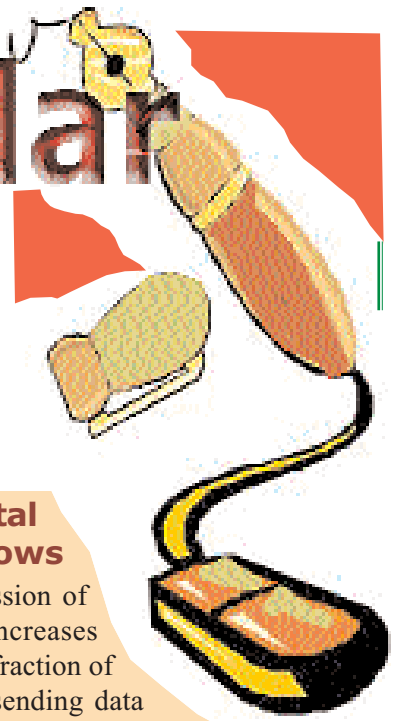
Digital Signature gets popular



Electronic signatures are already quite popular in various transactions in India. Read on to know the nitty-gritty of the system from the point of view of professionals.

Rajeev Khandelwal

Electronic signatures such as use of passwords and smart cards are already quite popular in various transactions. With technological advancement, digital signature -- a new type of electronic signature --, is coming to the forefront. Simply stated, it means use of some distinct digits in place of one's signature. It is an electronic aid to authenticate the identity of the sender. It is the extra data attached to a message that identifies and authenticates the sender and ensures that the original message is not altered in any manner. *The Information Technology Act of India, 2000 defines Digital signature as authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the relevant provisions.* This Act came out with a detailed policy on digital signatures and gave it the same status as that of physical signatures. In fact, Digital signature is safer than a hand written one as it cannot be forged. Moreover, if a contract is signed by the parties on the last page, there is no way one can check whether the other pages have been replaced or not. However, digital signatures on the same contract will ensure that the original contract is intact and not even a single letter has been changed.

Need for Digital Signature grows

Electronic transmission of data no doubt increases speed that too at a fraction of the cost spent on sending data manually. However, the following issues call for attention:

Authentication: Since there is no physical contact between the parties, it is important to ensure that the person with whom one is interacting, is in fact the same person with whom he intends to interact.

Confidentiality: Security is another major concern. Even if the data has reached the intended person, there is no guarantee that it has not been intercepted by anyone on the way to misuse it.

Integrity: The data received should be exactly the same as the data sent. Just to give a simple example, imagine the plight of a company who submits a tender online and a zero is added after the tendered amount during transmission accidentally or otherwise. Most of us feel that data sent by e-mail is absolutely safe. But this is far from the truth. Email is like an open letter. The data in the e-mail can be altered by anyone who has access to it.

Non-repudiation: In a written agreement, the parties are bound by their physical signatures, which they

The author is a member of the Institute. He can be reached at rajeev_khandelwal@hotmail.com

put on the agreement. At a later stage, none of the parties can back out of the agreement. A similar binding force is needed when parties deal electronically. Assessing the validity of contracts is complicated in the case of electronic transactions because the contracts are paperless.

Nowadays the Digital Signatures are becoming more and more popular due to following reasons:

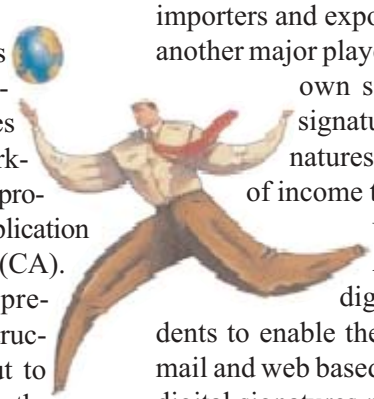
(a) Digital certificate can be used to access membership-based web sites automatically without the need for user name and password.

(b) It enables the recipient to ensure that the sender has sent the data and that the data has not been changed or tampered with.

(c) It enables others to send private messages to the person who has Digital Signature. No other person would be able to read the private message.

Position in India

The IT Act was passed in the year 2000 and is applicable to the whole of India. It has authorised the Controller of Certifying Authorities (CCA) to issue licenses and regulate the working of Certifying Authorities (CA). A detailed procedure has been prescribed for making an application for appointment as a Certifying Authority (CA). Inter alia, the applicant should have the prescribed net worth and the necessary infrastructure. Further, a detailed audit is carried out to ascertain its eligibility. To invite more players, the mandatory bank guarantee for CA for digital signatures has been slashed to Rs 1 crore from Rs 10 crore. The fee for acquiring digital signature would also significantly come down with the growth in subscriber base.



A Certifying Authority issues a digital signature certificate to individuals or organisations to enable them to prove the authenticity of data sent electronically. When a CA issues a certificate for a digital signature to a person it basically authorises the person to use the digital signature as he uses his manual signature. But there is a basic difference.

Whereas manual signature can be put anywhere, a digital signature can only be used for the purpose for which it has been issued. CCA maintains a National Repository of Digital Certificates (NRDC) containing all the certificates issued by the CAs in the country. At present, Safescrypt, Tata Consultancy Services, National Informatic Centre and MTNL are the major CAs authorised to issue digital signatures. SafeScrypt is the first CA in India. It has recently signed a MoU with the Director General of Foreign Trade (DGFT) to issue digital certificates to importers and exporters. Tata Consultancy Services is another major player in the market. It has developed its own software for implementing digital signature technology. It issued digital signatures to intermediaries for online filing of income tax returns. Recently it has also tied up with the Institute of Chartered Accountants of India for issue of digital signatures to CAs and its students to enable them to carry transactions such as e-mail and web based services electronically. NIC issues digital signatures mainly to government departments. As a licensed CA, MTNL can issue digital signatures to its subscribers for a host of services. In the near future, a Trump subscriber shall have digital signature on his pre-paid SIM-card and shall be able to recharge his account with it without having to rush to the nearby shop. A customer shall also be able to apply online to activate his STD facility and other facilities.

Digital signature is safer than a hand written one as it can't be forged. If a contract is signed by the parties on the last page, there's no way to find whether other pages have been tampered with. But digital signatures on the same contract will ensure that original contract is intact and not even a single letter is changed.

Content of Digital Signature Certificate

Digital certificates are electronic certificates. They serve the same purpose as that of physical certificates. For example, a physical share certificate is a proof that the person named therein is the holder of the specified number of equity shares of a particular company. Similarly, a person can show his digital certificate electronically to prove his identity or his right to access information or services on the Internet.

The IT Act was passed in year 2000 and is applicable to whole of India. It authorises Controller of Certifying Authorities to issue licenses and regulate working of Certifying Authorities (CA). A detailed procedure has been prescribed for applying for appointment as a CA.

There is no need to keep a digital certificate hidden from others as it does not contain any confidential information. It should be available to anyone who wants to send encrypted email. The browser automatically sends the digital certificate whenever one signs an email message.

A Digital Signature Certificate contains the following data:

(a) Serial Number (which distinguishes it from other digital certificates);
(b) Signature Algorithm Identifier (which identifies the algorithm used by Certifying Authority to sign the Digital Signature Certificate);
(c) Issuer Name (name of the CA who issued Digital Signature Certificate);
(d) Validity period of the Digital Signature Certificate;
(e) Name of the subscriber (whose public key the Certificate identifies); and
(f) Public Key information of the subscriber.

Types of D-Certificates

Personal certificate: A Personal certificate identifies the person to whom it is issued. It includes the name and personal particulars of an individual. It is normally used for securing e-mail messages and to access various websites without the use of username and password. e.g. ICICI Webtrade Ltd. has taken personal certificates for its employees who are required to digitally sign contract notes.

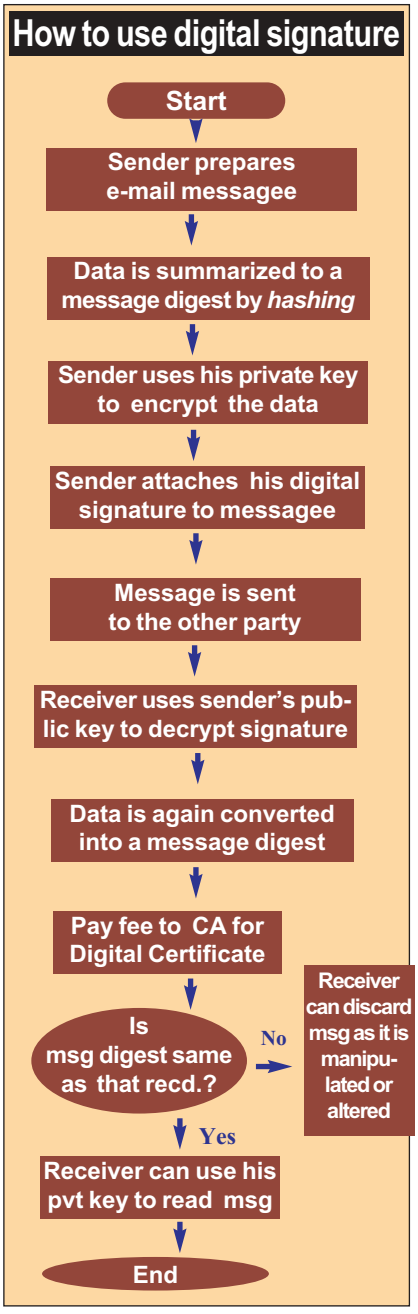
Server certificate: A Server certificate identifies a server or a computer. It includes the name of the host e.g. www.icicibank.com. For security, the bank has given username and password to its account holders to access their account or make online payments and avail other services. For greater security, the bank has taken a server certificate which ensures that the information exchanged between the account holder's computer and the website of the bank over the Internet is secure and cannot be accessed by any third party.

Procedure

a. To obtain digital signature, one has to apply in the prescribed form to a certifying authority (CA) together with the necessary documents such as proof of identity, proof of residence etc., and the necessary fee.

b. The CA verifies the documents submitted. The case is approved if the documents are in order and is as per the policy laid down for this purpose. Otherwise, more information is asked for or the case is rejected.

c. On approval, the CA issues a digital certificate to the applicant. It also provides a private key and a public key to the applicant. The certificate guarantees that the holder of the public key is the same person who holds the private key. The certificate is digitally signed. Just as in case of a physical certificate, the date of issue of certificate is given in the digital certificate. The period for which the certificate is valid is also given. Normally, a document



In the near future, a Trump subscriber shall have digital signature on his pre-paid SIM-card and shall be able to recharge his account with it without having to rush to the nearby shop. A customer shall also be able to apply online to activate his STD facility and other facilities.

signed with an expired key should not be accepted.

d. On receiving a digital certificate, the holder can use Public Key Infrastructure (PKI) to enter into secure electronic transactions. PKI is the combination of software, technology, certifying authority, issue of digital certificates to individual users and servers, tools for managing, renewing, and revoking certificates and related services, which enable electronic transactions. It is an overall Internet security system, which protects the security of the communications and business transactions on networks. PKI helps to trace any person who has used a digital signature for entering into any transaction and therefore he cannot back out of the transaction.

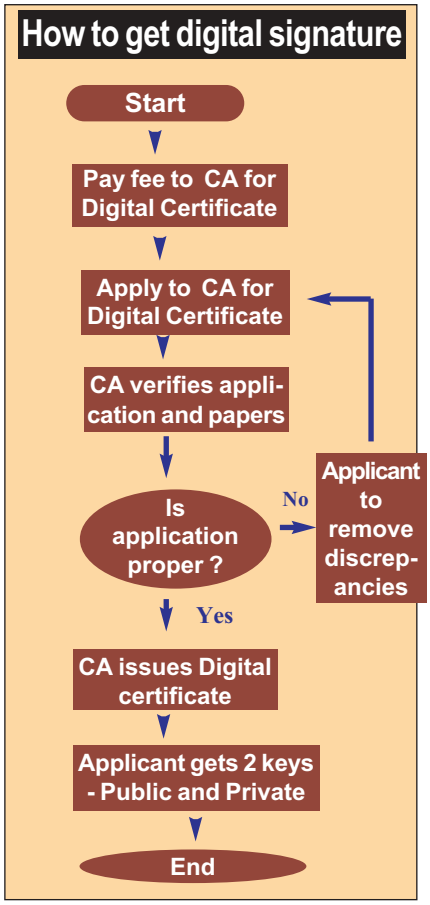
e. Specifically, the holder can use his distinct keys for the transmission of data or for other purposes. A physical key is used to lock or unlock a safe, a door and so on. The keys of a digital signature perform a similar task. These keys are mathematically related and are used to encrypt and decrypt the digitally signed documents. One of the two keys can encrypt data and the other key can decrypt that data. Encrypting means translation of information from readable form into some unreadable form. In other words, it means jumbling of information so that only a person with the necessary key can make it readable again. Decryption is the conversion of encrypted data back into readable form.

This can be explained with the help of a simple example: The Head office of a company sends quotations to its branch office for various tenders by e-mail. Since e-mail is not very secure, it uses a code system to send the quotation. It uses alternate alphabets for digits from 0 to 9. i.e. A=0, C=1, E=2, G=3 and so on. Therefore, the quotation figure - CGAAAAA would mean 13,00,000 but only the branch office shall be able to read it as it has the key or algorithm or the rule to decipher it.

f. The holder of a digital certificate uses his software to summarise the data, which he wants to send, into a few lines called a message digest by a process called hashing. A message digest is like a fingerprint of a person. The slightest change in a fingerprint would mean inability to track the right person. Similarly, a small change in the message digest would mean a lot of change in the original data.

g. Private key is available only to the holder of digital signature and is stored in his computer. For better security, it can be copied to a tamper-proof hardware token. The sender uses his private key to encrypt the message digest. Use of a digital signature per se does not encrypt the message. To ensure the privacy of the message, the sender should encrypt it using the receiver's public key.

h. Public key of the sender is available to the public at large. On receipt of the message, the software in the receiver's computer uses the public key of the sender to decrypt the signature. This proves that the sender has signed the document because only he has his private key.



i. The data is then again hashed into a message digest. If this message digest is the same as the message digest received from the sender, the receiver can be sure that no alteration has been made in the original message. The receiver can read the message by decrypting it with his private key.

Limitations Of Digital Signatures

a. The digital signatures are much more secure and safe but even their use cannot guarantee 100% safety from hacking and forgery.

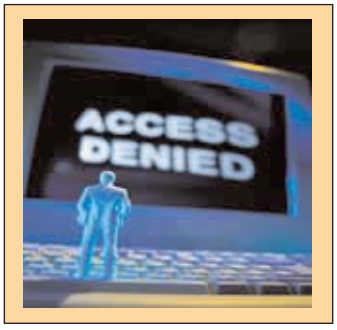
b. Use of Digital Certificates means recurring cost for the users as they are issued for a particular duration. Thereafter, they have to be renewed on payment of necessary fee.

c. Different authorities prescribe use of different digital signatures. For example, the Institute of Chartered Accountants issues certificates to its members exclusively for dealing with it filing of forms etc. Similarly, National Securities Depository Ltd. (NSDL) requires the assessees to obtain separate signatures for filing TDS returns electronically. Director General Foreign Trade (DGFT) also requires separate digital signatures for filing returns online with it. Considering the multiple government departments and other entities an organisation has to interact with, the number of digital signatures it would have to take is anybody's guess. Moreover, digital signature is for an individual and not for an organization. Therefore, an organisation would have to take different digital signatures for a person for different purposes. This not only increases cost for the user but is inconvenient as well.

The cost of issue is a major dampener on the use of Digital Signatures, particularly because it happens to be a cost of the recurring nature. Obtaining separate digital signatures for different entities is also a major irritant.

Conclusion

E-commerce is still in a very nascent stage, particularly in developing countries like India. People avoid giving their credit card and other personal details due to security considerations. Frauds worth millions of dollars have been committed due to low security levels in the use of credit cards. Online transactions such as transfer of funds in bank accounts, buying and selling, making application for and renewal of licenses, paying fines and bills of utilities are gaining popularity. In the not so distant future, it would be mandatory to do some of these transactions electronically using digital signature.



As a live example, the Income Tax Department Department first made e-filing of TDS returns through authorised TIN facilitation centres mandatory for companies. In the next stage, they have been recently given the facility of filing e-TDS returns online from one's own computer using digital signatures. In due course of time, this would also be made mandatory. The Income Tax Department has already undertaken the pilot project for online filing of Income Tax returns through banks. Recently it has extended the deadline for filing Income Tax returns for financial year 2003-04 to 31st October, 2004. Apparently this extension was given to finalise the modalities of appointing Chartered Accountants, tax consultants etc. as e-intermediaries who shall electronically file Income Tax returns for their clients. For this, they would need digital signatures. In fact, everyone who wants to or rather has to deal electronically, would need digital certificates.

Use of Digital Signatures can lead to a quantum jump in electronic transactions as it addresses the concerns of the transacting parties as to confidentiality, integrity, authenticity and non-repudiation. However, the cost of issue is a major dampener on the use of Digital Signatures, particularly because it is a recurring cost.

Necessary changes should be made by Government so that a single digital signature suffices for a person just as a manual signature.