Digital Signature
Signing the digital way

by **CA Tapas Ruparelia**

Introduction

The Central Board of Direct taxes announced on 1st July 2011, that all Individuals, HUFs and Partnership Firms who are liable to get their accounts audited under the Income Act 1961 will have to file their Income-Tax return online compulsorily using Digital signature for the financial year 2010-11.

Many people confuse a Digital Signature with an e-signature. An e-signature is a scanned image of your physical signature while Digital Signature is not a facsimile of a person's physical signature. A document with a **Digital Signature** will not contain any traditional signature but it will simply state that it has been digitally signed by (name of the person signing it). To know about **Digital Signatures** we will first have to understand what **Digital Signature Certificates** are.

What is a Digital Signature Certificate?

A Digital Signature Certificate, like hand written signature, establishes the identity of the sender filing the documents through internet which sender can not revoke or deny. Digital Signature Certificates (DSC) are the digital equivalent (that is electronic format) of physical or paper certificates. Examples of physical certificates are drivers' licenses, passports or membership cards. A digital certificate can be presented electronically to prove your identity, to access information or services on the Internet or to sign certain documents digitally. In simple words, a document can be **Digitally Signed** using a **Digital Signature Certificate.**

Why is Digital Signature Certificate (DSC) required?

Like physical documents are signed manually, electronic documents, for example e-forms are required to be signed digitally using a Digital Signature Certificate. The Information Technology Act, 2000 provides for use of Digital Signatures on the documents submitted in electronic form in order to ensure the security and authenticity of the documents filed electronically. This is the only secure and authentic way that a document can be submitted electronically. Moreover a Digital Signature is the only way one can authenticate electronic or online transactions “legally”. The potential for Digital Signatures is huge in services like e-procurement, filing of returns, filing of export-import licenses, financial transactions, digitization of land records, while using e-commerce web-sites and other transactional portals and other online transactions like internet banking. You can even encrypt information in your e-mail using a private key of a **Digital Signature**.

Types of Digital Signature Certificates:

There are basically 3 types (or classes) of Digital Signature Certificates Class-1, Class-2 & Class-3, each having different level of security.

Class 1 signatures are used for identification of username/email ID. However it cannot be used to sign any Statutory / Business Documents whereas Class 2 & Class-3 -DSCs are issued to the Individuals and can be used for either Personal or Business Purposes.

Class 2 signatures can be availed from Dealers / Resellers of Certifying Authority, by submitting the prescribed documents. Here, the identity of a person is verified against a trusted, pre-verified database.

Class 3 signature is the highest level where the person needs to present himself or herself in front of a Registration Authority (RA) and prove his/ her identity by submitting the documents.

How does it work!!

TECHNICAL ASPECTS:

Digital signatures are an application of asymmetric key cryptography. Cryptography is primarily used as a tool to protect national secrets and strategies. It is extensively used by the military, the diplomatic services and the banking sector.

CRYPTOGRAPHY:

Cryptography is the science of using mathematics to encrypt and decrypt data. It enables a person to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient

Data that can be read and understood without any special measures is called plaintext or clear text. Data which requires some special function to be performed on it before it can be read and understood, is called cipher text. The same plaintext, encrypted by using different keys, will result in different cipher text. The security of encrypted data is entirely dependent on two things: the strength of the cryptographic algorithm and the secrecy of the key.

Encryption is used to ensure that information is hidden from anyone for whom it is not intended, even those who can see the encrypted data. The process of reverting cipher text to its original plaintext is called decryption.

A cryptographic algorithm, or cipher, is a mathematical function (known as hash function) used in the encryption and decryption process. This hash function works in combination with a key (private key) to encrypt the plaintext (the original message).

The hash function software produces a fixed length of alphabets, numbers and symbols for any document. This is known as the hash result. However, the contents of this fixed length are never the same for two different documents. If even one letter in the document is altered, an entirely different hash result will be generated. The hash function software will always produce the same hash result for a particular message & it is practically impossible to reconstruct the original message from the hash result.

Customers are given two codes for verification —private and public keys. The public key and private key are nothing but extremely large numbers. Although the keys are mathematically related, it is almost impossible to obtain the private key by using the public key. If a particular private key was used to "sign" a message, then only the corresponding public key will be able to verify the "signature". A Digital Signature usually contains owners name, company name and address, public key, certificate serial number, expiry date of the public key, certifying company ID, and Certifying Company's Digital Signature.

Illustration

1) CHETAN wants to digitally sign emails and electronic contracts. So he would use computer software (asymmetric crypto system) to generate two keys, a public key and private key. CHETAN will give his public key to the whole world but will keep his private key to himself. Once he has done that, he can use his private key to sign contracts etc. Anyone can use CHETAN's public key to verify his signature. That's where the problem begins. How can anyone be sure which is CHETAN's public key? What if Mr. CHETAN denies that a particular public key is actually his? To solve this problem digital signature certificates are used. CHETAN would apply to a licensed CA (Certifying Authority) for a digital signature certificate.

As part of the application process he would submit identification documents as discussed earlier. He would also send his public key to the CA. The CA would then "certify" the public key as belonging to Mr. CHETAN and issue a digital signature certificate that contains Mr. CHETAN's public key along with information identifying him.

Now CHETAN wants to enter into a transaction with Pankaj. He composes an electronic document containing the words:

I, CHETAN owe Pankaj the sum of Rs. 500 only.

Using his computer CHETAN runs this document through a hash function. The computer then performs the process on the document as discussed above.

CHETAN now uses his computer to “sign” the hash result of his document. His computer software uses his private key to perform some calculations upon the hash result. This produces a signature, which consists of some digits. This set of digits is attached to the hash result.

CHETAN now sends the original message and the signed message digest (hash result) to Pankaj. Pankaj has the same hash function software on his computer. He also has his (CHETAN’s) public key. When Pankaj receives CHETAN’s email, he runs the original document through the hash function software and generates a hash result. The computer compares this hash result with the one that was sent to him by CHETAN. If the two hash results are the same, it means that the message is unaltered.

Pankaj also verifies whether CHETAN’s private key was actually used to sign the hash result. For this Pankaj’s computer uses CHETAN’s public key. Only a message signed by CHETAN’s private key can be verified using CHETAN’s public key.

Cost and validity

A Digital Signature certificate has to be purchased from a government-licensed Certification Agency known as “Certifying Authority (CA)”. Certifying Authority (CA) means a person who has been granted a license to issue a digital signature certificate under Section 24 of the Indian IT-Act 2000. At present, there are eight such agencies (CAs) namely, IDRBT, iCERT (Customs and Central Excise) and MTNL. Tata Consultancy Services (TCS), Safescrypt (from Sify), (n)Code Solutions (from GNFC), and e-Mudhra (from 3i Infotech).

The Digital Signature Certificates come with a validity period of one-two years, implying there is a cost attached. We are not used to paying for our own signature.

While Digital Signatures are estimated to cost CAs Rs. 175-225, individuals typically end up paying anyway between Rs. 1,500 and Rs. 3,000 —and sometimes even up to Rs. 7,000 for the high-level Class-3 security certificates. The prices include a one-time payment for a crypto (USB) e-token, which contains the software. Typically, if you want to use a digital signature for sensitive transactions like e-filing of returns or internet banking & broking then the costs are between Rs. 2,200 (without token) to 3,200 (with token). Much depends on the bundling schemes & packages offered by the distributors.