# Digital Signatures

Date: May 29, 2003
Section: Articles :: Authentication, Access Control & Encryption
Author: Ricky M. Magalhaes
Printable Version

In this article I will clarify what a digital signature is and will demonstrate ways of using this technology to validate the identity of a user. The internet is filled with fraudulent villains that can take you or your organization to the cleaners, without you even knowing about it till it's too late.

In this article I will clarify what a digital signature is and will demonstrate ways of using this technology to validate the identity of a user. The internet is filled with fraudulent villains that can take you or your organization to the cleaners, without you even knowing about it till it's too late. Vendors like Verisign and through sell signatures that help you in the validations process giving the transacting party piece of mind. Knowing that the identity of the 3rd party is verified makes it easier to prosecute if there were to be an issue in the remaining part of the transaction and honoring of the guarantees. Spam is an area that can be rectified by making digital signatures mandatory and using a net police to prosecute where the illegitimate mail originated from. Although in some countries it is law to have digital signature to conduct contractual business it is increasingly becoming the way secure business is conducted.

## What are Digital ID's?

Digital ID signature or certificate is an installed file resident on a computer validates who you are. Digital signatures are used by programs on the internet and local to the machines to confirm your identity to any third party concerned. Digital signatures have been confused with electronic signatures. Electronic signatures are scanned copies of a physical written signature.

## When do you need to verify identity?

New ways of verification are being developed daily. Biometrics and other methods keep getting formulated and incorporated into the information technology industry. One interesting biometric authentication mechanism developed by a leading Japanese biometric company has found a way to get your DNA into a pen. You sign a document and it is digitally scanned. This document then can be scanned in the future to verify its authenticity. Identity should be verified when ever there is doubt of the 3rd party being whom they say they are or when there is personal information at risk. Personal information like credit card details and banking information should be kept safe using digital certification as one of the security layers. Some banking institutions require that a user verifies his/her identity by validating identification credentials using a digital certificate. Important e-mail can also use Digital signatures that verify that the e-mail is from the originating sender and that it has not been tampered with. On many occasions users are unsure if they are dealing with reputable suppliers of institutions. Digital certification gives the user a sense of legitimacy and formalizes the process. It ensure that the company that the user is dealing with has a registration with a trusted authority and that the transaction is guaranteed to be done with the intended parties.

## Reasons for using digital security.

- It insures by means of verification and validation that the user is whom he/she claims to be. This is done by combine the users credential to the digital certificate and in turn this method uses one point of authentication.
- Digital certificates insure data Integrity giving the user piece of mind that the message or transaction has not been accidentally or maliciously altered. This is done cryptographically.
- Digital certificates ensure confidentiality and ensure that messages can only be read by authorized intended recipients.
- Digital certificates also verify date and time so that senders or recipients can not dispute if the message was actually sent or received.

## The components that a digital signature comprise of.

1. **Your public key:** This is the part that any one can get a copy of and is part of the verification system.
2. **Your name and e-mail address:** This is necessary for contact information purposes and to enable the viewer to identify the details.
3. **Expiration date of the public key:** This part of the signature is used to set a shelf life and to ensure that in the event of prolonged abuse of a signature eventually the signature is reset.
4. **Name of the company:** This section identifies the company that the signature belongs too.
5. **Serial number of the Digital ID:** This part is a unique number that is bundled to the signature for tracking ad extra identification reasons.
6. **Digital signature of the CA (certification Authority):** This is a signature that is issued by the

authority that issues the certificates.

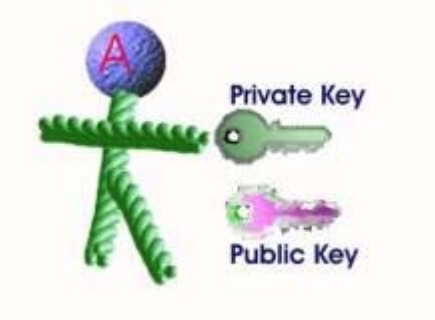


*Figure A*

User A is depicted above and has two keys a public key, this key is available to the public for download, and a private key, this key is not available to the public. All keys are used to lock the information in an encrypted mode. The same keys are required to decrypt the data.

Another user can encrypt the data using users A's Public Key. User A will use the Private Key to decrypt the message. Without user A's Private Key the data can not be decrypted. Figure B below depicts the encryption method and decryption method and witch keys are used.

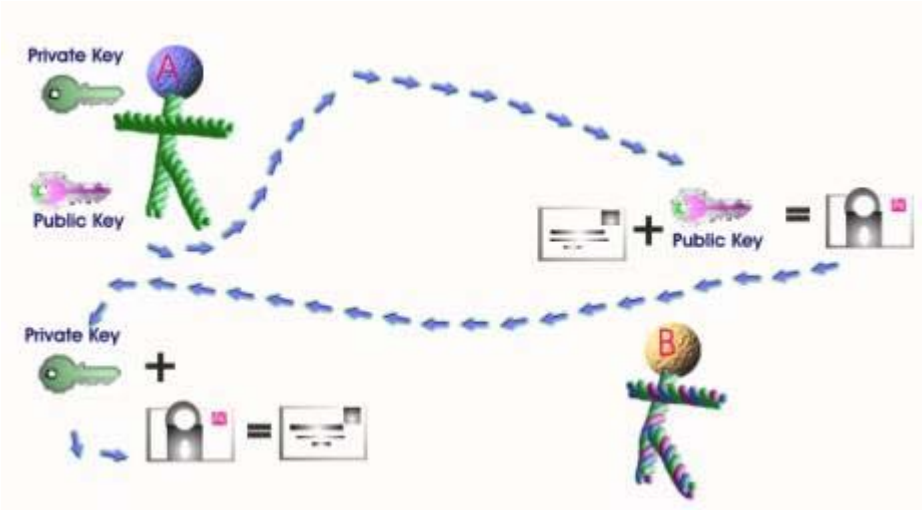


*Figure B*

Digital signature can be used to make document e-mails and other data private. Big brother is out there and choosing a high encryption mechanism ensures that any one attempting to decrypt the data would find it unviable to attempt decryption.

User A's machine digests the data into a simple string of code after user A's software has encrypted the message digest with his private key. The result is the digital signature. User A's software then appends the digital signature to document. All of the data that was hashed has been signed. User A then passes the digitally signed document to user B.

First user B's software decrypts the signature, using User A's public key then changing it back into a message digest. After the decryption if it has decrypted the data to digest level then verifies that user A in fact did sign the data. To stop fraud certificate authorities have been introduced. Certificate authorities can sign User A's public key, ensuring that no one else uses Bobs information or impersonated his key.

If a user is uncertain of the digital signature it is possible to verify the digital signature with the certificate authority. Signatures can also be revoked if they are abused or if it is suspected that they are abused. When a digital signature is compromised the user that suspects that the certificate is compromised should report the incident to the certificate authority.

## The process of checking the validity of digital signature.

- User A sends a signed document to User B.
- To verify the signature on the document, user B's application first uses the certificate authority's public key to check the signature on user A's certificate.
- Successful de-encryption of the certificate proves that the certificate authority created it.
- After the certificate is de-encrypted, user B's software can check if user A is in good standing with the certificate authority and that all of the certificate information concerning user A's identity has not been altered.
- User B's software then takes user A's public key from the certificate and uses it to check user A's signature. If user A's public key de-encrypts the signature successfully, then user B is assured that the signature was created using user A's private key, for the certificate authority has certified the matching public key.
- If the signature is found to be valid, then we know that an intruder didn't try to change the signed content.

## The importance of private key revocation

At times there may be grounds for believing that a private key may have been compromised. This will then result in the key pair being revoked. When a digital signature is revoked the user that is requesting the revoke needs to be verified. If a key is wrongfully revoked legal action can follow.

Digital signatures deliver assurances in the role that the other party will keep their part of the bargain. Knowing the identity of the other party is one way of gaining that assurance. Keys used for digital signatures are very long series of bits, which can be represented as long series of alphanumeric characters. This makes digital signatures unfeasible for an individual to remember. They must consequently be stored in a method which is suitable, portable and protected. The most likely current technology to support such storage is a chip. Smart cards, bios chips, e-prom ships found in cable modems and other types of descrambles are all examples or primitive forms of digital signatures that act as away of identifying user. No form of identification to this date is used more than digital signature to verify the existence of a user and confirmation of credential over the internet. Digital signatures in some form or other are her to stay.

## Summary

Verification of user credential is big business on the internet. Knowing that a user is how he claims to be 1000 miles away seems to be the way the world or global commerce is functioning today. Knowing that this technology exists and leaning is fundamentals helps when dabbling in the digital signature arenas. I trust this article has given you an overview of the technology and how it functions.

*If you would like us to email you when Ricky Magalhaes releases another article on WindowSecurity.com, subscribe to our 'Real-Time Article Update' by clicking here. Please note that we do NOT sell or rent the email addresses belonging to our subscribers; we respect your privacy!*