility and velocity of the transaction environment. It also creates retention management issues because the conversion to paper requires management of paper documents for their official life.

While the nature of the transaction these documents are meant to support has not changed, the environment in which the transaction is made is changing. To support the new environment we must provide rules and practices that employ electronic and digital signature technology to achieve and surpass the functionality historically expected from paper based documents with ink signatures.

The Kansas 2000 legislative session saw the passage of the Senate substitute for House Bill 2879, known as the Uniform Electronic Transactions Act. This law position's Kansas as a leader in laying the legislative groundwork necessary to provide for electronic document based transactions and the use of digital signatures for those transactions.

Passage of this law also allows Kansas to move forward rapidly in the area of both electronic commerce and digital government. To do so, the technical infrastructure necessary to this digital environment must be put in place.

The purpose of this brief paper is to present a description of what this new technical infrastructure is comprised of, how it could be delivered and how Kansas state agency's could take advantage of it.

The ultimate result of implementing these tools will be a more secure environment to execute electronic transactions that will serve the citizens of Kansas and improve operational efficiency within state government organizations. With the expanding use of Web based services the citizens of Kansas can increasingly transact business with the state "online" rather than by standing "inline".

Why Do We Need This New Environment?

Many organizations, both public and private are interested in replacing paper-based systems with automated electronic systems. The reason for this is simple economics. It is much cheaper to process an electronic transaction with digital documents and signatures than with their paper counterparts. For example, a recent study concluded that processing a paper based expense report in the private sector costs approximately $36.00. The electronic version of the same expense report costs $4.00 to process. Clearly, this is a considerable difference. In fact, much of the rapid increase in productivity that has contributed to the country's inflation resistant yet expanding economy is based on this kind of improvement.

According to the Center for Research in Electronic Commerce at the University of Texas, revenue generated from the Internet totaled $524 billion (US dollars) in 1999. That figure is expected to reach $850 billion by the end of this year. With legislation in place to secure this environment, explosive growth of Internet based transactions can be anticipated.

Two factors have inhibited the increasing use of electronic documents and transactions. One has been the legal status of electronic documents. Simply put, there has been a cloud over the legitimacy of such documents. The other (related factor) has been the concern for the risk of forgery or manipulation of documents and data moving over unsecured networks. Both of these factors are rooted in a concern for the legitimacy and integrity of electronic documents and the security and privacy of the transactions for which they are used.

This has brought about the need for a reliable, cost-effective way to secure information in transit and to replace a handwritten signature with a digital signature. The new Kansas law and similar federal legislation provide for the legitimacy of both electronic documents and signatures.

Thus, the legal status of electronic documents and signatures is resolved by addressing the issues of legitimacy, security and integrity. This is accomplished by insuring that information (document or data) in transit between two points is not intercepted and manipulated or otherwise tampered with.

For example, let's suppose your attempting to make an electronic transaction with a bank. You give instructions to move $1,000.00 from account A to account B. Without protection this transaction is subject to a "man in the middle" attack that works like this. Your message is captured off the network while in transit to the bank by a hacker. The hacker takes your message and modifies it to read move $1,000.00 from account A to account Z, the hackers account. The hacker then waits for the confirmation from the bank that says $1,000.00 has been moved from account A to account Z, we are glad to be of service. The hacker then modifies the message to read - $1000.00 has been moved from account A to account B, we are glad to be of service. He then sends the message on its way to you. You receive the confirmation and are none the wiser until whoever owns account B calls to complain that they have not received your payment of $1000.00. The hacker is long since gone and so is account Z.

How would this change in the new environment? The new infrastructure, generally referred to as Public Key Infrastructure (PKI) includes a service component called Certificate Authorities (CA) and a technical component called asymmetric cryptography. Together, they secure transactions like this by adding new security functionality.

By using asymmetric cryptography, (explained in the next section of this paper) the message to the bank would be coded so that it could not be read by the hacker. This encryption insures that the message is not tampered with thus achieving confidentiality. However, the bank must know if it is a legitimate message that will not be repudiated even if it is certain that the message itself has not been comprised. Using the same technology, a digital signature can be used with the message so that it could also be "signed" and effectively sealed. This insures authenticity by creating and locking a coded value to the message using your digital signature. If the message were tampered with, the value changes and the message would not yield the correct code value

indicating it has been tampered with. When the bank receives your message they can authenticate it by checking for the correct code value using a “key” you provide them.

In this example both encryption for confidentiality and encryption for authenticity are applied. If the message were simply encrypted, the bank would be able to open the message with the key provided but would not be able to authenticate the source of the message. The fact that asymmetric cryptography can be used to accomplish both encryption and authentication of information and the parties that provide them can be confusing. While the issues are related there is a difference.

In the case of confidentiality, data is encrypted so that somebody watching the wire can't see the information. In the case of authentication, which is usually tied with integrity, you're not actually encrypting the information, you are, in effect, sealing or locking down the message as yours. This prevents third parties from claiming your identity or tampering with something that was originated by you. In fact, even if you were to lose your key or worse yet, you were no longer in existence, your authentication of the message or document persists just as your written signature on paper does.

The other element of PKI is the Certificate Authority. This is ultimately a service organization of some type with the software in place to provide “key pairs” (public and private) to individuals or to computer systems. We will discuss the role of the CA later in this document.

What Is Asymmetric Cryptography?

Asymmetric cryptography (a specific cryptographic system type) provides the technical foundation that makes a Public Key Infrastructure (PKI) possible. It not only secures information in transit; it can also be used as a means of authenticating the identity of the person that sent the document. In doing so, a digital signature can also be used to verify that information sent has not been altered after it is signed.

Cryptography in general is the science of creating and identifying code systems intended to scramble a readable message containing information (paper, email, etc.) so that the message cannot be understood by anyone other than an intended party.

Historically most cryptographic systems have been symmetric. This means that a code is used to scramble a message and the exact same code must be used to de-scramble it at the receiving end. It also means that both parties must know the code in use. This need to communicate the code becomes the source of compromise in the system. Once the code is discovered, captured messages can be translated.

Asymmetric cryptography is very different. In this system, a pair of codes (also called keys) is used to scramble and de-scramble the message. In most instances you would use the *public* key of the person (or system) you want to communicate with to scramble the message. This key is generally available and might even be published in a directory. The public key has an associated *private* key that is in the exclusive possession of the receiving party. When their message arrives only the private key can be used to read the message. Your private key must be kept private if it is to be effective to its purpose. If your private key is in the control of anyone else it can be used to open messages intended for you.

This is not the only way to use this technology. As described, it can be an effective tool to secure a message from being used by an unauthorized third party. However, what if you must be certain that the message is legitimate and from a source you can validate?

To achieve the goals of legitimacy and authenticity we also use asymmetric cryptography to create digital signatures. You could use your private key to "sign" a document you want to authenticate as having originated by you. In this instance, the public key is used to validate the signer or sender. Your private key must be secured just as you would make sure a rubber stamp with your physical signature was protected.

The various ways this technology can be implemented is the source of considerable confusion. This confusion is further compounded by the fact that by the fact that asymmetric cryptography is also used as the technical underpinning for digital certificates. This is further exacerbated by the fact that digital certificate as a term is occasionally used interchangeably with digital signature.

What Is A Signature?

Before explaining what a digital signature is, it is worth noting what the traditional signature is and the purposes it serves. Historically, a signature is any mark made by a person that is "intended" to be theirs. English common law (on which much of our law is based) has defined not only what a signature is but also what purpose it serves. This has been discussed in a number of American Bar Association articles and summarized as follows:

Evidence	A signature authenticates a writing by identifying the signer with the signed document. When the signer makes a mark in a distinctive manner, the writing becomes attributable to the signer.
Ceremony	The act of signing a document calls to the signer♦ attention the legal significance of the signer♦ act, and thereby helps prevent inconsiderate engagements.
Approval	In certain contexts defined by law or custom, a signature expresses the signer approval or authorization of the writing, or the signer intention that it have legal effect.
Efficiency & Logistics	A signature on a written document often imparts a sense of clarity and finality to the transaction and may lessen the subsequent need to inquire beyond the face of a document. Negotiable instruments, for example, rely upon formal requirements, including a signature, for their ability to change hands with ease, rapidity, and minimal interruption.

What Is A Digital Signature?

There has been some confusion on what the definition of a digital signature is. More recently, this confusion has been resolved with most people distinguishing between an electronic signature, digital signature and digital certificate. The following definitions are generally agreed to:

Electronic Signature	This can be nothing more than a Personal Identification Number (PIN) or a bitmap of the user's signature on a document. In some cases, the use of the PIN and the application of the bitmap may involve some type of biometric identification of the user to help insure the signature is genuine and is not later repudiated. In the end however, all that is accomplished is

another layer of password based security where the password might be a retinal scan or fingerprint. Electronic signatures have no built in functionality that would verify whether a document has been altered since it was signed that can work on a broad basis. Where biometrics are concerned, every user would require a software application to get validation. This is impossible to implement on a large scale although it may work very well in closed environments such as within a given organization. Keep in mind however that if an electronic signature is an indication of the signers intent and it is not repudiated, it will stand with the full force of law as a legitimate signature.

Digital signature

A digital signature is generally more acceptable than an electronic signature because it provides signer and document authentication. Signer authentication is the ability to identify the person who digitally signed the document. Document authentication ensures that the document or transaction cannot be altered as a result of the digital signatures invocation. Digital signatures are created and verified by the use of two different keys, one private and one public as described in the discussion of asymmetric cryptography.

When you apply your digital signature to a document, it is used to create a hash value exclusive to the combination of your signature and the specific document. If the document were altered in any way, this hash value would not match and the document would be invalid and (in effect) lose the signature. Because it is computationally infeasible to derive one key from the having other, digital signature has great integrity. Consequently, it is legally more acceptable than an electronic signature.

A digital signature looks like a random series of numbers and alphabetical characters. Each signature is unique because it uses the content of the electronic document to create the character string. An example of a digital signature is:

--------- BEGIN SIGNATURE ---------

idkflkmejsdaoiB441klklk08+kadlkdflioe993+1alkfdlasd4k
srlk41ksafj81kadfkl61ardlfj+kd akljfl61adfldfjl+adfsdfddf+

--------- END SIGNATURE---------

Digital Certificate

A *digital certificate* (or digital ID as it is sometimes called) is an electronic ID file, operating like a driver's license or passport. It is meant to certify that the certificate issuer is who or what (since it could be another computer system rather than a person) they claim to be. A digital certificate acts like an electronic envelope in which the public key travels. The digital certificate is issued by a Certificate Authority and signed with that Certificate Authority's private key, authenticating the public key.
The digital certificate generally includes the following:

- Public key and the corresponding owner's name.
- Certifying Authority that issued the key.
- A serial number

- The digital signature of the Certificate Authority, signed using the Certificate Authority's private key.
- Other optional identifying information that might be required by a Certificate Management Policy.

The digital certificates cannot be altered, with the Certificate Authority making it tamper-proof through the strength of the authentication from their digital signature.

Digital Certificate versus Digital Signature

The digital certificate is sometimes confused with a digital signature because they both make use of asymmetric cryptography. The digital certificate authenticates a public key and identifies the owner of that key. The digital certificate may also answer the question "who" is authorized to use the key.

The digital signature provides a means to electronically replace a handwritten signature. The digital signature is used to authenticate a specific document or transactions, and the person, company or system that created the transaction.

What Is A Certificate Authority?

A CA is any service provider that takes responsibility for the issuing and maintenance of key pairs also referred to as certificates. The most comprehensive services will provide the full range of activities associated with PKI. This includes at least the following:

Secure Facility A minimum qualification of any CA that will be providing key pairs is a secured facility where the data systems maintaining them are protected physically from outside threats and operationally from service disruption. A goal of 100 percent availability with achievement in the range of 99.999 percent is a typical requirement.

Key Issuance The CA provides keys at a wholesale or retail level. Basically, this means that they maintain a listing of who was issued a key pair and a copy of each public key. At the wholesale level this means that they simply provide the keys to a Registration Authority (RA). The RA in turn is responsible for assigning a specific key set to a party. At the retail level it means that they would also make the assignment.

Registration This is also called Vetting but by either name, it is the process associated with establishing some level of identity with the party to whom a key pair is associated. This function might also be performed by a Registration Authority. A RA would work in cooperation with a CA by providing the customer interface to complete the key assignment transaction for which the CA provides the technical infrastructure. The extent of the process can range from nothing more than establishing a email address to requiring an applicant to appear in person with photo identification, birth certificate and other forms of proof including finger prints. The type of Vetting required is called for in a formal structure called a Certificate Policy described later in this document.

Repository Housing the public keys of assigned key pairs is an ongoing task that involves maintaining keys and the associated identities behind them.

This may also involve (in cooperation with affiliated RA's) renewal and revocation of keys and long term retention of expired keys.

Key Access The public keys of registered parties must be available from the CA along with the associated registration information. In effect, the CA acts as a clearinghouse by validating keys or making them available. This is sometimes referred to as "publishing" and may be part of the repository function when the CA functions have been distributed to multiple third parties.

Certificate Management Policy

Having a CA in place and ready to issue certificates (key pairs) is not enough to complete the PKI environment. There must be guidance to both CA and affiliated RA's on the type of keys that must be made available and the registration (vetting) process associated with each level. The American Bar Association (ABA) in their discussion of digital signatures refers to this as "reliance levels".

Just as there are times when you apply of your physical signature seriously (contract to buy a house) or indiscriminately (birthday card), so too your digital signature(s) may have a variety of purposes. Along the same line of reasoning, there are times when your physical signature must be notarized to insure the signer's identity is validated and as a safeguard against repudiation (you deny you signed the document). In the digital world, these reliance levels are intended to provide the same range of purpose and security.

The certificate management policy also provides direction to CA and RA's regarding key (certificate) retention, expiry, revocation and renewal requirements.

Once a CA has the direction from the certificate management policy, it may be incorporated into a larger Certificate Authority Practice Statement. This document speaks to the operational issues regarding such issues as security of the facility, systems availability, audibility and information protection and privacy

What Is The Opportunity For Kansas

As discussed in the overview, the growing need to maintain electronic information whether in data or document form has become increasingly critical to agency operations. Conversion to and management of paper costs Kansas millions of dollars annually. Paper based operations require transactions that can only be resolved by "in person" appearance of parties to these transactions. This is unnecessarily inconvenient, time consuming and costly for both the government and the constituencies it must serve.

Implementation of digital signature infrastructure is expected to have a number of positive results for Kansas. Among these benefits are an ability to;

- Provide more efficient delivery of government services.
- Enable traditional commerce to be conducted electronically such as with routine banking services.
- Better protect privacy of information used in Government business.
- Improve the States competitive stature in the international marketplace.
- Secure private Email.
- Provide workflow automation using electronic forms with signatures for state agencies to work more efficiently with each other.

- Broader distribution of Kansas based products and services.
- Legally binding electronic contracts.
- Reduced administrative costs for all agencies by eliminating the need to manage the redundant paper based document infrastructure.
- Smooth out seasonal spikes in workloads created when large numbers of citizens must file or appear to perform state required transactions.