**Electronic And Digital Signatures**

**Summary**
The advent of e-government and e-services is changing the way we do business. Traditionally, we created records on paper and we authenticated a record by signing it in ink. Today, technology is making both paper and ink irrelevant to many business processes.

This has all sorts of consequences, but, whether in ink or in an electronic format, a signature must fulfill the same functions: it has to authenticate the signer and the document. To use electronic signatures effectively, you need to select the appropriate technological application and make sure they meet these legal obligations. Because signatures are important for their legal and evidentiary value foremost, legal concerns must be the guiding factor in the selection of technologies.

Since different laws affect different agencies and governmental functions, you will need to define your legal needs and connect them to your business processes before deciding which electronic signature application is appropriate for you. In addition, you need to consider your technology architecture, since that application has to work with all the others that create, preserve, and make available your records. As you implement an electronic signature application, you will need to document the key features of the system in order to demonstrate its trustworthy operation and establish its evidentiary value.

**Key Concepts**
When selecting and implementing an electronic signature technology, keep in mind:

- Legal and technological definitions
- Functions of signatures
- Additional legal considerations
- Electronic signature technologies

**Legal and Technological Definitions**
There is a problem with the terminology we use. In Minnesota and in most states, there is a clear legal distinction between the definitions of “electronic signature” and “digital signature.” This distinction is not made in other forums, especially among information technology communities, where “electronic” and “digital” are used synonymously and interchangeably. Since signatures are important because of their evidentiary value, there should not be any confusion about a technology you might have to describe before a judge.

In Minnesota, these are the important statutory definitions:
Minnesota Statutes, Chapter 645.44 Subd. 14 (available at: <http://www.revisor.leg.state.mn.us/stats/645/44.html>) contains the basic and traditional definition of a signature:

The signature of a person, when required by law, (a) must be in the handwriting of the person or, (b) if the person is unable to write, (i) the person's mark or name written by another at the request and in the presence of the person or, (ii) by a rubber stamp facsimile of the person's actual signature, mark, or a signature of the person's name or a mark made by another and adopted for all purposes of signature by the person with a motor disability and affixed in the person's presence.

A reliance on this definition would make it virtually impossible to use technology to deliver services and to meet all legal and evidentiary requirements at the same time. To address this problem, and to provide a standard approach to the use of electronic signatures, Minnesota adopted the Uniform Electronic Transactions Act (UETA) in the 2000 legislative session [Minnesota Statutes, Chapter 325L] (available at: <http://www.revisor.leg.state.mn.us/stats/325L>). UETA defines electronic signatures as:

An electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record.

This definition is not technology specific, and so does not mandate the adoption of any particular hardware or software application. Any technology, theoretically, that could authenticate the signer and the signed document could generate a legally admissible signature, if the parties could demonstrate the trustworthiness of the process that created and preserved the records in question.

Another approach has emphasized the use of a specific application, public key infrastructure (PKI). The Minnesota Electronic Authentication Act [Minnesota Statutes, Chapter 325K] (available at: <http://www.revisor.leg.state.mn.us/stats/325K>) defines a digital signature uniquely in terms of PKI. A digital signature is:

A transformation of a message using an asymmetric cryptosystem such that a person having the initial message and the signer's public key can accurately determine: (1) whether the transformation was created using the private key that corresponds to the signer's public key; and (2) whether the initial message has been altered since the transformation was made.

Digital signatures are a particular type of electronic signature. The advantage a digital signature may offer is that, by providing a unique identifier and linking the signature to the record, it can authenticate both the signer and the signed document. This promises to meet legal requirements for admissibility and trustworthiness. A further advantage is that PKI technology can be adaptable to a wide range of applications and so can work with basic office software.
Functions of Signatures
Signatures serve specific functions. The American Bar Association enumerates these as:

- **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's attention the legal significance of the signer's act, and thereby helps prevent inconsiderate engagements.

- **Approval**: In certain contexts defined by law or custom, a signature expresses the signer's approval or authorization of the writing, or the signer's intention that it have legal effect.

- **Efficiency and 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.

An electronic signature will have to fulfill some or all of these functions. You should determine which are pertinent to your business processes before selecting a particular electronic signature technology.

Additional Legal Considerations
Many government agencies and functions have unique and specific legislative mandates. These very often include particular concerns for signatures. A simple search of the online version of the Minnesota Statutes for the keyword “signature” generated hundreds of references. You should thoroughly research the statutes applicable to your agency and functions before making any choices about electronic signature technologies.

For example, a federal law, HIPAA, the Health Insurance Portability and Accountability Act of 1996, is concerned with non-repudiation. Non-repudiation “provides assurance of the origin or delivery of data,” so that the sender cannot deny sending a message and the receiver cannot deny receiving it. This prevents either party from modifying or breaking a legal relationship unilaterally. HIPAA holds that only a digital signature technology can currently provide that assurance.

In addition, there are a number of statutes pertaining to government records which you need to understand because any document signed in the course of an official transaction becomes a government record. The most important are:

- **Official Records Act [Minnesota Statutes, Chapter 15.17]** (available at: <http://www.revisor.leg.state.mn.us/stats/15/17.html>), which mandates that government agencies must keep records to fulfill the obligations of accountability and specifies that the medium must enable the records to be permanent. It further stipulates that you can copy a record and that the copy will be legally admissible in court.

• Minnesota Government Data Practices Act (MGDPA) [Minnesota Statutes, Chapter 13] (available at: <http://www.revisor.leg.state.mn.us/stats/13/>), which mandates that your records should be accessible to the public unless categorized as not-public by the state legislature.

• Uniform Electronic Transactions Act (UETA) [Minnesota Statutes, Chapter 325L] (available at: <http://www.revisor.leg.state.mn.us/stats/325L/>) and Electronic Signatures in Global and National Commerce (E-Sign), a federal law (available at: <http://thomas.loc.gov/cgi-bin/query/z?c106:S.761:>). Both UETA and E-Sign address the issues of the legal admissibility of electronic records created in a trustworthy manner and the application of the paper-oriented legal system to electronic records.

For more information on the legal framework you must consider when developing an electronic signature technology, refer to the Introduction and Appendix D of the Trustworthy Information Systems Handbook.

Electronic Signature Technologies
The Uniform Electronic Transactions Act (UETA) [Minnesota Statutes, Chapter 325L] (available at: <http://www.revisor.leg.state.mn.us/stats/325L/>) purposely allows for a wide range of signature technologies. It says, “An electronic record or electronic signature is attributable to a person if it was the act of the person. The act of the person may be shown in any manner, including a showing of the efficacy of any security procedure applied to determine the person to which the electronic record or electronic signature was attributable.”

An example of this is the “click through” option used on many web sites. To order a product, be it a shareware application, an airline ticket, or a book, a web user has to “click through” a page or form that indicates approval of the vendor’s conditions for the sale. The system makes it impossible to transact any business without first establishing that agreement. In this instance, there is no “signature” or anything like it. Instead, the system is designed to make it necessary to move from “A” to “C” only through “B,” with “B” serving as the equivalent of a signature. Authentication is demonstrated by the documentation of the system and its procedures, not by a signed record of a specific, individual transaction.

UETA implicitly legitimates the use of more familiar technologies, such as faxes and imaging, and more exotic ones, such as iris scans, for electronic signatures. In all cases, the key to demonstrating the trustworthiness of a record and its signature is demonstrating the trustworthiness of the system that creates and manages the record. Having sufficient and appropriate systems documentation is the only way to achieve this.

Digital signatures demand the use of a specific technology, PKI. PKI uses two different keys. One key is kept secret (the private key) and the other key is made publicly available (the public
Electronic Records Management Guidelines
Electronic and Digital Signatures

key). The two keys are generated simultaneously and collectively; they are known as a “key pair.” Once a message has been signed using one of the two keys, it can only be verified by the other key. The resulting digital signature is a cryptographic checksum computed as a function of the message and the signer’s private key.

Because the digital signature is generated as a function of the key and a unique message, the signature serves two purposes. It authenticates the signer, since only the individual owner has (in theory, anyway) access to the private key. It also indicates the reliability and integrity of the message, since any alteration to the text would invalidate the signature.

This is not the same as encryption. PKI technology was originally developed for encryption (as in the Pretty Good Privacy applications), but the use of a digital signature does not automatically encode a message. In fact, encryption is not covered in the Minnesota Electronic Authentication Act [Minnesota Statutes, Chapter 325K] (available at: <http://www.revisor.leg.state.mn.us/stats/325K>); that only addresses the use of PKI for digital signatures.

The effective use of PKI for digital signatures relies on some policy and organizational factors. There has to be some way to guarantee and to prove that a specific person actually owns a specific key. And there has to be some way to provide quick and easy access to public keys. Because it is completely impractical for each sender and each recipient of a message to work this out on a case-by-case basis, the use of PKI for digital signatures is dependent on the operation of certificate authorities.

A certificate authority is an independent, trusted third party who issues and manages key pairs. To get a key pair, individuals must prove to a certificate authority that they are who they claim to be. The certificate authority also provides secure access to public keys that allow for the validation and verification of signatures. The Minnesota Electronic Authentication Act [Minnesota Statutes, Chapter 325K] (available at: <http://www.revisor.leg.state.mn.us/stats/325K>) creates a mechanism to license and regulate certificate authorities.

Key Issues to Consider
No electronic signature technology in and of itself is sufficient to meet your legal needs. The evidentiary value of your signed records will ultimately rely on your ability to produce legally admissible documentation of your recordkeeping system. In addition, you will, of course, have to produce the electronic records themselves. Just preserving and providing access to electronic records present some daunting challenges. (For more information, refer to the Electronic Records Management Strategy guidelines). Adding electronic signatures to the equation can complicate the situation even further.

Every option available to you has its own advantages and disadvantages. Some issues are constant, though:
• Consider technology obsolescence: hardware and software become quickly outdated, often making it difficult, if not impossible, to preserve and provide access to older electronic records. If you are using two different technologies to create and to sign a record, they might “age” at different rates.

• Plan to document your decisions and transactions: understanding your legal needs and addressing them at the design phase of an application are keys to making this work. Keeping documentation up-to-date is an on-going responsibility, which could be complicated if you are relying on a third party. If you are using digital signatures, for example, you need to make sure that your certificate authority is managing its records and documentation adequately.

• Make sure that your electronic signature technology is interoperable with your and your constituencies’ other software applications: requiring complex or expensive solutions is probably not practical. It would be especially difficult to ask citizens to buy and maintain multiple signature technologies.

• Evaluate risks and allocate liabilities: one of the functions of signatures is to provide the evidence of agreement to a transaction. There is no guarantee, either with paper or electronic signatures, that all parties will be one-hundred percent satisfied with the results all the time; litigation will always be with us. Because of that, you should understand the risks any system presents and you should manage the liabilities that result.

• Remember that the human side of the equation is critical: no technology will completely address your legal requirements. For example, despite all its attractive features as a technology, a digital signature is only as reliable as the certificate authority standing behind it.

Overall, selecting the appropriate electronic signature technology means defining the criteria you consider important and then determining if your system and proposed application meet those criteria. The criteria should give priority to legal concerns, since signatures are primarily valuable for evidentiary purposes. But your assessment should include the consideration of other factors, such as technology architectures, costs/benefits, your business practices, and all the policies, hardware, software, controls, and audit procedures that are pertinent.

For a model of and methodology for system development and assessment, refer to the Trustworthy Information Systems Handbook. For a specific example of the criteria pertinent to a digital signature application, see the American Bar Association’s PKI Assessment Guidelines (See the Annotated List of Resources at the end of these guidelines).

Discussion Questions
• Why do you want to use electronic signatures? What business functions will the technology support?

• Who will have to use and rely on the electronic signature?
• How long will the signatures and the records to which the electronic signatures are affixed have to be preserved?

• Which state and federal statutes pertain to the functions and transactions that generate your signed records? What case law is there?

• How does the electronic signature technology fit into your overall technology architecture? What’s the total cost of the technology? What’s the cost per transaction?

• What sort of electronic signature technologies do your customers use? Will you have to share these records with any other organizations or agencies? What technologies do they use?

• What methodology will you use for documenting your information systems, policies, and practices?
Annotated List of Resources

Primary Resources
<http://www.abanet.org/scitech/ec/isc/dsg-tutorial.html>

In 1996, the ABA’s Section on Science and Technology produced the first legal overview of electronic and digital signatures, as well as related concerns. Although there have been many legal and technological developments in the years since, the site still contains fundamental information on signatures that is of value. The term “tutorial” is slightly misleading; this is basically a short essay, but it is the best introduction to signatures available. It has recently been complemented by the ABA’s PKI Assessment Guideline.

<http://www.abanet.org/scitech/ec/isc/pag/pag.html>

The Information Security Committee of the Electronic Commerce Division of the ABA issued a draft version of its PKI Assessment Guidelines (PAG) in 2001. The PAG offers a practical guide for the evaluation and assessment of PKI systems and vendors. This is a very detailed document, almost four hundred pages long. It is available as a PDF file. As noted, it is currently a draft and will be updated in the future.


Blanchette’s paper provides a succinct overview of digital signature and evidence law in the United States and Europe, along with an examination of the signature lifecycle and the technical preservation problems facing the archivists and the cryptographic community.


McBride Baker & Coles is Chicago law firm with an interest in information technology and the law. The Legislative Analysis Database for E-Commerce and Digital Signatures is a set of tables that allow for the comparative analysis of practices in different states. These tables systematically list and distinguish enacted digital signature legislation and uniform laws. The firm’s e-commerce site provides a variety of other tables for study of pertinent issues around the world.
Electronic Records Management Guidelines
Electronic and Digital Signatures

<http://www.mnhs.org/preserve/records/tis/tis.html>

This handbook provides an overview for all stakeholders involved in government electronic records management. Topics center around ensuring accountability to elected officials and citizens by developing systems that create reliable and authentic information and records. The handbook outlines the characteristics that define trustworthy information, offers a methodology for ensuring trustworthiness, and provides a series of worksheets and tools for evaluating and refining system design and documentation.

<http://csrc.nist.gov/encryption/tkdigsigs.html>

NIST’s web site provides access to three Federal Information Processing Standards (FIPS) standards for digital signature algorithms, along with a variety of other resources on cryptography.

Additional Resources

HIPAA, the Health Insurance Portability and Accountability Act of 1996, has created a small industry of guidelines, consultancies, and web sites devoted to explaining how its mandates can be implemented. This site provides easy access to the rules created by the Department of Health and Human Services for “standards for the security of individual health information and electronic signature use by health plans, health care clearinghouses, and health care providers.” Since so many important government functions are related to health care, HIPAA’s requirements will probably heavily influence the development of standards and technology architectures for electronic signatures.

<http://www.secstate.wa.gov/ea>

Washington’s digital signature law was a model for a number of other states, including Minnesota. The Secretary of State oversees the implementation of the law and particularly the regulation of certificate authorities. The web site includes useful information and resources on the workings of the law.