South Dakota Legislative Research Council

Issue Memorandum 97-2

Digital Signatures

Introduction

The use of digital signatures is becoming more prevalent across the country and internationally. As a result, it is increasingly important for lawmakers to be aware of the technology, its capabilities, and its drawbacks. Legislation which seeks to address digital signatures has varied greatly. There are also those who believe such legislation is premature. Before beginning a discussion of digital signatures, they must first be distinguished from electronic signatures. A digital signature is but one type of electronic signature. Other types of electronic signatures are digitized renditions of inked signatures and biometric signatures using fingerprints or retinal scans which may be scientifically traced to a particular person. Digital signatures are the most established form of electronic signature and of those states that are enacting laws and implementing methods to deal with this technology, the vast majority are addressing digital signatures. What follows is an overview of digital signatures intended to aquaint the reader with the technology and what some states are doing to address this emerging technology.

Digital Signature Technology

A digital signature is created by using a system which provides a secure key pair consisting of a private key and a public key. The private key is known only to the signer and is used to create the digital signature. The public key is generally more public and is used to verify the signature. The two keys are mathematically related but one cannot be used to derive the other. Computer equipment and software using a private key and public key is often referred to as an asymmetric cryptosystem. A digital signature is a transformation of a message using an asymmetric cryptosystem--a key pair system--so that a person having the initial message and the signer's public key can accurately determine whether the transformation was created using the private key that corresponds to the signer's public key and whether the message has been altered since the transformation was made.

The use of a digital signature thus involves two steps, that of creation and that of verification. The signer creates the digital signature, a process that consists of applying the private key of the sender to the contents of the message. The receiver then must verify the message, that is, check the digital signature by referring to the message and the public key.

A hash function is used to both create and verify a digital signature. A hash function creates a digest of the message which is usually much smaller than the message, yet unique to it. If the message changes, the hash result will be different. This digesting of the message is important because the signed message itself is usually too large. The hash function enables the software creating digital signatures to operate on smaller amounts of data, while still providing sufficient correlation to the original message.
To begin the process the signer must first delineate the message. The hash function

then computes a hash result or a code unique to the message. The hash result is then transformed into a digital signature by reference to the signer's private key. This is often referred to as encryption. As noted above, this digital signature is unique to both the message and the private key used to create it. Usually, the digital signature is attached to the message; however, they may be stored separately as long as there is a reliable association between them. Since a digital signature is unique to its message, it is useless if disassociated from the message.

Verification is accomplished by computing a new hash result of the message by using the same hash function used to create the digital signature. Then the verifier, with the public key, checks to see whether the digital signature was created using the corresponding private key and whether the new hash result matches the hash result derived from the digital signature. If the hash results are the same, the message is verified. If they are not, the message is a forgery or was tampered with after the signature was attached. Verification indicates not only that the digital signature was created with the signer's private key but also that the message has not been altered since it was signed.

Certification Authorities

Underlying this process is the premise that some remote party is reliably identified. To guard against imposters or disavowal of a digital signature if the transaction turns out to be disadvantageous for the purported signer, the verifier must not only obtain the public key but also have assurance the public key corresponds to the signer's private key. Since the key pairs are simply a data string, they have no intrinsic association with an individual. Yet some association must be made between the key pair and a particular person. But identifying a remote party takes considerable effort especially when the parties are geographically distant, communicate over an insecure network, or are corporations or some similar entity rather than natural persons. To assure each party is identified with a particular key pair, some trusted third party, usually referred to as a certification authority, must associate an identified person on one end with a key pair creating the digital signature received at the other end, and vice versa.

A certification authority issues a certificate to associate a key pair with a signer. The certificate is an electronic record that identifies the certification authority issuing it, contains the public key, and names or identifies the signer holding the corresponding private key. To assure the authenticity of the certificate, the certification authority digitally signs it. This digital signature on the certificate can be verified by using the public key in another certificate.
Certificates may be published in a repository to make the public keys and their association with a particular person available. A repository is a database of certificates which can be retrieved to verify signatures.

If, after a certificate is issued, it becomes unreliable for any reason, the certification authority may suspend or revoke the certificate. A certificate may become unreliable if the proper signer loses control of the private key by either divulging it or losing a computer card and its associated password. Also, a company may terminate or lose an employee who has a certificate issued in its name. In any such case the certification authority should be notified so that it can provide notice of the revocation or suspension.

Using Digital Signatures

The authentication of digital signatures interrelates technology and the law. Signatures have special significance in legal transactions. Certain formalities are generally required for legal transactions to be valid. These formalities include documentation of the transaction and a signature or other form of authentication. A signature is not part of the substance of a transaction but a representation of it. A signature serves several legal purposes. A signature identifies the signer with the signed document making it attributable to the signer. It also draws attention to the legal significance of the event. Often, a signature shows approval of the writing, evidencing an intention of legal effect. A signature also denotes finality.

These legal purposes are achieved if the signer and the document can be authenticated and the transaction is marked by an event. A signature should indicate who signed the transaction and should be difficult for anyone else to reproduce without authorization. The signature should identify what is signed and both the signature and the transaction itself should be virtually impossible to alter. The signature should mark an event, signify approval, and consummate a transaction.

Digital signature technology can provide these results. The signer can be identified by the private key if the public and private key pair are properly associated by a reliable certification authority. Since the process of signing digitally identifies the substance that is signed, digital signatures provide authenticity to the transaction as well. Moreover, verification indicates whether the message has been tampered with. As for marking an event, the signer must provide a private key so that software can produce a digital signature. This can be used as signifying the consummation of the transaction.

All this can be done with a high degree of assurance without greatly increasing costs. Implementing the technology of digital signatures does comes with certain costs. There are costs associated with establishing certification authorities and oversight, whether it be by professional accreditation or governmental regulation or other means. There are also costs associated with the software used to create and verify digital signatures.

Legislation Addressing Digital Signatures

Digital signatures have the potential to provide reliable authentication. If properly implemented, digital signatures would minimize the risk that the other party is an imposter and that the substance of the transaction itself has been altered. However, for this to be true, the certification authority must have reliable information. In addition, the certification authority itself must be reliable. A few states have enacted laws to license certification authorities to address this issue.

Legislation addressing the use of digital signatures ranges from very comprehensive to quite general. Utah and Washington have enacted comprehensive laws which include provisions for certifying, validating, and relying upon digital signatures. Utah was the first state to authorize the use of digital signatures for commerce. The law, first enacted in 1995, governed the use of public and private key pairs and certification authorities. The law was substantially amended in 1996 with regard to authentication to include such items as certification requirements; enforcement responsibilities; obligations of certification authorities; suspension, revocation, and expiration of certificates; signature

requirements and presumptions in adjudications; repositories and their liabilities; and performance audits. Utah has selected a vendor to develop a repository and provide digital software and certification authority for the state.

Those states that have adopted less comprehensive laws include Arizona, California, Mississippi, New Mexico, and Virginia. The laws of each of these states vary greatly. California, for instance, narrowed its law to govern only digital signatures affixed to communications with public entities. The law provides that a digital signature has the same effect as a manual one if it is unique to the person using it, capable of verification, under the sole control of the person using it, and linked to the substance so that any alteration invalidates the signature. In addition, the digital signature must conform to regulations promulgated by the Secretary of State.

Still other states have enacted legislation pertaining to electronic signatures generally, with digital signatures as merely one alternative. Florida and Georgia are two examples. Florida authorized the Secretary of State to be the certification authority and required a study of the use of digital signatures for commercial purposes. The resulting report of the study did not recommend comprehensive legislation, concluding that while licensure of certification authorities may be necessary in the future, there is no immediate demand for the service. The report further recommended that the Legislature authorize the Secretary of State to establish a voluntary system of licensure of certification authorities when it is clear that it is necessary.

Conclusion

The emerging technology of digital signatures can provide a computer-based alternative to traditional signatures for a wide variety of transactions. With a secure key pair, a message can be transformed to a code that remains private until it is received at its intended destination. With this key pair also comes verification of the contents of the message itself. This all rests on reliable authentication, making the credibility of certification authorities imperative. A number of approaches have recently been enacted as states grapple with this emerging technology. For all the advantages and disadvantages of these approaches, there are several concerns surrounding any legislation aimed at digital signatures. Some contend that legislatures are enacting legislation without a common vision when it is important that these systems be compatible. Another concern espoused is that restrictive statutes could not keep pace with the technology. Others believe it is premature for states or any governments to legislate electronic commerce. Ultimately, lawmakers are left with the challenge of deciding how best to deal with this technology that is sure to have a profound impact on all our lives.

This issue memorandum was written by Jacque Storm, Senior Legislative Attorney for the Legislative Research Council. It is designed to supply background information on the subject and is not a policy statement made by the Legislative Research Council.