ESIGN Electronic Commerce and Electronic Signature Law Clarified.

NOTE: the information in this document is provided for convenience only and does not constitute legal advice or a guarantee about the compliance or noncompliance of any electronic process or technology with any relevant or applicable laws or about the content, spirit, letter, or interpretation of these laws. Consult a legal expert before making decisions about the legal ramifications of eSignature technology in your application.

ABSTRACT

In the year 2000, spurred by the interests of businesses and government agencies looking to achieve greater efficiency through electronic transactions, Congress passed the Electronic Signatures in Global and National Commerce Act (ESIGN) to allow greater freedom and flexibility to implement electronically signed transactions. ESIGN is intentionally broadly defined and technology-neutral, allowing entities the freedom to utilize whatever technological means they deem appropriate to achieve eCommerce solutions. The broad nature of ESIGN seems to make common systems such as email and fax as well as more sophisticated digital encryption and digitized handwritten signature systems viable options for companies desiring to do business electronically. However, since ESIGN essentially specifies only that an electronic record or transaction may not be rendered invalid solely on the basis of its electronic or digital nature it makes no guarantees about the overall enforceability of such electronic contracts. An electronic record is only enforceable if it meets the criteria specified in relevant contract laws as well as the language of ESIGN (ESIGN applies to interstate or government interactions. In-state transactions are bound either by the Uniform Electronic Transactions Act [UETA] or the governing Statexs relevant eSignatures laws, which in some cases are stricter than ESIGN or UETA). Therefore, it is very important for businesses and government agencies to choose their electronic signature technology carefully or risk making agreements that they can not enforce.

This paper explores the requirements of signature laws such as ESIGN and UETA, specific signature technologies, how these technologies satisfy the requirements for enforcement under existing contract law, and how these technologies practically function in open and closed system environments.

REQUIREMENTS FOR LEGAL CONTRACT ENFORCEMENT

For an electronically signed document to be enforceable in court, it must meet the requirements for legal contracts in addition to the electronic signature guidelines specified in the appropriate laws (e.g. UETA, ESIGN, etc.). According to ESIGN, an electronic signature is "an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record." In contract law, signatures serve the following general purposes:

Evidence: authenticates agreement by identifying the signer with a mark attributable to the signer that itself is capable of authentication
Ceremony: act of signing calls attention to the legal significance of the act, preventing inconsiderate engagements
Approval: express approval or authorization per terms of agreement

Authentication can be defined as evidence that a given record, contract, or form is a genuine unaltered written representation of an agreement approved by two or more parties, whether in paper or electronic form. An authentic document contains no evidence of fraud or tampering, such that it may be reasonably concluded that the parties in agreement did indeed assent to the enclosed terms. Assent is evidenced by an attributable, authenticated signature. To be authenticable, the transaction must contain enough information uniquely attributable to the user that fraud, forgery, or validity can be reasonably proven. For an electronic transaction to withstand scrutiny in court, it must meet the definitions and criteria stated above: be capable of authentication and non-repudiation, call attention to the document's legal significance (this is accomplished through the simple act of creating the signature itself), and demonstrate approval of the terms of the agreement. Some electronic signature technologies sufficiently meet these criteria and some do not.

DIGITAL SIGNATURE TECHNOLOGIES

The above conditions for legally-binding signed contracts are best met by more sophisticated systems including asymmetric cryptographic signatures and digitized handwritten electronic signatures. These two methods incorporate technology that makes it possible to authenticate both a signerxs identity and document integrity. Each of these two technologies has unique characteristics that make it well suited for specific applications in open or closed systems. Conversely, simple systems such as fax and email are not well-suited for use where electronic contract enforceability is a critical issue.

PKI Digital Signatures

Asymmetric encryption digital signatures consist of asymmetric encryption keys that are issued by a Certificate Authority (CA) and used to encrypt non-biometric "digital signatures" to electronic documents. Essentially, digital signatures use a 128-digit encryption key to bind a "signer's" identity to an electronic document in place of a unique handwritten signature. Think of it as an encrypted "rubber stamp" to signify approval of an electronic document. This private key is associated with a particular person's computer and can usually be accessed by entering some form of identification, wither a password, PIN, or biometric input such as a fingerprint or handwritten electronic signature capture pad. This system requires that the recipient of a digitally signed document possess a means to de-crypt the message (A public key, disseminated by the owner of a given private key to persons he trusts to view and validate his or her signed electronic documents). A CA serves as a regulatory authority that verifies that a particular encryption key has been issued to the person claiming to transmit a given digitally signed document. It is the private key signature

in conjunction with the claimed identity of the signer and certificate authority that serve to validate and authenticate a document.

Handwritten Electronic Digitized Signatures

Handwritten electronic signature capture systems literally mimic the biometric practice of signing one's name on a piece of paper. Using an active electromagnetic digitizing pen and tablet or stylus and pressure-sensitive pad, a user signs his or her name in an electronic document. The system's tablet and software capture the signature and bind it into the body of the document to prevent changes or tampering after signing. Signature data is stored as encrypted data which contains the precise path of the pen or a signature image and summary biometric measurements. The most sophisticated method of electronic signature capture uses an active digitizing pen and tablet to record pen events up to several hundred points per second. An electromagnetic field determines pen location, so the possibility of pressure error in the sensor can be eliminated. A benefit of this feature is that the sensor can capture signatures through pads of paper, enabling paper forms or contracts to be signed while one party can retain a simultaneously inked paper copy, if desired. The second class of electronic signature capture sensors includes pressure-sensitive pads. Users sign with a stylus directly on the sensor surface. As a result, the signer may need to press harder than they normally would in order to activate the sensor, resulting in an unnatural signature record. Although it is possible to record electronic signature data that is of similar quality to active tablets using this less expensive technology, they tend to be less durable, reliable and functional. Evaluated holistically, electronic signature digitizer systems provide the greatest capacity for authentication and non-repudiation.

Email, Fax, and Other Simplistic Approaches

Conversely, simple general-use systems such as email and fax do not meet the attribution or authentication requirements of electronic signature or contract law. Email is an electronic text-based system in which the user's name is typed into the body of the document with a series of keystrokes which, in turn, create a 'signature.' However, there is nothing in the email to prove that the signer's mark or identity is indeed authentic since any person can type a given name indistinguishably from another person (e.g. if two persons were to type the name "John Q. Fraudvictim" into separate emails and send them, aside from server logs the recipient would not have sufficient evidence to determine which person typed which email; the text is the same). Typing one's name is also a common activity and does not necessarily satisfy the Ceremonial capacity of a signature since it does not require a unique event or process preventing inconsiderate agreements (typing one's name has many purposes, but a signature is reserved for documents of legal significance). The same is true of a typed fax. Attribution is also not achievable in the case of a document that has been signed by hand and then faxed to a recipient. The fax that is received bears only a flat image of the original signature with no attributable biometric characteristics that a forensic document examiner would need to make a determination of the mark's authenticity (e.g. hand pressure, stroke speed, etc.). Additionally, the document itself may be altered with a previously existing signature or signature image "pasted on" to a document and then faxed, with the proof of the

fraud lost when transmitted electronically and printed out on the receiving end. As such, even though ESIGN and other signature laws do not express that these systems are unacceptable for conducting electronic commerce, it is not at all likely that they are legally enforceable (some states, including California and Utah, have passed laws that are not technology neutral and imply that only more sophisticated electronic signature systems are valid for use in that state). While they might serve as an acceptable method for "keeping honest people honest," they will not satisfy non-repudiation requirements and should only be used in situations that are of very high trust where little of real value is at stake in a closed system, and should never be considered for use with high-value agreements of any kind or in any open system.

DIGITAL SIGNATURE TECHNOLOGY IN OPEN AND CLOSED SYSTEM ENVIRONMENTS

Perhaps the most important factor in deciding which technology is best for a given application is to determine whether the electronic transactions will be taking place over a closed or open system. A closed system can be defined as an environment where all parties involved have knowledge and a degree of familiarity with one another, possibly built over time with a repetition of transactions or where all parties are agents of the same entity. Government agencies, corporate departments, or familiar business entities are examples of closed systems – no input from outside this xcircle of trustx is necessary to complete a transaction or agreement. Conversely, open systems consist of actors that either have no previous experience with one another or have an anonymous-type relationship, as in almost any situation involving the general public. Brick-and-mortar or Internet retailers, mortgage brokers, and unfamiliar business entities are examples of open system users who have little ability to make determinations about clients or customersx identity when completing face-to-face or remote electronic agreements. Open systems require an extra degree of security and authentication ability as a result, unlike a relatively secure closed system where the identity and intent of all parties is widely known and accepted. PKI works best in closed systems where there are other structural checks and balances and where multiple levels of approval are present. Without this, a single compromised PKI key can result in disaster. It is the differences in the natures of these two systems that make different electronic signature technologies better- or worse- suited to enable true, secure, legally enforceable electronic transactions in an open system.

Closed System and PKI

In a closed system such as a government agency, corporate department, or where two parties have a history of trustworthy interaction, asymmetric cryptography systems like PKI digital signatures have a better chance of being effective. A receiver can be fairly certain that the person they are dealing with is a legitimate party acting in good faith. A digitally signed document is also encrypted in such a way as to make tampering unfeasible, preserving the authentication of the agreement. The person-specific nature of the digital signature's private key makes attribution possible via the CA. Additionally, there is no disincentive to institute an integrated system of PKI and digitized signatures for added security, since all the benefits of digital signature

encryption can be coupled with the non-repudiation capability of digitized electronic signatures.

Closed System and Digitized Electronic Signatures

Digitized electronic signatures function at least as effectively as PKI digital signatures in closed system environments, but present several unique operational advantages. For example, digitized electronic signatures can be implemented much more inexpensively than PKI digital signatures because extra keys do not need to be purchased for each user, nor does a certificate authority need to be paid to provide signature certification. Also, since no environment is totally insular, even a closed system requires some degree of open-system interface (purchase orders, for example). Therefore, even in a closed system, open system problems can surface and make PKI signatures a less attractive option, as illustrated below.

Open System and PKI

In an open system (and potentially in a closed system as well), digital signatures present several challenges to secure and authenticable operation. Like a PIN, a digital signature bears no biometric or authenticable information. It is only a series of number that can be accessed and used by anyone able to gain access to the computer on which it is stored. As a result, it would be impossible to detect a fraudulently signed document since each individual encrypted signature is identical. Additionally, a digital signature is only as accurate and reliable as is the CA or local system administrator issuing the private key. It would be very easy for a dishonest CA or administrator to create extra keys for their own use or to reveal or duplicate an individual's own private key for fraudulent use or sale to third parties. Users of digital signature systems must also trust that the person they are accepting a digital signature from has provided accurate and true personal information to an issuing CA, or all signatures from that person would be fraudulent and unenforceable. Since asymmetrical encryption systems are dependent on 1) preservation of integrity and secrecy of private key, 2) reliability, trustworthiness, and security of CA or system administrator and 3) assumption of continued ability of CAs to operate and generate a profit to remain in business, they are not viable options for use in an open system. Asymmetrical encryption systems are only as valuable as the "weakest link" in their usage chain as a result of their unique system architecture.

Encryption-based digital signatures present practical problems in addition to structural shortcomings in open systems. For security and logistical reasons, a user's private key is permanently associated with that user's own identifiable physical computer station. While this may reduce the risk that a user's private key is compromised, it restricts the user's ability to engage in electronic transactions not originating at that single specific computer. The private encryption key is 128 digits in length, making memorization and portability impossible. This makes digital signatures unfit for use in any public environment, e.g. retail POS and healthcare, where users must complete transactions at a kiosk or register terminal. If two parties are to sign an agreement, each must have paid for a digital signature issued by a CA and be at their respective computers. Two parties in the same room, for example, as in a banking or mortgage lending environment, would not be able to each sign the

loan application or closing forms because the borrower would not be at his or her computer at the time of signing. In these cases, digital signature systems actually slow down the electronic document process rather than expedite it and make it more efficient. Since there is no unique biometric data in the digital signature, fraud detection is impossible since all digital signatures from a given computer will be identical regardless of which person is able to gain access and "stamp" a document. To successfully implement a digital signature infrastructure within a given corporation, a secure private key must be bought from a CA for each employee, making costs potentially very high. Many companies also opt to hire an extra information technology professional to maintain the system and keep it secure, because if an encryption-based digital signature stamp becomes compromised the whole system of which it is a part is compromised as well. It is these limitations that, in part, prevent digital signature technology from becoming an electronic signature standard.

Open System and Digitized Electronic Signatures

A technology that provides an open system solution where digital signatures fail is digitized handwritten electronic signatures. Signature capture is a good choice for use with the general public as the act of signing a name is familiar and intuitive, and any user may sign their name electronically on any given tablet without needing to purchase an account or certification from a CA. Additionally, each user's signature is unique to that specific signature instance unlike an encryption key that is indistinguishable across a number of instances. Each user's signature contains pen events attributable to that user which makes fraud detection possible, just as with traditional ink-on-paper signatures. Unlike "rubber stamp" digital signatures, it is virtually impossible to exactly replicate a given electronic signature. If two signatures contain identical biometric data it proves one of them has been fraudulently copied. Additionally, the only investment required to implement electronic signature capture technology is a tablet and software, and one tablet is capable of supporting many unique users. For example, an insurance agent can enroll thousands of clients using only a single tablet.

The most sophisticated and authenticable method of organizing and binding captured electronic signature data is direct storage of the biometric information as a raw, unchanged image-free pen event file which records the path and exact timing of the pen tip during the act of signing. Using this method, all of the original characteristics and biometrics of the handwritten signature are present in the file, which is then bound to the document using an encryption technique that prevents tampering or modification. Each captured electronic signature is unique to a signing instance and can be examined by a forensic document examiner to determine its authenticity using sample paper or electronic signatures as a guide. Speed, timing, and direction of strokes and loops can be verified just as in a paper signature, except that the signature data is directly available without having to be subjectively "lifted" from the paper document, resulting in a truer analysis. This gives captured signatures a huge advantage in determining attribution, as they cannot be stolen or copied (as an exact copy is proof of forgery).

A second method of signature capture binding takes a vector-type file and generates an image of the signature and "pastes" it into the document. The original raw biometric data is discarded in favor of an electronic signature image. While the resulting signature image is more attributable than a PKI digital signature it does not contain any true biometric record of the signature, casting doubt as to whether it can be sufficiently expertly analyzed and authenticated in a court of law. The timings of strokes and loops is not objectively quantified, but rather transformed into a flat image. For this reason, this method is not as reliable or enforceable as the biometric pen data method. To be sure that an electronic signature is attributable and authenticable, as much original unaltered biometric data should be bound to and present in the signed document.

CONCLUSIONS

For reasons of ease of use, low technological and marginal cost barriers, and non-repudiation and authentication capability digitized electronic signatures are a superior system for use in both closed- and open-system environments. Asymmetric encryption is confronted by too many technological and logistical shortfalls to become a viable long-term electronic signature standard. Simple systems such as email and fax serve little purpose and fall short of attribution and authentication requirements for legal enforcement. The single most attributable and authenticable system that complies with both electronic signature legislation and existing contract law is captured handwritten electronic signatures. As a result, investment in a particular dedicated electronic signature system should be a requirement for any business or governmental body looking to implement electronic signature technology.