

Digital Signatures – Best Practice for e-Business Transactions



Digital Signatures and e-Business

New business opportunities have emerged as paper-based transaction systems are moved online. Yet the road to an economy where the vast majority of transactions are electronic is not without concerns. These include knowing whom you are dealing with (identification), who is authorized to access what information (entitlements), and how individuals will be held accountable for their online commitments (digital accountability).

Digital signatures powered by public-key infrastructure (PKI) technology, are widely recognized as best practice for ensuring digital accountability for electronic transactions. Digital signatures are the most effective, secure, and easy-to-implement method of providing accountability while enabling electronic transactions. This paper will help readers develop a better understanding of what digital signatures are, their role as an enabling tool in e-business, and how they can be used to advantage in light of recent legislative changes.

Digital signatures deliver e-business advantage

Aside from enabling new business processes, moving existing transaction systems online offers compelling advantages. These include dramatic gains in:

- efficiency
- lower costs
- stronger partner/customer relationships
- personalization
- tighter integration of supply chains

Rather than visiting a Web site, filling out an application form, then printing, signing, and sending a paper copy by courier or fax, the use of digital signatures allows the final step in an otherwise online process to be automated. The fundamental technology that enables security and accountability for electronic transactions is the digital signature.

In today's business environment, organizations must be aware of security and privacy issues, including regulatory issues such as national and international

legislation on privacy and digital signatures, as well as industry-specific regulations for selected broad verticals. Examples of such legislation in the United States alone include the Electronic Signatures in Global and National Commerce Act (e-Sign), the Uniform Electronic Transactions Act (UETA), the Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley (GLB) Financial Services Act and the Government Paperwork Elimination Act (GPEA). These types of regulations and legislation have created not only compliance challenges, but also opportunities for competitive advantage over slower-moving rivals.

The broad adoption of digital signatures built on PKI foundations is now generally acknowledged. The infrastructure build-out is currently underway, and the scale is enormous - for example, the U.S. Department of Defense has requested \$700 million in funding from fiscal year 2000 through 2005 solely for PKI development [*Information Security - Advances and Remaining Challenges to Adoption of Public Key Infrastructure Technology*, GAO, February 2001].

Digital signatures were first conceived of in 1976. Now 25 years later, wide-scale acceptance of PKI-based enhanced security solutions includes legislative support, with essentially all modern economies having existing or pending legislation giving digital signatures legal recognition. Leading organizations using digital signatures have raised global awareness of their vast potential.

Paper signatures

We are all familiar with paper signatures, by which we mean handwritten signatures on paper documents. Aside from legal and contractual issues, the primary characteristics of a paper signature are:

1. it is intended to be associated with a particular individual; and
2. it generally denotes a commitment related to a particular document, with the exact meaning depending on context.

Though far from perfect, paper signatures serve surprisingly well in many parts of the world as the basis for business and legal transactions. This is due not to the inherent features of paper signatures, but rather to accompanying processes, supplemental contracts, and the overall context surrounding acts of signing. Various customs of witnessing, public ceremony, and evidence have emerged over time, in large part aimed at increasing the chances of accurately reconstructing events should a dispute arise later.

Paper signatures in and of themselves are generally not meaningful. In fact, in many cases a witnessed "X" serves equally well. If extracted through coercion, trickery or forgery, almost all societies will find a paper signature legally non-binding. The use and interpretation of a paper signature are typically defined by culture and context. State laws evolve to define reasonable default terms, both in the absence of explicit contracts and in the presence of contracts with ambiguous terms. Common conditions necessary for a party to be legally bound by a signature include the signature mark representing a desire to be bound to a well-defined commitment, the mark being made of free will, and the mark being an act of the party to be bound (or a duly authorized deputy of that party).

A popular myth is that a paper signature can be easily traced to a particular individual. In practice, this turns out to be difficult. Most office workers are unable to recognize the paper signature of a colleague, or of the company officers that sign their expense checks. Nonetheless, this is not a problem because in most cases paper signatures are effectively a formality; their subsequent verification is rare. The reason paper signatures seem to work so well is that over time, societies learn to discontinue their use, or support them by additional means (e.g. witnesses, notaries, corporate letterhead, seals), in situations where it has been difficult to resolve disputes. The end result is that signatures are only rarely called into dispute, and there is confidence that the rare cases can be resolved through special procedures that rely on context, collective memory, and any

and all available evidence beyond a physical signature itself.

In summary, societies have learned to use paper signatures in circumstances in which a physical marking on a paper document, augmented by sufficient controls and context, provides sufficient recallable evidence of a commitment related to that document by the marking party. The evidence is important in order to reconstruct circumstances, in the rare case of later disputes.

Digital signatures

A *digital signature* is the term used for marking or signing an electronic document, by a process meant to be analogous to paper signatures, but which makes use of a technology known as public-key cryptography. The analogy to paper signatures is helpful, though not precise. Clearly paper signatures cannot be applied to documents that remain in electronic form. More significantly, additional security properties are required of signatures in the electronic world. This is because the probability of disputes rises dramatically for electronic transactions without face-to-face meetings, and in the presence of potentially undetectable modifications to electronic documents. Digital signatures address both of these concerns, and offer far more inherent security than paper signatures. Compared to all other forms of signatures, digital signatures are by far the most easily verified and the most reliable with respect to providing document integrity.

This is not to say that digital signatures cannot be misused. If poorly implemented or not supported by appropriate procedures and processes, they are no more reliable than paper signatures or corporate seals under similar conditions. (This is a point which critics of digital signatures appear to miss - the fact that paper signatures, without the procedures and processes generally accompanying them, do not provide any inherent security, and moreover have been subject to forgery since their first use.) It is, therefore, insightful to take a few minutes to

understand why digital signatures provide a far more secure basis for contracting and commitments than paper signatures, and offer the only viable solution to providing reliable evidence of commitments in an online world.

A given individual's paper signature is essentially identical regardless of the document being signed. For this reason, a threat related to paper signatures is a *cut-and-paste* attack from one physical document to another. This risk is usually small because typically such an act would leave physical evidence of the misdeed. However, the point worth noting is that such an attack is not possible for digital signatures, because the digital signature of George W. Bush differs significantly with each different document digitally signed by Mr. Bush, even if the document varies by only a single character or bit. Yet the digital signature can be easily associated back to the correct individual. This is possible through the elegance of public-key cryptography.

The important summary points are that, when properly implemented and supported by the robust foundation of a PKI:

1. digital signatures are to electronic documents what paper signatures are to paper documents;
2. digital signatures provide trustworthy evidence of the identity of the signing party (identification);
3. digital signatures are not subject to being copied to (or forged from) other documents;
4. digital signatures ensure that a signed document cannot later be modified to the advantage of one party (if the original is modified, the verification process detects this); and
5. digital signatures already have a legal footing equal with paper signatures in many countries.

In addition, the exact time of signing for a digital signature can be recorded more reliably than that for paper signatures, through the use of a trusted time-stamping server or service. With digital signatures, witnessing and notarization are naturally facilitated more efficiently and conveniently. Table 1 compares several important properties of paper signatures and digital signatures.

Creating and verifying digital signatures

To understand why a digital signature is more secure than alternate signature forms on electronic data, it is necessary to understand how a digital signature is created. A digital signature can be thought of as a numerical value, represented as a sequence of characters, and computed using a mathematical formula. The formula depends on two inputs: the sequence of characters representing the electronic data to be signed, and a secret number referred to as a signature *private key*, associated with the signing party and which only that party has access to. (A matching *public key*, which can be published for everyone to see like a phone number in a phone directory, allows signature verification.) The resulting computed value, representing the digital signature, is then attached to the electronic data just as a paper signature becomes part of a paper document. This results in two critical properties:

1. The digital signature can be uniquely associated with the exact document signed, because the first input is the precise sequence of characters representing that data.
2. The signature can be uniquely associated with the signing individual, because the second input is the private key that only that individual controls.

Property	Paper Signatures	Digital Signatures
Can be applied to electronic documents and transactions	No	Yes
Signature verification can be automated	No	Yes
Signature makes it possible to detect alterations to the detect	No	Yes
Can be used to signify a commitment to a contract or document	Yes	Yes
Can be augmented by use of a witness to the signature process	Yes	Yes
Recognized by legislation	Yes	Yes

Table 1. Comparison of paper and digital signature properties.

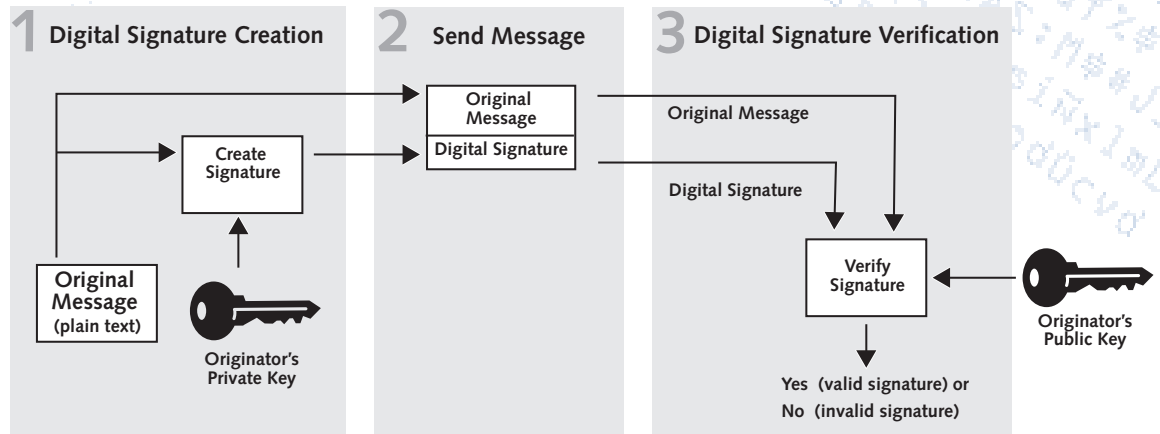


Figure 1. Digital Signature Creation and Verification

Verifying the authenticity of a digital signature can also be viewed as a process relying on a formula. Here the formula depends on three inputs: the sequence of characters representing the supposedly originally signed electronic data, the public key of the signing party, and the value representing the supposedly authentic digital signature. The formula produces as output a simple answer: yes or no. Yes signifies that the digital signature is indeed an authentic digital signature on the presented electronic data, and associated with the party linked to the public key used. This process is presented in Figure 1.

A public-key certificate generally provides the linkage between the signing party and the public key. In essentially all commercially relevant digital signature systems, the public-key certificate support is provided through a PKI. Entrust pioneered this architectural technology with the introduction of the world's first commercially available PKI product in 1994.

Digital signatures, digital accountability, and transaction evidence

The stock price of Emulex Corporation plunged over 60% in August 2000, following a fake press release. This could easily have been avoided by using digital signatures to confirm the source and integrity of the release. Instead, the fragility and insecurity of current information networks was highlighted.

Digital signatures are a fundamental part of an overall plan for digital accountability of electronic transactions. Such a plan requires appropriate security policies, practices and procedures as is customary in commercial IT environments. Important elements specifically relevant to the digital signature process include simple user interfaces, so that users understand the significance of their actions. For signatures not only to provide data integrity, but also to capture user intentions to make commitments, the digital signature process may include:

- a) capturing the entire context of the electronic transaction or document, and precisely what the signer is committing to;
- b) ensuring that the data displayed to the user accurately reflects the data to be digitally signed;
- c) requiring the user to signal an understanding of the commitment being made, and a desire to be bound to this;
- d) authenticating the user in order that the user's private key becomes available to the signing device;
- e) computing the signature based on the signer's private key and the data being signed;
- f) a timestamp server optionally appending a time-date field to the data and signer's signature and then signing; and
- g) forwarding the signed transaction for processing, storage, or subsequent verification.

A computer or handheld device generates the signature for the signing party, after that party indicates consent to the signing operation, and provides appropriate authentication to the device. The device typically stores the private key in secure storage. Digital signatures can be made very easy to use, and largely transparent to the sender and recipient. As with any good infrastructure, detailed system information should only become visible if a problem arises (e.g. if signature verification fails, it is because a document has been tampered with).

The term *non-repudiation* often arises in technical discussions about digital signatures. Unfortunately, because there is no universally accepted definition of this term, its use generally creates a great deal of confusion and misunderstanding. We prefer to define and use the concept of *digital verification*. The main question is whether the recorded evidence related to a transaction is sufficient to establish, at a later point, all-important details of the transaction. The evidence may be needed to resolve later disputes, including a party attempting to escape commitments or deny involvement. All parties must be held accountable for their commitments. Verification requires the generation and maintenance of appropriate evidence (e.g. transaction records serving as electronic receipts), provides a high degree of confidence that the evidence is accurate and that any subsequent manipulation or forgery can be detected.

Ultimately, whether the available evidence is sufficient depends on the situation and the authorities that must be convinced - a corporate manager, a business partner, an independent arbiter, or a court judge and jury. The use of products and services that provide high-trust digital signatures, together with a set of appropriately enforced security policies, provides best practice evidence. In most cases, this will be better than all available alternatives including paper signatures.

Digital verification ultimately does not depend on any single feature, such as the use of cryptographic hardware or the location where a private key is generated. Overall accountability depends on all aspects of a

system, including non-technology components such as security policies, procedural processes, and human-machine interfaces.

Digital signatures - best practice for electronic signatures

An *electronic signature* is any form of marking that might be used to represent the equivalent of a paper signature, for the case of an electronic document. As discussed earlier, digital signatures, based on public-key cryptography and supported by PKIs, are one type of electronic signature. Other types of electronic signatures have been proposed. One example is *digitized signatures* - scanned images of paper signatures that are then simply attached as graphical representations (bit-map images) at the bottom of electronic documents. Another possibility is *scripted-font signatures* - simply attaching the name of a signing party in a special scripted computer font, giving the likeness of a paper signature but including nothing characteristic of the signing party. Many other technologies, including *smart cards*, *biometrics*, and *passwords*, are confused as substitutes for digital signatures; the majority of these are in fact complementary to digital signatures, rather than substitutes.

It is clear that scripted-font signatures offer no security on their own (say in the absence of witnesses), as it would be very easy for anyone to enter the name George W. Bush at the bottom of a message, in a particular computer font. Digitized signatures similarly offer little security - one could obtain a signature image from a copy of an electronic or paper document, and an electronic representation could be easily copied and transferred to any other document. As discussed earlier, such *cut-and-paste* fraud is also possible with paper signatures, but in the paper world it leaves physical evidence and is therefore less of a risk.

Such attacks, which are possible with many weaker forms of electronic signatures, are not possible with digital signatures. A main reason is that, as discussed earlier, a digital signature varies with each transaction. If a single message word or bit is altered after a document is digitally signed, the signature

verification process will detect this. This is very important, because there is no point in verifying the identity of a signer if you cannot detect whether someone else has altered the document thereafter.

It is also important to note that simply obtaining the consent of a user - for example by having the user click on an "I accept" button - does not provide tangible evidence, at a later point in time, that such consent was actually obtained. An online brokerage would be hard-pressed to prove to an arbiter, at a later point in time, that the button was located in an appropriate place, in an appropriate overall context, six months after a disputed customer transaction took place. Indeed, recreating the environment of a past user transaction is extremely challenging, as the design of Web sites and online forms changes frequently. This highlights the difference between obtaining user consent, and recording evidence that such consent was obtained. While passwords are in common use for identification and entitling access to accounts, passwords alone are of little help in generating evidence generation such as easily verifiable *digital receipts*, that is, reliable electronic transaction records replacing paper receipts. Best practice for securing digital receipts is through digital signatures.

Digital signatures, when appropriately implemented in accordance with standard practice, provide more security than paper signatures or any form of electronic signature. They are the only known means for reliably binding a signature to electronic data in a manner that is both secure and easily verifiable - a property that is absolutely fundamental to e-business. They also offer the ideal means for guaranteeing the integrity of audit trails and online storage. As a result, digital signatures are equated with best practice for digital verification.

Contractual agreements vs. legislation-based business transaction systems

Although E-Sign and related legislation provide an important framework for digital signatures, some degree of uncertainty is inevitable regarding a court's interpretation of

any new legislation. It is therefore instructive to examine how the business community previously approached a similar situation, involving the emergence of electronic data interchange (EDI) systems in the 1980s.

EDI systems automated the purchase of goods through the electronic exchange of information such as purchase order requests, quotes, acknowledgements, and invoices. They were set up to allow automated processing of standardized messages. Trading partners reached common technical understandings as to how exchanged messages should be interpreted. Nonetheless, because there remained a legal requirement of a "signed writing", it was unclear how a court would interpret an EDI message exchange should a dispute arise. To reduce uncertainty regarding possible legal interpretations, EDI *trading partner agreements* were created. These were signed traditional contracts specifying rules for how exchanged messages should be interpreted, and the legal significance the parties intended these to have. The contracts would be available to a court should any disputes arise, for example with respect to fraud. The expectation was that a court would respect the desired interpretations as set out in the contract.

The volume of EDI transactions over the past 20 years has been huge. Interestingly, few or no reported cases of EDI trading partner disputes are known. While a single reason for this is difficult to establish, the use of contracts to remove uncertainty and clarify expectations appears to work very well. Consequently, the use of contractual agreements offers an attractive solution for any similar concerns in particular transaction systems intending to use digital signatures.

Open vs. self-governed systems, and the relevance of digital signature legislation

Business transaction systems can be divided into *open systems* and *self-governed systems*. In open systems, such as most cash-based retail sales, the rules of operation exist without special negotiation or membership. For example, in many countries rules governing the sale of goods include consumer

protection legislation. Open systems provide ground rules and a degree of comfort that is generally welcome in the case of strangers doing business with strangers.

Self-governed systems, in contrast, are based on some form of membership or semi-closed community. A relationship is formed based on voluntary agreements, often bilateral. Parties then transact business based on this relationship. The agreements may include allocation of risks between the parties, the definition of rights and obligations, and terms regarding how disputes should be resolved. By this means, any uncertainties as to how a court might interpret existing laws may be reduced, as in the case of EDI trading partner agreements.

Electronic signature legislation has the greatest impact on open systems. However, the majority of commercial electronic transaction systems can be realized as self-governed systems, including intra-business, business-to-business (B2B), and e-commerce transaction systems in general.

Enabling legislation and compliance issues related to digital signatures and privacy

Digital signatures enable business innovation by allowing paper processes to be moved online, while ensuring continued accountability. Legislation related to digital signatures such as the Electronic Signatures in Global and National Commerce Act (E-Sign) and the Uniform Electronic Transactions Act (UETA) are important as they remove uncertainties regarding legal interpretations of online transaction systems. Privacy legislation is closely related, as digital signatures play an important role in identification, entitlements, and verification - all of these being fundamental to online privacy. Important sector-specific examples of legislation include the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley (GLB) Financial Services Act.

Entrust provides leadership with digital signature solutions

Entrust has unique expertise and a long history of helping organizations integrate digital signatures into their business operation across a broad range of applications including e-mail, Web-based applications, electronic forms, and customer applications. Global 2000 organizations have been using Entrust technology to power digital signatures since 1994.

Proven expertise and enhanced security solutions from Entrust, combined with partner solutions, can help you meet the best-practice security and privacy expectations of your employees, customers, partners, and suppliers. We can also help you interpret the national and international regulatory compliance requirements of existing and emerging privacy and digital signature legislation.

For more information on digital signatures, visit the Entrust Resource Center at <http://www.entrust.com/digitalsig/index.htm>

Entrust®, Inc. (Nasdaq: ENTU) is a leading global provider of enhanced Internet security solutions and services that make it safe to do business and complete transactions over the Internet. Entrust has the industry's broadest set of identification, entitlements, verification, privacy and security management capabilities. More than 1,200 major corporations, service providers, financial institutions and government agencies in more than 40 countries rely on the privacy, security and trust provided through Entrust's portfolio of award-winning technologies. For more information, visit www.entrust.com.