

Digital Signature Technology, Part 1

The most established system of electronic signatures involves *digital signature* technology. This technology relies upon public/private key encryption, a technique that has been with us for approximately 20 years. In this system, each user generates two related but not identical encrypted keys, which are like giant passwords.

The private key remains secret to the person who generates the key pair. It must never be disclosed or security is compromised. The public key can be freely distributed to any person with whom the owner of the key pair wishes to communicate. It can even be published without fear of compromising security in the *New York Times*. The attributes of the private key cannot be determined from the public key, even though the two are related.

If you are using Netscape Navigator 3.0 or higher, then your browser has the built-in ability to generate a private/public key pair. Later in this presentation there will be an opportunity to generate such a key pair directly from the Netscape browser.



Digital Signature Technology, Part 2: Encrypting Communications

The private key and the public key perform reverse actions. If Alice wishes to communicate in secret without fear of eavesdropping over the internet, she can encrypt (code) the communication. Bob decrypts the communication using the related key. In the example below, Alice tells Bob to bid three billion units for her. Bob has given Alice his public key. He retains the private key. Alice encrypts the message using Bob's public key, making the message unintelligible to outsiders. Bob decrypts the message using his private key.

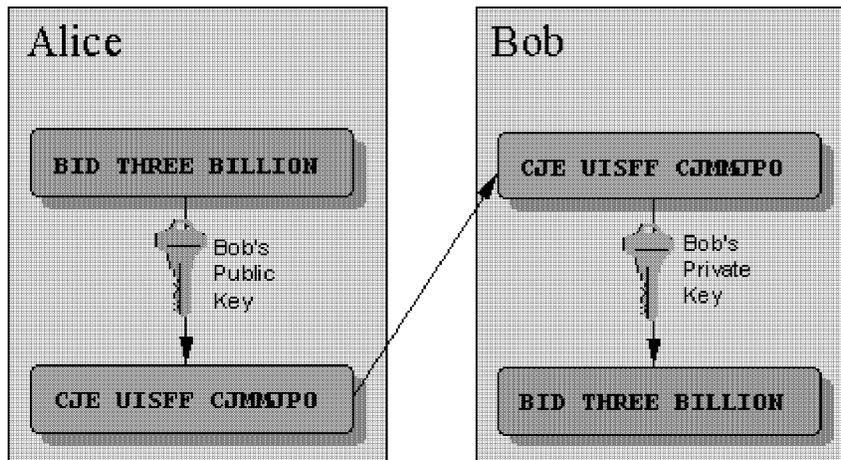


Illustration courtesy of Terisa Systems



Digital Signature Technology, Part 3: Signing

In addition to, or in place of encrypting the message, the sender can sign it. Signing in this case does not involve a handwritten signature, but instead consists of applying the private key of the sender to the contents of the message in a particular way. In our previous example, even though Bob received a coded message from Alice to bid three billion, he has no way of knowing if Alice was really the sender. Someone else could have obtained a copy of his public key, which he may have distributed to many people, and used it to code the message under Alice's name. If he bids the three billion, and a trick was played on him, there could be serious consequences to Bob. He should require Alice to sign the message before acting on it.

Signing involves two distinct processes. First, the message is indexed to a digest, or "hash." The message digest is a reduced form (in terms of information) of the message. The digesting is necessary on the one hand because the signed message itself usually is too large, absent digesting, for efficient transmission over the internet. Digesting also provides a handy way to verify messages. Creating the message digest is an essential step in the signature process.

Before sending, the signer also processes the message hash by encrypting it using the sender's private key. In the example below, Alice signs her message digest to Bob using her private key. Please also note that Alice could have but did not also encrypt the message contents.

After transmission, Bob has not only the unencrypted message, but also the attached and encrypted message hash, and the algorithm used to create the hash, which was exchanged between the computers as a "session key." These latter tools permit Bob to verify not only that the signer was the sender, but that the message has not been changed since it was signed. Bob recreates the message hash using two independent methods. First, he repeats the process of generating the message hash from the message itself, which Alice did initially, by applying the session key which he obtained from Alice along with the message. Secondly, and independently, he decrypts the encrypted message hash which was appended to the message using Alice's public key, which was given to him by Alice prior to transmission. If the two resulting message hashes are the same, then Bob is assured that the signature is genuine and the message is authentic. If the message hashes are not the same, then the message is a forgery or was tampered with after signature. In either case, Bob should not rely on the message as authentic.

These relationships are represented graphically below.

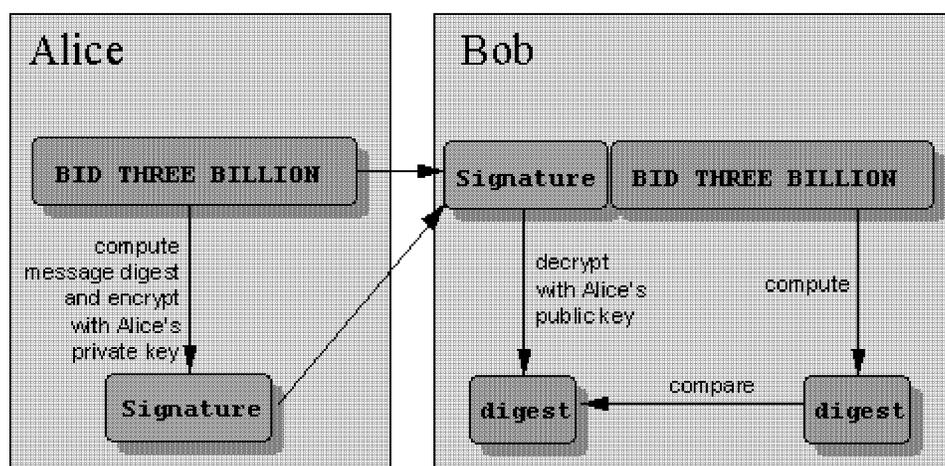


Illustration courtesy of Terisa Systems



Digital Signature Technology, Part 4: Digital Certificates

Bob still has a potential problem with the message. He obtained Alice's public key from Alice. But how can he be sure that it was really Alice who gave him her public key in the first place? Unless he knows Alice personally and has some confirmation of her identity independently of the internet, it is theoretically possible that someone pretending to be Alice sent the public key to him in Alice's name, intending to deceive him all along.

To guard against this possibility, trusted authorities provide digital certificates to persons, identifying them as belonging to the public keys which they distribute to others. An example of such a certificate, which is downloaded into an encrypted database located in the user's browser, is shown below. These certificates are graphical representations of the fact that the user's public key has been countersigned with the public key of the certificate authority.

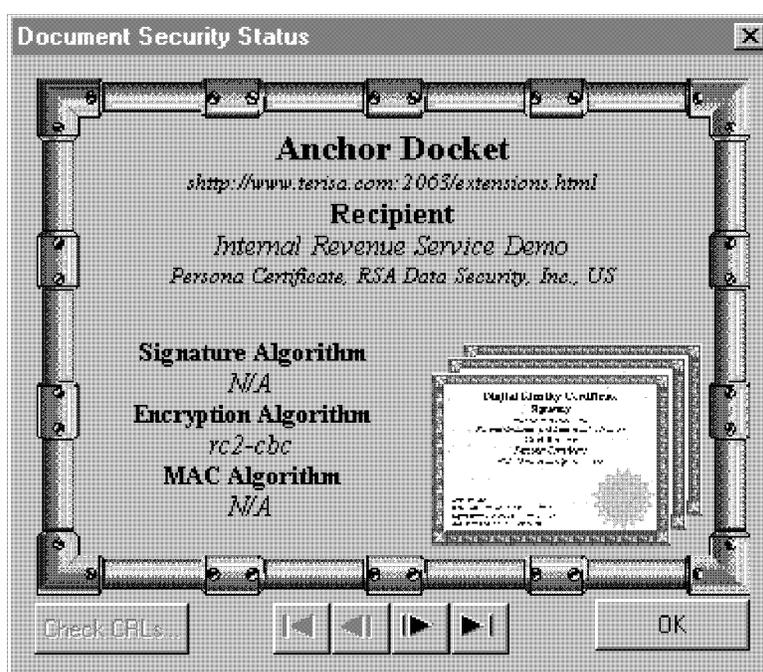


Illustration courtesy of Terisa Systems

In the illustration which follows, Alice's public key has been certified by CA1, which is ordinarily a company that provides this service to the public for free or for a small fee. CA1's identity in turn is verified by another company, which provided a similar service to CA1. The second company is a "trusted root."

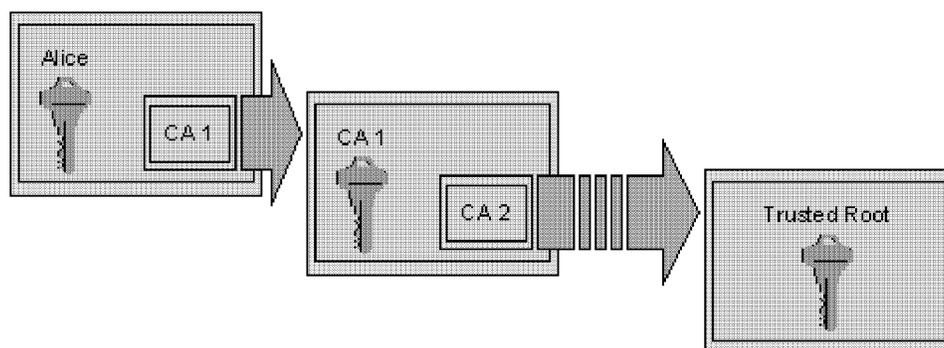


Illustration courtesy of Terisa Systems

If CA1 has taken pains to identify Alice as being Alice, and provides a digital certificate to her, and in turn

CA1 is identified by a trusted root, then Bob can be reasonably sure based on the hierarchy of certificates that Alice is who she purports to be.

Or can he?



Digital Signature Technology, Part 5: Reliability

Digital signature technology is about to gain general acceptance through Secured Electronic Transactions ("SET"), a service/product launched in the first quarter of 1997 jointly by Visa and Mastercard to promote secure commerce over the internet by encrypting credit and debit card numbers and thus securing them from snooping third parties and merchants alike (merchant credit card fraud constitutes over 90% of all credit card abuse in the United States).

Notwithstanding this push for acceptance of digital signature technology by the US technology industry for commercial transactions, close examination of its tenets raises questions about its suitability for legal filings over the internet.

One of the weaknesses of the digital signature technology is the notion that digital certificates properly assure identification of parties over the internet.

First, when all is said and done, digital certificates do not identify people. They identify internet addresses. A digital certificate identifies `www.somecompany.com` or `joeblow@somewhere.com`, not real people. A machine, not a human, bears the digital identity. When a different person than the owner uses the machine, few can be the wiser.

Secondly, with respect to individual consumers, not necessarily web servers, the degree of effort put into verifying identities is extremely disappointing. VeriSign, considered to be a leading "trusted root", offers two classes of consumer certificates. The class 1 certificate requires no identity check whatever and may be considered to be a trial or educational certificate for the principal purpose of acquainting persons with the digital identification process. The class 2 certificate, which is supposed to be more secure, is scarcely suitable for legal purposes since beyond a cursory credit check, no further attempt is made to verify identities, although much is made by the company of the number of people involved in actually issuing the certificate once the credit company report is received, scarcely an improvement on the quality of the information used to make the decision whether to issue the identity certificate or not. [View VeriSign class 2 certificate policy.](#)

Third, the digital certificate is downloaded by the user into a database located in the browser on the user's computer. While the database is encrypted and thus presumptively secure, access to the database is by unencrypted password established by the user. The user's digital identity is thus accessible to outsiders if the unencrypted password can be discovered, regardless of the other controls. If the digital certificate is obtained by a third party, that party can masquerade as the true owner for all practical purposes over the internet.



Digital Signature Technology, Part 6: Legal Aspects

Assuming the suitability of digital signature technology for legal filings and other legal purposes, one question arises whether communications involving legal documents over internet should only be digitally signed, or both digitally signed and encrypted.

With respect to public filings of matters intended to become a public record, only digital signing should be required. Encryption of the contents of the document itself is neither necessary nor desirable. Since the filed document will be available to all requestors once it becomes a public record, absent unusual circumstances, there is no need for privacy through encoding during the transmission to the document repository. If the document is not encoded, there will be no need to decode the document upon arrival at the public facility. This represents a savings in terms of processor performance at the public facility's computer.

For private matters not intended to be made public, such as contract negotiation and conclusion, both signature and encryption should be considered. Terisa Systems, a software manufacturer, distributes a free Netscape plug-in which is designed to permit both encryption and digital signing, or either of them separately, of information destined for secure web servers. At the time of writing, it is the only such software which is generally available for this purpose. In the realm of personal communications, the computer program Pretty Good Privacy, which relies on digital signatures, encryption, and a voluntary web of trust for e-mail between individual users without also invoking a formal certificate authority hierarchy, is available as freeware for non-commercial purposes. It can be adapted to communications for legal purposes, and one company distributes a commercial version of the product for such purposes.

Assuming the adoption of a digital signature system with one or more certificate authorities for electronic legal filings, proper administration of certificates by the certificate authorities will be critical. As with any public record system involving elements which are subject to revocation and expiration, accurate, up-to-date information will become essential. For example, a corporation may terminate or lose employees who have digital certificates issued in its name. After termination, the corporation should promptly notify the certificate authority that the certificate in that employee's name is no longer valid. If the ex-employee attempts improperly to use the certificate after termination to create obligations for the former employer, the use should be thwarted by up-to-date and accessible information from the certificate authority.

Qualification and regulation of the certificate authority therefore becomes of prime importance to the workability of a digital signature scheme. The United States Postal Service is presently proposing to become the national Certificate Authority of last resort for all transactions taking place in the United States. Under the proposal, users will obtain annual digital certificates in person at local post offices throughout the country. Each applicant will be required to show a photo id. Presentation of false identification or information will render the offender subject to criminal prosecution under existing federal laws prohibiting making false claims or providing false information to agencies of the U.S. government. Opponents argue that allowing the government to perform this service invites a "big brother" relationship with respect to very private information. If the government has access to private key information, the notion goes, it can use that information to gain access to encrypted communications.

Many states are in the process of establishing or adopting digital signature laws. Utah is a pioneer in this effort, as is Washington. However, the Utah legislation may be subject to the criticism that the metaphor between a digital signature and handwritten signature is imperfect, and that unlike handwritten signatures, which remain constant regardless of the document to which they are annexed, digital signatures change with each message because of the consistent use of the message digest or hash, which varies with the content and length of each message. A closer analogy to a digital signature than a handwritten signature or a seal may be a cigarette butt,

which is casually tossed over the railing of a boat into the wake. Once consumed, it is of no further use. The key pair persists, not the digital signatures they create. The Utah legislation arguably may confuse certain technical distinctions in the process of inappropriately applying this metaphor of a handwritten signature. [View examples](#). A list of pending and adopted state legislation to enable legal uses of digital signatures at the state and local level is readily available on the internet. [View now](#).

