Digital Signatures are the only designated system of legally recognized authentication of electronic documents in India. As per ITA 2008, Digital Signature is the PKI based system which uses Asymmetric Cryptosystem and Hashing where the digital certificate is issued by a licensed certifying authority.

Digital Signatures Made Easy

Naavi

Digital Signatures

Naavi

Na.Vijayashankar
No 37," Ujvala"
20th Main, B S K Stage I,
Bangalore- 560050
Director: Cyber Law College
Director: Ujvala Consultants Pvt Ltd

Web: www.naavi.org

E-Mail: naavi@vsnl.com: Mobile: +9343554943

The System of Signatures in the Digital World

Signatures are an essential part of the "Literate World". In the physical space, any person who cannot sign is often and prefers to affix his "Thumb Impression" is popularly treated as an "Illiterate". If we extend the same logic to the digital world, we have only around 12 lakh persons in India who is "Digitally Literate" and who can "Sign" an "Electronic Document. The rest of the population including those who are "Computer Literate" are not literate enough to affix their signatures on an electronic document.

It is strange that many of us who do Banking on the Internet or Manage responsible e-Governance positions or Exchange electronic documents of great financial implications do not consider it necessary to insist that the documents are signed by the originator of the document so that it can bind him/her to the statements made there in and he/she can be taken to the Court in case of any dispute.

It is time we think if it is safe to do commercial transactions on the digital space without appropriate signatures while we give so much of importance to signatures in the paper.

But part of the problem is because we donot know "What is Signing of an Electronic Document?", "How an electronic document can be signed ?" , "Why signing is necessary?" and " What are the risks of not signing an electronic document?".

Answers to all these questions have been provided through the legislation called Information Technology Act 2000 (ITA 2000). ITA 2000 has recently been amended substantially through the Information Technology Amendment Act

2008 which has been passed by the Parliament on December 23 and 24th and assented to by the President on 5th February 2009. Presently the rules under the Act are being framed and once the rules are ready, the date of effect of the new provisions will be notified.

A summary of what ITA 2008 says about "Signatures of Electronic Documents" is provided below.

Signature and Authentication

ITA 2008 speaks of two terms namely "Digital Signatures" and "Electronic Signatures". Both are forms of "Authentication of an electronic document".

Out of these two, the term "Electronic Signature" was added in ITA 2008 and as of now there is no specific format notified which constitutes Electronic Signatures. Hence it is only an "Enabling Feature" and we need to wait for a form of “Electronic Signature” to emerge in future.

On the other hand, “Digital Signature” was introduced in ITA 2000 and has been in our statute since 17th October 2000 though the first use of a Digital Signature became possible only on 5th February 2002 when the first Certifying Authority in India namely Safescrypt was licensed. Digital Signature continues to be the legally accepted form of authentication of an electronic document even after ITA 2008 becomes effective .

“Digital Signature” is defined under Sec 2(p) of ITA 2000/8 as

> "Digital Signature" means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3;

Section 3 states:

Authentication of Electronic Records

(1) Subject to the provisions of this section any subscriber may authenticate an electronic record by affixing his Digital Signature

(2) The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record

> *Explanation: For the purposes of this sub-section, "Hash function" means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as "Hash Result" such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input*

making it computationally infeasible

(a) to derive or reconstruct the original electronic record from the hash result produced by the algorithm;
(b) that two electronic records can produce the same hash result using the algorithm.

(3) Any person by the use of a public key of the subscriber can verify the electronic record.
(4) The private key and the public key are unique to the subscriber and constitute a functioning key pair.

The purpose of “Authentication” of an electronic document is two fold.

1. The first objective of authentication is to link a person as signatory to an electronic document.

2. The second objective of authentication is to confirm that the signatory is giving his confirmation of some data which is present in the electronic document.

We say that an electronic document is “Authenticated” or “Signed” by Mr X when it can be verified that Mr X stands in agreement to abide by what is contained in the document.

In the physical world, this consent is provided by a person in the form of affixing his signature at the bottom of a paper document containing the said information which he is authenticating. In the event any changes are made in the document after the signature is affixed, the person confirms his assent to the authentication by a further signature near the place where a change is made to signify that the change has his consent. When a person cannot sign, he may use a

“Thumb Impression” as a mark of his ”signature”.

While the “Signature” or “Thumb Impression” provides the “Identity” of the person who has signed a document, the multiple signatures or thumb impressions where there are alterations or lack of any alteration testifies to the fact that the signatory consents to what has been written in the document. Any unauthenticated alteration will make the entire document in valid.

In the electronic world too we need the “Signature” to perform the twin objectives of authentication namely “identification” of the person authenticating and “confirming that no change has been made to the document after it was signed”. To achieve these objectives the law has identified the two technologies namely the “Asymmetric Crypto System” and “hash Function”

Hash and Asymmetric Crypto system are both based on mathematical operations that can be performed on a numerical value. These systems can also be used with “Electronic Documents” since every “Electronic Document” is a “Binary Expression” which can be treated as a “number”.

The rules framed under ITA 2000 defined two standard algorithms called MD5 and SHA1 to be used for Hashing and the standard RSA algorithm for asymmetric cryptosystem.

Additionally, ITA 2000 has made it mandatory that only a person who obtains a “Digital Certificate” from a licensed Certifying Authority” in India can affix digital signatures as recognized by law. Such a digital signature will legally be equivalent to “Signing” as is understood in the use of paper documents in any law.

What is Hashing

When an electronic document is passed through the hash algorithm, it produces a result which is called “Hash Code” or “Message Digest” or “Hash Value”.

A Hash Value of a stream of data which we normally read in the computer as “My Name is Naavi” using MD5 algorithm looks like the following.

ece376f327f3128a4aca3e823a5ab334

If the above sentence is modified as “My name is Naavi”, then the hash value would be

4dd7fe3dd404bd0fca37592a8bbd6c75

Note that when the capital “N” in “Naavi” is changed to “n”, the hash code shows a significant change.

This is the unique character of the hash algorithm that it produces a unique hash value for a document and any minor change would show up as a change in the value. No two documents can produce the same hash value unless they are absolutely identical bit by bit. This property is used in digital signatures to check the "Data Integrity" of a document between the time the document is signed and the time the signature is verified.

By calculating the hash value of an electronic document at two different points of time, one can check if there has been any change that has been made in the document during the period.

What is Asymmetric Cryptosystem?

Asymmetric Cryptosystem is a system of encryption and decryption of electronic documents where the encryption key is different from the decryption key but the two are related in such a manner that any document encrypted with one of the keys of the pair can be decrypted with the other key of the pair.

The Asymmetric Cryptosystem has an advantage over the Symmetric Cryptosystem where the encryption and decryption keys are same. If Mr X does the encryption which has to be decrypted by Mr Y, X has to send the decryption key to Mr Y. If the encryption and decryption keys are same as in the case of "Symmetric encryption" then Mr Y as well as any person who can steal the encryption/decryption key during transmission can use the key just as Mr X would use. Hence from an encrypted document it is not possible to find out who exactly has encrypted a document.

On the other hand, if Asymmetric Crypto System is used for encryption, Mr X can use one key for encryption and send the other key of the pair to Mr Y for decryption. In the use of Asymmetric Encryption, out of the two keys of the pair, one is designated as “Private Key” and the other is designated as “Public Key”. The Private Key is kept confidential and always used by the person who creates the key pair for encryption. Such encrypted documents can be decrypted with the use of the corresponding public key which is freely distributed.

Thus whenever an encrypted document can be decrypted with the use of the public key of Mr X, one can conclude that the key used for encryption must be the private key of Mr X. Since by convention the private key is always kept with the person who generated the key pair and held confidential, no body else is expected to have access to the private key and the fact that the private key has been used for encryption proves that it must have been encrypted by Mr X only.

In view of this, Asymmetric Crypto System enabled identification of the person who has encrypted a document and serves part of the requirement of a “Digital Signature”.

How Digital Signature is Constructed

The properties of Hashing and Asymmetric Cryptosystem is used in combination to create a digital signature of an electronic document which authenticates the document and confirms who has signed the document and also confirms that no change has occurred in the document since it has been signed.

For this purpose, a document which needs to be digitally signed is first passed through a hashing algorithm which generates the “Hash Code” of the document. Then using the private key of the person who intends signing the document, the hash code is encrypted. This encrypted file of the hash code constitutes a digital signature.

Thus we can define a "Digital Signature" of a person X on document D is the hash value of D encrypted with the private key of X.

After creating such a digital signature of a document, the person creating the digital signature will attach the digital signature file to the document and forward it to the person who has to read the document. If the addressee of the document has to rely on the document, he verifies the digital signature by first decrypting the digital signature file using the public key of the sender which yields the hash value as calculated by the sender and then calculates the hash value of the document once again at his end and compares it with the decrypted hash value. If the two hash values are same it means that the document has not been changed since it has been last signed. Since the successful decryption with the public key of the person indicates that the encryption was done by the owner of the public key, he will consider the document as having been "signed".

One may understand from the above process that

> *"Digital Signature" of a person of a document is the hash value of the document encrypted with the private key of the person.* (Naavi's definition as applicable in India).

We can also conclude that "Digital Signature" is not the "Scanned form of a physical signature" nor "Scanned form of thumb impression" or any other biometric technique of identification or use of passwords or tokens.

Effect of Digital Signature

Section 5 of the ITA 2000/8 provides legal recognition of "Digital Signature" to "Signature" as we know in the paper world.

The section states:

> *“Where any law provides that information or any other matter shall be authenticated by affixing the signature or any document should be signed or bear the signature of any person then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of digital signature affixed in such manner as may be prescribed by the Central Government. “*

Administration of Digital Signature System

One of the features of the Digital Signature is that it consists of a pair of encryption/decryption keys and one of them namely the Public Key has to be distributed to the intended recipient of the message through a trusted third party. Further, the hash algorithm as well as the key generation mechanism has to be handled through standard error proof software. These functions are discharged by an intermediary called the "Certifying Authority". They play a very crucial role in the administration of Cyber Laws.

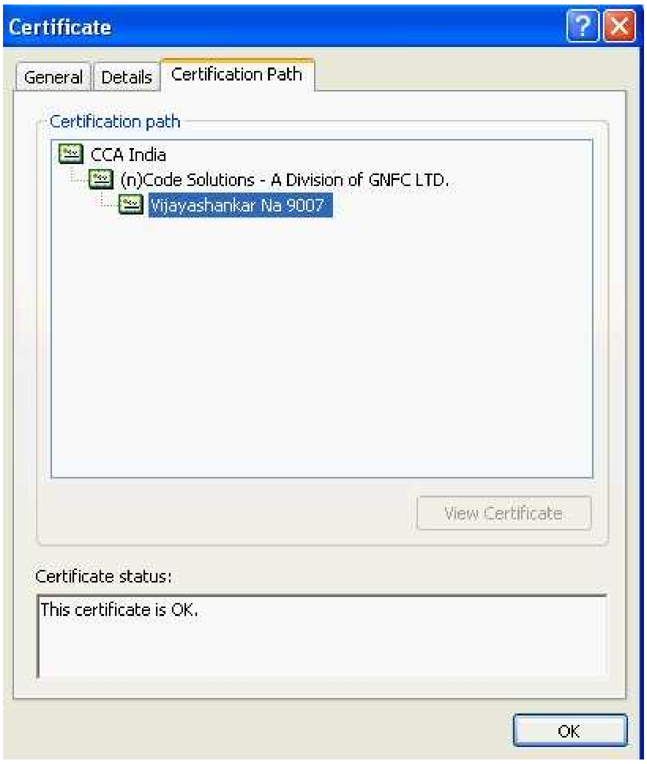
Certifying Authorities deliver their services through " Digital Certificates" which is the product they produce, distribute and maintain in conformity with the legal requirements and subject to commercial viability.

The Certifying Authority business is the important commercial offshoot of the passage of Cyber Laws and introduction of Digital Signatures in business. It lends opportunities for business houses with a good reputation, and technical ability to take up the business as "Certifying Authorities" or "Registration Authorities". Individuals can also act as authorised agents of Certifying and Registration Authorities for the purpose of “physical identification and authentication of documents”.

Digital Certificate:

Digital Certificates are the products issued by Certifying authorities for the purpose of enabling a person to affix “Digital Signatures”. They are issued to individuals for signing e-mails, or digital files. They are also issued for “Secured Servers”. Enterprise level certificates are also issued for enabling employees of a Virtual Private Network to communicate in a secured manner and identify each other through digital signatures.

Digital Certificates are identification devices for transactions on the Internet. The digital certificate is an electronic file that contains the public key of a person and the details such as his name, validity period etc., encrypted with the private key of the Certifying authority. A typical digital certificate for personal e-mails looks as under to a recipient.


Certificate

Certification path

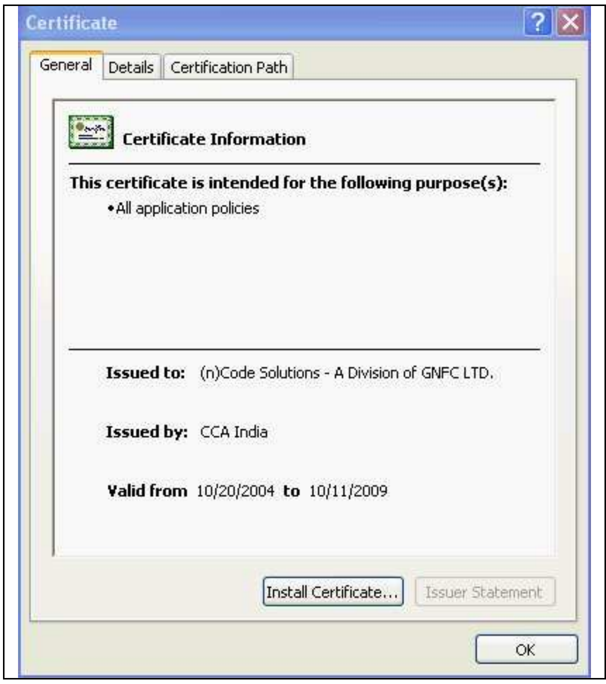
CCA India
(n)Code Solutions - A Division of GNFC LTD.
Vijayashankar Na 9007

Certificate status:

This certificate is OK.

Please note the certification path of the certificate. It is issued by the Certifying Authority, (n) code which itself derives the authority from the root certifying authority CCA.

The digital certificates of (n) code and CCA will look as follows.



Certificate Information

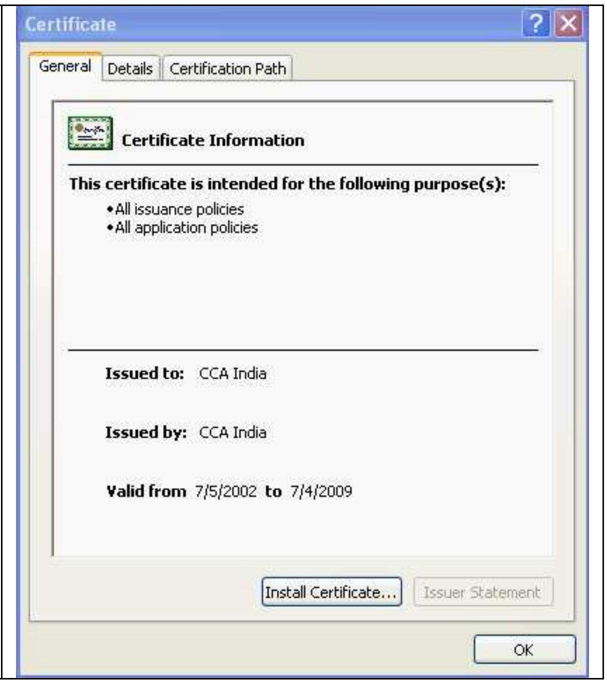
This certificate is intended for the following purpose(s):

- All application policies

Issued to: (n)Code Solutions - A Division of GNFC LTD.

Issued by: CCA India

Valid from 10/20/2004 to 10/11/2009



Certificate Information

This certificate is intended for the following purpose(s):

- All issuance policies
- All application policies

Issued to: CCA India

Issued by: CCA India

Valid from 7/5/2002 to 7/4/2009

Licensing:

In order to issue digital certificate valid in law, the Certifying authority has to be "Licensed". During the process of licensing, the Certifying authority is himself issued a "Digital Certificate" by the representative of the legal authority of a country called the "Root Certifying Authority".

Certifying Authorities in India.

According to the ITA-2000, digital signatures backed by digital certificates issued only by those Certifying authorities who have been licensed in India would be considered legally valid in India. Any other Digital signature, even though subscribing to the same security standards as envisaged under the laws, will not have legal sanctity.

At present the following organizations have been licensed as Certifying Authorities.

1. Safescrypt Ltd, a joint venture between Sify Ltd and Verisign
2. Tata Consultancy Services
3. (n) Code Solutions, a subsidiary of GNFC
4. MTNL
5. IDRBT (Institute for Development and Research in Banking Technology), A division of RBI for issue of digital certificates to Bank employees
6. NIC (National Informatics Center), a division of the Department of Information Technology, Government of India, for issue of

digital certificates to the Government sector.

7. e-Mudra CA, a division of 3i Infotech Consumer Services Ltd

Details of the terms and conditions under which each of these Certifying Authorities issue Digital Certificates is available on their websites. Links to the websites of licensed Certifying Authorities is available on the CCA’s website http://www.cca.gov.in.

The digital certificates of the CCA is available for download from the CCA’s website above. Similarly the digital certificates of the Certifying Authorities is also available from their respective websites.

These certificates can be downloaded and installed in the applications such as outlook express along with the digital certificate of the subscriber.

Secured Digital Signatures

The Government of India has prescribed a security procedure under ITA 2000 which accords a better evidentiary value to digital signatures which are termed “Secured Digital Signatures”.

Secured Digital Signature system is one where the key pair is generated in a hardware token such as a cryptographic key or smart card, and digital signature is created only in the hardware token. The private key is always held in the token and not exported outside even to the user’s computer.

How to Use Digital Signatures

Use of digital signatures requires that the user has the pair of keys with him and the appropriate hashing algorithm. He also requires the software that can calculate the hash and do the encryption.

When a person applies for and obtains the digital certificate, he generates the key pair and stores the private key securely in his computer. Hashing algorithms are also made available by the CA at the time of the installation of the certificates if not already available in the operating system.

Standard e-mail client applications such as Outlook express or Mozilla Thunderbird as well as applications such as Microsoft Office have an inbuilt capability of creating hash of the document and to search for the private key, encrypt the hash value and embed the encrypted hash value (digital signature) with the document.

Other stand alone applications are also available for application and verification of digital signatures.

Legal Liabilities in wrong usage of Digital Signatures

The users of digital signatures in India have two important obligations namely

1. Obtain the digital certificates with correct particulars stated there in.

Providing in-correct particulars for obtaining the digital certificates and using a certificate with false particulars or with fraudulent intention are offenses under ITA 2000/8 carrying imprisonment of 2 years and fine of RS 1 lakh.

2. Keep the Private key confidential and ensure that in case of suspected compromise of the private key inform the CA without delay.

Certain Unresolved Issues

Users should be aware of some of the following issues while using digital signatures.

1. Some of the digital certificates issued by Certifying Authorities may work only for specific applications and may not be available for all purposes such as digitally signing an e-mail.
2. Users who use web mail services cannot apply digital signatures on the

mails unless they have POP access for the mails.

3. Secured Digital Signature users cannot use digital signatures for encryption of the document during transmission
4. Certain digital signature certificates are not compatible with the latest versions of operating software that the user may be using.
5. Revoked Certificates are not renewed by CAs even within the original validity period and may have to be re purchased.
6. Certification revocation list and repository of digital certificates issued are not always current and special care has to be taken while relying on certificates which cannot be checked for revocation.

Some Precautions:

1. Users should themselves pick up digital certificates at the time of first issue and not entrust the work to their subordinates

2.Users should not allow any other person to use the digital signatures on their behalf including their Chartered Accountants as it amounts to a compromise of the private key.

3. After obtaining the digital certificate, users should check and ensure that the name and e-mail address on the digital certificate is correct and belongs to them only.

Summary

Information Technology Act 2000/8 defines the term Digital Signature and provides it a legal equivalence to signatures as we know in the physical world of paper based documents. It is a technical system which uses hashing and asymmetric cryptosystem. The Government has appointed CCA as the root certifying authority which has licensed several Certifying Authorities who issue digital certificates to applicants that enable them use digital signatures on electronic documents. Persons desirous of using the digital signatures should apply and obtain digital certificates from any of the licensed Certifying Authorities. They have to install the certificates in their computers and use an appropriate application that can create the digital signatures for the documents in the computer. Users have to ensure that the private key is always kept confidential and report compromise of the key to the respective CA so that it can be revoked. Users should also ensure that the digital certificates carry their correct name, address and e-mail address and get it corrected if required before using the certificates.

For Complete discussion of Cyber Laws in India,

Visit www.naavi.org

Also Read E Book Cyber Laws For Engineers which can be downloaded from http://www.naavi.org/ebook2011

For Online Course in Cyber Laws, visit www.Cyberlawcollege.com

For Corporate Training on HIPAA and ITA 2008 Compliance contact Naavi@vsnl.com

For Archival of digital evidence, visit www.ceac.in