PUBLIC KEY INFRASTRUCTURE (PKI) 101

Overview

All legally binding communications or transactions, whether electronic or paper-based, must meet these fundamental requirements:

- The message provide for sender authenticity to enable the recipient (or relying party) to determine who really sent the message and if that individual is, in fact, authorized to commit his organization to the transaction.
- There be some means to ascertain that the message has integrity. The recipient must be able to determine whether or not the message received has been altered en route or is incomplete.
- The most critical requirement addresses the ability to "prove up" the message in court. Referred to as non-repudiation, this requires some way to ensure that the sender cannot falsely deny sending the message, nor falsely deny the contents of the message.
- Certain signature formalities must be satisfied. For example, the statute of fraud specifies "in writing" and signature requirements for transactions over a certain dollar value or time period.

Satisfying the Requirements in Electronic Commerce

In electronic commerce, the focus to date has been on securing the medium through the use of private leased lines and networks. This is prohibitively expensive and, in some cases, unfeasible for potential parties to a transaction. For the Internet to offer an inexpensive and ubiquitous solution, the focus must be on information security. The goal here is to protect the message, not the medium. The Internet is insecure - potentially millions of people have access and "hackers" can intercept anything traveling over the wire. There is no way to make it a secure environment; it is, after all, a public network, hence its availability and affordability. In order for it to serve our purposes as a vehicle for legally binding transactions, efforts must be directed at securing the message itself, as opposed to the transport mechanism. Public key cryptography, a data encryption technique, provides just that kind of message protection. Originally recognized within the context of electronic funds transfer and UCC Article 4A, digital signatures - which are based on public key cryptography - have been thrust into the legal limelight as the solution to the problem of guaranteeing secure electronic commerce. The Utah Digital Signature Act was the first legislative initiative to address secure electronic commerce, with efforts by other states and the federal government trailing close behind.

Digital Signatures and Information Security

In defining digital signatures and how they work, it is helpful to begin by clarifying what they are not. A digital signature is not a digitized image of a handwritten signature. We are all familiar with the electronic pad a person signs upon receiving a package from a delivery service such as Federal Express. In these cases, the handwritten signature is digitized and the image transferred to the electronic document. Once captured, these digitized signatures can be cut and pasted on to any electronic document, making forgery a simple matter. Digital signatures on the other hand are an actual transformation of an electronic message using public key cryptography. Through this process, the digital signature is tied to the document being signed, as well as to the signer, and therefore cannot be reproduced. Furthermore, with the passage of the federal digital signature bill, digitally signed electronic transactions have the same legal weight as transactions signed in ink. Now, a legally binding contract may be formed over the Internet by two parties who have never met, without requiring notarization. This will radically alter the way business is conducted and accelerate the already rapid adoption of so-called electronic commerce.

The Basic Principles

The principles underlying the use of cryptography in electronic communications are as follows:

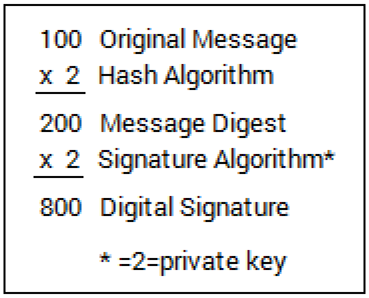
1. All data entered into a computer is read as a binary number. For example, when "Jack and Jill went up the hill" is typed in, the computer reads it as "1000111010100111000101," etc.
2. Because electronic messages are represented numerically in the computer, it is possible to perform mathematical functions on them.
3. Electronic messages can thus be transformed into alternate representations that are unique to the original.

Public Key Cryptography

There are two distinct encryption techniques. Symmetric cryptography is the most familiar. It is based on a shared secret, or key, and works well within isolated environments. An example of symmetric cryptography is the automated teller machine (ATM) at a bank. When you use an ATM, you gain access to your account by entering a personal identification number (PIN). You are, in effect, authenticating yourself to the bank. You and the bank share a secret, in this case your PIN, and, as such, can communicate securely upon revealing knowledge of this secret. The inherent problem with symmetric cryptography is one of scalability. In order for the communications to be confidential, the exchange of the key, or shared secret, must be done securely. Obviously, this type of secure distribution is not feasible when the number of different people with whom you want to communicate securely escalates beyond a manageable number. The other encryption technique is asymmetric cryptography - also known as public key cryptography - because it involves an asymmetric key pair. This key pair is comprised of what is referred to as a public key and a private key. The public key, as its name suggests, may be freely disseminated. This key does not need to be kept confidential. The private key, on the other hand, must be kept secret. The owner of the key pair must guard his private key closely, as sender authenticity and non-repudiation are based on the signer having sole access to his private key. There are several important characteristics of these key pairs. First, while they are mathematically related to each other, it is impossible to calculate one key from the other. Therefore, the private key cannot be compromised through knowledge of the associated public key. Second, each key in the key pair performs the inverse function of the other. What one key does, only the other can undo.

Digital Signature Components

Digital signatures are based on asymmetric, or public key, cryptography. In addition to a key pair and some type of electronic communications, the digital signing and verification processes involve something known as a hash algorithm and a signature algorithm. The hash and signature algorithms are extremely complex mathematical equations. The hash algorithm is performed on the original electronic message's binary code, resulting in what is referred to as a message digest, which is a 160-bit string of digits that is unique to the original message. The signature algorithm is then performed on this message digest. The resultant string of digits is the digital signature. The signer's private key is incorporated into the signature algorithm during the signing process, and the public key is incorporated into the signature algorithm during the verification process. An extremely rudimentary mathematical example of this would be as follows:



100 Original Message
x 2 Hash Algorithm

200 Message Digest
x 2 Signature Algorithm*

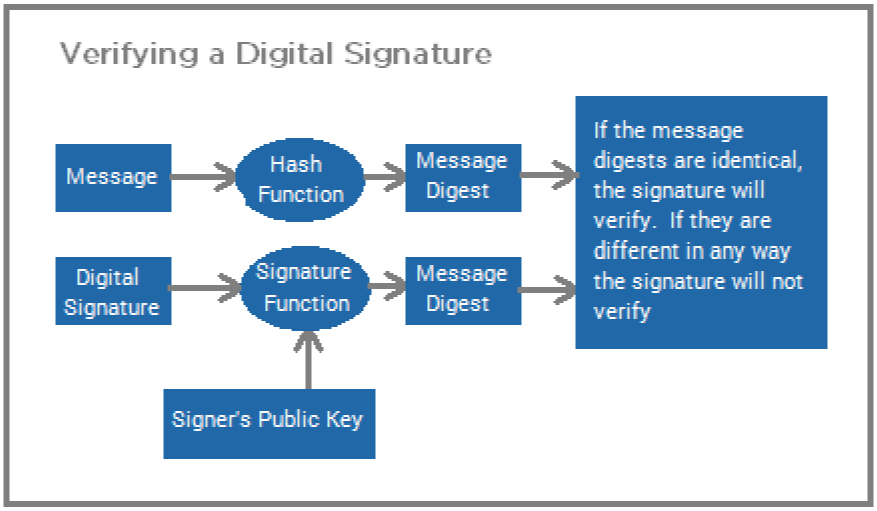
800 Digital Signature

* =2=private key

For the sake of simplicity, assume that the binary number 100 represents the original message. Again for simplicity, assume the hash algorithm is simply to multiply the binary by two. The result of passing the binary of the original message through the hash algorithm is the message digest, or the unique fingerprint of the message, which is 200 in this example. This message digest is then passed through the signature algorithm, of which the signer's private key is a component. In this example, the signature algorithm has been drastically simplified to multiplying by two to the *, where * equals the signer's private key, in this case 2. The resulting number of 800 is the digital signature. In contrast to a digitized signature, a digital signature has nothing to do with the signer's name or handwritten signature. It is an actual transformation of the message itself that incorporates a "secret" known only to the signer, and is therefore tied to both the signer and the message being signed. A signer's digital signature will be different for each different document he signs.

Digital Signature Processes

The following are graphical representations of the digital signing and verification processes, respectively:



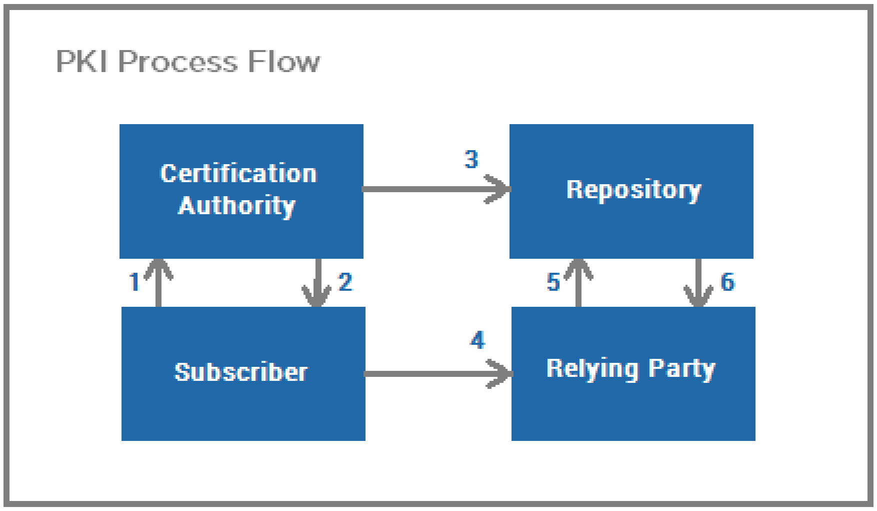
Verifying a Digital Signature

Message
Hash Function
Message Digest
Digital Signature
Signature Function
Message Digest
Signer's Public Key
If the message digests are identical, the signature will verify. If they are different in any way the signature will not verify

Public Key Infrastructure

It is now possible for an individual to purchase digital signature software, or download it from a browser, and install it on his computer. He can then generate a key pair and release his public key to the on-line world, using any identity he chooses; however, in this scenario there is still no guarantee that the identity is authentic. This situation underscores the need for some type of entity to serve as a trusted third party (TTP) to vouch for individuals' identities, and their relationship to their public keys. This entity, in public key infrastructure (PKI) terminology, is referred to as a certification authority (CA). The CA is a trusted third party that issues digital certificates to its subscribers, binding their identities to the key pairs they use to digitally sign electronic communications. Digital certificates contain the name of the subscriber, the subscriber's public key, the digital signature of the issuing CA, the issuing CA's public key, and other pertinent information about the subscriber and his organization, such as his authority to conduct certain transactions, etc. These certificates have a default life cycle of 1 year, and can be revoked upon private key compromise, separation from an organization, etc. These certificates are stored in an on-line, publicly accessible repository. The repository also maintains an up-to-date listing of all the certificates, that have not yet expired, which have been revoked, referred to as a certificate revocation list (CRL). The repository also maintains an electronic copy of the certification practice statement (CPS) of each CA that publishes certificates to it. The CPS outlines the policies and procedures of each CA's operations from registration of a subscriber to the physical security surrounding their CA system.

The following is a graphical representation of the PKI process flow.



PKI Process Flow

1. Subscriber applies to Certification Authority for Digital Certificate.
2. CA verifies identity of Subscriber and issues Digital Certificate.
3. CA publishes Certificate to Repository.
4. Subscriber digitally signs electronic message with Private Key to ensure Sender Authenticity, Message Integrity and Non-Repudiation and sends to Relying Party.
5. Relying Party receives message, verifies Digital Signature with Subscriber's Public Key, and goes to Repository to check status and validity of Subscriber's Certificate.
6. Repository returns results of status check on Subscriber's Certificate to Relying Party.

Digital Signature Applications

Digital signatures, created using identity-based digital certificates, are critical to the electronic conversion of any presently paper-based process that requires strong authentication of both the sender and the contents of the message, and/or non-repudiation. The number of such applications is virtually endless, ranging from purchase order systems, time cards and automated forms processing to contracts and remote financial transactions or inquiries.

Obligations and Legalities

The effective use of digital signatures imposes certain obligations on the parties involved. The signers of electronic messages must protect their private key from compromise. This is the fundamental building block of the PKI. If a signer's private key is compromised, he must report it immediately so the CA can revoke his certificate and place it on a CRL. Certification authorities are obligated to use due diligence to verify the identity of their subscribers and their relationship to their public keys. The CA must also promptly suspend or revoke a certificate at a subscriber's request. Finally, the reliant parties must actually verify the digital signature and check its validity against the current CRL maintained by an on-line repository.